EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

인공 지능에 관한 조화* 규칙(인공지능법) 제정 및 특정 유럽 연합 법규 개정을 위한 유럽 의회 및 유럽 이사회의 규정(Regulation) 제안

*** 국제협력담당관 주석**

'EU 조화 규칙'(harmonised rules) 또는 'EU 조화 법령'(harmonization legislation)은 EU의 입법 방식 중 하나로서, GDPR과 같은 통일 규칙(unified rules) 제정이 어려운(비효과적인) 분야에 대해서, "회원국 법률의 주요 차이점을 제거하고, 회원국이 준수해야할 최소한의 요구사항 또는 공통표준을 만드는 방식'을 의미합니다. 기존의 EU 조화 법령 목록은 본 규정(AI법) 부속서II에 열거되어 있습니다.

참고로, ESO(유럽표준개발기구)가 제정하는 표준 중에서도 EU 조화 법령에 따라 제정되는 표준을 '조화 표준(harmonised standard)'으로 칭하고 있습니다.

EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

유럽연합 집행위원회

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

인공 지능에 관한 조화 규칙(인공지능법) 제정 및 특정 유럽 연합 법규 개정을 위한 유럽 의회 및 유럽 이사회의 규정(Regulation) 제안

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Artificial Intelligence (AI) is a fast evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy. Such action is especially needed in high-impact sectors, including climate change, environment and health, the public sector, finance, mobility, home affairs and agriculture. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society. In light of the speed of technological change and possible challenges, the EU is committed to strive for a balanced approach. It is in the Union interest to preserve the EU's technological leadership and to ensure that Europeans can benefit from new technologies developed and functioning according to Union values, fundamental rights and principles.

This proposal delivers on the political commitment by President von der Leyen, who announced in her political guidelines for the 2019-2024 Commission "A Union that strives for more"[1], that the Commission would put forward legislation for a coordinated European approach on the human and ethical implications of AI. Following on that announcement, on 19 February 2020 the Commission published the White Paper on AI - A European approach to excellence and trust[2]. The White Paper sets out policy options on how to achieve the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of such technology. This proposal aims to implement the second objective for the development of an ecosystem of trust by proposing a legal framework for trustworthy AI. The proposal is based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them. AI should be a tool for people and be a force for good in society with the ultimate aim of increasing human well-being. Rules for AI available in the Union market or otherwise affecting people in the Union should therefore be human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights. Following the publication of the White Paper, the Commission launched a broad stakeholder consultation, which was met with a great interest by a large number of stakeholders who were largely supportive of regulatory intervention to address the challenges and concerns raised by the increasing use of AI.

The proposal also responds to explicit requests from the European Parliament (EP) and the European Council, which have repeatedly expressed calls for legislative action to ensure a well-functioning internal market for artificial intelligence systems ('AI systems') where both benefits and risks of AI are adequately addressed at Union level. It supports the objective of the Union being a global leader in the development of secure, trustworthy and ethical artificial

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.

해설서

1. 제안의 배경

1.1. 제안의 이유 및 목적

본 해설서(explanatory memorandum)는 인공 지능에 관한 조화 규칙(인공지능법)을 제정하는 규정(Regulation)에 대한 제안에 수반된다. 인공 지능(AI)은 산업과 사회 활동의 전 영역에 걸쳐 광범위한 경제적·사회적 편익을 창출할 수 있는 빠르게 진화하는 기술이다. 인공 지능의 사용은 예측을 개선하고, 운영과 자원 할당을 최적화하며, 서비스 전달을 개인화함으로써 사회적·환경적으로 유익한 결과를 이끌어내고 기업과 유럽 경제의 경쟁력을 크게 높여줄 수 있다. 이러한 기술은 특히 기후 변화, 환경 및 보건, 공공 부문, 금융, 모빌리티, 행정, 농업 등 영향이 큰(high-impact) 부문에 필요하다. 하지만 AI의 사회 경제적 편익을 뒷받침하는 기술과 요소들은 또한 개인과 사회에 새로운 위험 또는 부정적 결과를 초래할 수 있다. EU는 기술 변화의 속도와 예상되는 과제에 비추어 균형 잡힌 접근법을 개발하기 위해 노력하고 있다. 유럽 연합의 관심사는 EU의 기술 리더십을 유지하고 유럽 시민들이 유럽 연합의 가치와 기본권 및 원칙에 따라 개발되고 기능하는 새로운 기술을 유익하게 활용할 수 있도록 하는 것이다.

본 제안은 2019-2024 유럽연합 집행위원회를 위한 정책 가이드라인 "더 많은 것을 위해 노력하는 유럽 연합(A Union that strives for more)"[1]에서, 유럽연합 집행위원회가 AI의 인간적·윤리적 함의에 대한 협의된 유럽 접근법을 모색하기 위한 법안을 제출할 것이라고 발표한 폰 데어 라이엔(von der Leyen) 위원장의 정치적 공약을 이행하는 것이다. 이 발표에 이어, 2020년 2월 19일 유럽연합 집행위원회는 인공 지능 백서(White Paper on AI - A European approach to excellence and trust)[2]를 발표했다. 이 백서는 AI의 활용을 촉진하고 그러한 기술의 특정한 사용과 관련된 위험을 관리하는 이중의 목표를 달성하는 방법에 관한 정책 대안을 제시한다. 본 제안의 목적은 신뢰할 수 있는 AI를 위한 법적 프레임워크를 제안함으로써 신뢰 에코시스템의 개발을 위한 두 번째 목표를 이행하는 것이다. 본 제안의 목적은 EU의 가치와 기본권을 바탕으로, 사용자들이 안심하고 AI 기반 솔루션을 수용할 수 있도록 지원하는 한편 기업들이 그러한 솔루션을 개발하도록 장려하는 것이다. AI는 인간의 행복을 증진한다는 궁극적 목표 하에 사람들을 위한 도구가 되고 사회의 선(善)을 위한 동력이 되어야 한다. 따라서, 유럽 연합 시장에서 사용되거나 유럽 연합의 시민에게 영향을 주는 AI를 위한 규칙은 인간 중심적인 관점에서 기술이 기본권을 포함한 법률에 따라 안전하게 사용되고 있다는 확신을 주어야 한다. 백서의 발표에 이어, 유럽연합 집행위원회는 이해관계자들과 폭넓은 협의를 가졌다. 이는 AI 사용이 증가함에 따라 제기되는 과제와 우려를 해소하기 위한 규제 개입을 지지하는 다수의 이해관계자들로부터 큰 호응을 얻었다.

아울러 본 제안은 유럽 연합 수준에서 AI의 편익과 위험이 적절히 관리되는 인공 지능 시스템('AI 시스템')을 위한 역내 시장이 원활히 기능하도록 보장하기 위한 입법 조치의 필요성을 거듭 표명해 온 유럽 의회 및 유럽 이사회의 명시적 요청에 응답한다. 본 제안은 유럽 이사회가 명시한 안전하고 신뢰할 수 있으며 윤리적인 인공 지능의

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.

intelligence as stated by the European Council[3] and ensures the protection of ethical principles as specifically requested by the European Parliament[4].

In 2017, the European Council called for a 'sense of urgency to address emerging trends' including 'issues such as artificial intelligence …, while at the same time ensuring a high level of data protection, digital rights and ethical standards'[5]. In its 2019 Conclusions on the Coordinated Plan on the development and use of artificial intelligence Made in Europe[6], the Council further highlighted the importance of ensuring that European citizens' rights are fully respected and called for a review of the existing relevant legislation to make it fit for purpose for the new opportunities and challenges raised by AI. The European Council has also called for a clear determination of the AI applications that should be considered high-risk[7].

The most recent Conclusions from 21 October 2020 further called for addressing the opacity, complexity, bias, a certain degree of unpredictability and partially autonomous behaviour of certain AI systems, to ensure their compatibility with fundamental rights and to facilitate the enforcement of legal rules[8].

The European Parliament has also undertaken a considerable amount of work in the area of AI. In October 2020, it adopted a number of resolutions related to AI, including on ethics[9], liability[10] and copyright[11]. In 2021, those were followed by resolutions on AI in criminal matters[12] and in education, culture and the audio-visual sector[13]. The EP Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies specifically recommends to the Commission to propose legislative action to harness the opportunities and benefits of AI, but also to ensure protection of ethical principles. The resolution includes a text of the legislative proposal for a regulation on ethical principles for the development, deployment and use of AI, robotics and related technologies. In accordance with the political commitment made by President von der Leyen in her Political Guidelines as regards resolutions adopted by the European Parliament under Article 225 TFEU, this

---

3 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

4 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

5 European Council, *European Council meeting (19 October 2017) – Conclusion* EUCO 14/17, 2017, p. 8.

6 Council of the European Union, *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019.

7 European Council, *Special meeting of the European Council (1and 2 October 2020) – Conclusions* EUCO 13/20, 2020.

8 Council of the European Union, *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020.

9 European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

10 European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence, 2020/2014(INL).

11 European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).

12 European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI).

13 European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI). In that regard, the Commission has adopted the Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education – Commission Communication COM(2020) 624 final.

개발에서 글로벌 리더가 된다는 유럽 연합의 목표[3]를 지원하고, 유럽 의회가 명시적으로 요청한 윤리 원칙의 보호[4]를 보장한다.

2017년에 유럽 이사회는 '인공 지능 등의 문제를 포함한 새로운 동향을 긴급히 파악하고…, 그와 동시에 높은 수준의 데이터 보호, 디지털 권리 및 윤리적 표준을 보장할 것'을[5] 촉구했다. 유럽 이사회는 유럽에서 이루어진 인공 지능의 개발 및 사용에 대한 통합 계획(Coordinated Plan)에 관한 결론(2019 Conclusions)[6]에서 유럽 시민의 권리가 완전히 존중되도록 보장하는 일의 중요성을 다시 한 번 강조하고, 기존의 관련 법규를 재검토하여 AI에 의해 제기된 새로운 기회와 과제에 부합하도록 개정할 것을 요구했다. 아울러 유럽 이사회는 고위험으로 간주해야 할 AI 애플리케이션을 명확하게 결정할 것을 요구했다[7].

가장 최근인 2020년 10월 21자 Conclusions에서는 AI 시스템이 기본권과 양립할 수 있도록 보장하고 법규의 집행을 촉진하기 위해 특정 AI 시스템의 불투명성, 복잡성, 편향성, 예측 불가능성, 부분적 자율성 등을 관리할 것을 추가로 요구했다[8].

아울러 유럽 의회는 AI 분야에서 상당한 양의 작업을 수행했다. 2020년 10월에는 윤리[9], 책임[10], 저작권[11] 등 AI와 관련된 주제에 대해 다수의 결의안을 채택했다. 이어서 2021년에는 사법 문제와[12] 교육, 문화, 시청각 부문[13]에서 AI에 관한 결의안을 채택했다. 인공 지능, 로봇 공학 및 관련 기술의 윤리적 프레임워크에 관한 유럽 의회 결의(EP Resolution on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies)는 유럽연합 집행위원회에 대해 AI의 기회와 이점을 활용하고 윤리 원칙을 보호하기 위한 입법 조치를 제안할 것을 명시적으로 권고한다. 이 결의안은 AI, 로봇 공학 및 관련 기술의 개발, 배포, 사용을 위한 윤리 원칙에 관한 규정을 위한 입법 제안의 본문을 포함한다. TFEU 제225조를 근거로 유럽 의회가 채택한 결의안과 관련하여 폰 데어 라이엔 위원장이 자신의 정책 가이드라인에서 밝힌 정치적 공약에 따라, 본 제안은 비례성,

---

3 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

4 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

5 European Council, *European Council meeting (19 October 2017) – Conclusion* EUCO 14/17, 2017, p. 8.

6 Council of the European Union, *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019.

7 European Council, *Special meeting of the European Council (1and 2 October 2020) – Conclusions* EUCO 13/20, 2020.

8 Council of the European Union, *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020.

9 European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

10 European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence, 2020/2014(INL).

11 European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI).

12 European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI).

13 European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI). In that regard, the Commission has adopted the Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education – Commission Communication COM(2020) 624 final.

proposal takes into account the aforementioned resolution of the European Parliament in full respect of proportionality, subsidiarity and better law making principles.

Against this political context, the Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following **specific objectives**:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

To achieve those objectives, this proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market. The proposal sets a robust and flexible legal framework. On the one hand, it is comprehensive and future-proof in its fundamental regulatory choices, including the principle-based requirements that AI systems should comply with. On the other hand, it puts in place a proportionate regulatory system centred on a well-defined risk-based regulatory approach that does not create unnecessary restrictions to trade, whereby legal intervention is tailored to those concrete situations where there is a justified cause for concern or where such concern can reasonably be anticipated in the near future. At the same time, the legal framework includes flexible mechanisms that enable it to be dynamically adapted as the technology evolves and new concerning situations emerge.

The proposal sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach. It proposes a single future-proof definition of AI. Certain particularly harmful AI practices are prohibited as contravening Union values, while specific restrictions and safeguards are proposed in relation to certain uses of remote biometric identification systems for the purpose of law enforcement. The proposal lays down a solid risk methodology to define "high-risk" AI systems that pose significant risks to the health and safety or fundamental rights of persons. Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle. For some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used.

The proposed rules will be enforced through a governance system at Member States level, building on already existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board. Additional measures are also proposed to support innovation, in particular through AI regulatory sandboxes and other measures to reduce the regulatory burden and to support Small and Medium-Sized Enterprises ('SMEs') and start-ups.

보충성 및 선진 입법의 원칙을 최대한 존중하여 전술한 유럽 의회의 결의안을 고려한다.

이러한 정치적 맥락을 배경으로, 유럽연합 집행위원회는 다음과 같은 **구체적 목표**를 가지고 인공지능에 관한 규제 프레임워크를 제안한다.

- 유럽 연합 시장에서 사용되는 AI 시스템이 안전하게 관리되고 기본권과 유럽 연합의 가치에 관한 기존 법규를 존중하도록 보장한다.
- AI에 대한 투자와 혁신을 촉진하기 위한 법적 확실성을 보장한다.
- AI 시스템에 적용되는 기본권과 안전 요구사항에 관한 기존 법규의 관리와 효과적 집행을 강화한다.
- 합법적이고 안전하며 신뢰할 수 있는 AI 애플리케이션을 위한 단일 시장의 개발을 촉진하고 시장 파편화를 방지한다.

이러한 목표를 달성하기 위해, 본 제안은 기술 개발을 지나치게 억제 또는 방해하거나 AI 솔루션을 출시하는 비용을 불균형하게 증가시키지 않으면서 AI와 관련된 위험과 문제를 해결하기 위한 최소 필요 조건에 한정된, AI에 대한 균형 잡히고 비례적인 수평적 규제 방식을 제시한다. 본 제안은 견고하면서도 유연한 법적 프레임워크를 설정한다. 한편으로 이는 AI 시스템이 준수해야 할 원칙 중심 요구사항을 포함한 기본적 규제 선택의 측면에서 포괄적이고 미래 지향적(future-proof)이다. 다른 한편으로 이는 교역을 불필요하게 제한하지 않으면서 우려할 만한 정당한 이유가 있거나 그러한 우려가 가까운 미래에 합리적으로 예상될 수 있는 구체적 상황에 맞추어 법적 개입이 이루어지는, 잘 정의된 위험 기반 규제 방식에 중점을 둔 균형 잡힌 규제 시스템을 구축한다. 이와 동시에, 법적 프레임워크에는 기술이 진화하고 새로운 문제 상황이 발생함에 따라 동적으로 채택할 수 있는 유연한 메커니즘이 포함된다.

본 제안은 균형 잡힌 위험 기반 접근법에 따라 유럽 연합에서 AI 시스템을 개발, 출시, 사용하는 데 대한 조화 규칙을 제시한다. 아울러 AI에 대한 단일하고 미래 지향적(future-proof)인 정의를 제안한다. 특히 해로운 AI 관행은 유럽 연합의 가치에 위배되므로 금지되고, 법 집행 목적의 원격 생체 인식 시스템 사용과 관련하여 특정한 제한 및 보호 조치가 제안된다. 본 제안은 개인의 건강과 안전 또는 기본권에 중대한 위험을 초래하는 '고위험' AI 시스템을 정의하는 견고한 위험 방법론을 규정한다. 그러한 AI 시스템이 유럽 연합 시장에 진입하려면 먼저 신뢰할 수 있는 AI를 위한 일련의 수평적 필수 요건을 준수하고 적합성 평가 절차를 따라야 할 것이다. 또한, AI 시스템의 수명주기 전반에 걸쳐 안전을 보장하고 기본권을 보호하는 기존 법규를 존중하기 위해 예측 가능하고 비례적이며 명확한 의무가 시스템 제공자와 사용자들에게 부과된다. 특히 챗봇이나 '딥 페이크(Deep Fake)'를 사용하는 경우에는 특정 AI 시스템에 대해 최소한의 투명성 의무만이 부과된다.

제안된 규칙은 기존의 구조를 바탕으로 유럽 인공지능 위원회(European Artificial Intelligence Board)의 설립을 통한 유럽 연합 수준의 협력 메커니즘을 활용하여, 회원국 수준의 거버넌스 시스템을 통해 시행될 것이다. 이와 더불어, 특히 중소기업('SME')과 스타트업을 지원하고 규제 부담을 완화하기 위한 AI 규제 샌드박스 및 기타 수단을 통해 기술 혁신을 촉진하는 추가 조치가 제안된다.

1.2. Consistency with existing policy provisions in the policy area

The horizontal nature of the proposal requires full consistency with existing Union legislation applicable to sectors where high-risk AI systems are already used or likely to be used in the near future.

Consistency is also ensured with the EU Charter of Fundamental Rights and the existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality. The proposal is without prejudice and complements the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems. Furthermore, the proposal complements existing Union law on non-discrimination with specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle. The proposal is without prejudice to the application of Union competition law.

As regards high-risk AI systems which are safety components of products, this proposal will be integrated into the existing sectoral safety legislation to ensure consistency, avoid duplications and minimise additional burdens. In particular, as regards high-risk AI systems related to products covered by the New Legislative Framework (NLF) legislation (e.g. machinery, medical devices, toys), the requirements for AI systems set out in this proposal will be checked as part of the existing conformity assessment procedures under the relevant NLF legislation. With regard to the interplay of requirements, while the safety risks specific to AI systems are meant to be covered by the requirements of this proposal, NLF legislation aims at ensuring the overall safety of the final product and therefore may contain specific requirements regarding the safe integration of an AI system into the final product. The proposal for a Machinery Regulation, which is adopted on the same day as this proposal fully reflects this approach. As regards high-risk AI systems related to products covered by relevant Old Approach legislation (e.g. aviation, cars), this proposal would not directly apply. However, the ex-ante essential requirements for high-risk AI systems set out in this proposal will have to be taken into account when adopting relevant implementing or delegated legislation under those acts.

As regards AI systems provided or used by regulated credit institutions, the authorities responsible for the supervision of the Union's financial services legislation should be designated as competent authorities for supervising the requirements in this proposal to ensure a coherent enforcement of the obligations under this proposal and the Union's financial services legislation where AI systems are to some extent implicitly regulated in relation to the internal governance system of credit institutions. To further enhance consistency, the conformity assessment procedure and some of the providers' procedural obligations under this proposal are integrated into the procedures under Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision[14].

[14] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338–436.

1.2. 정책 분야에서 기존 정책 조항과의 일관성

본 제안의 수평적 성격은 고위험 AI 시스템이 이미 사용되고 있거나 가까운 미래에 사용될 가능성이 있는 부문에 적용되는 기존 유럽 연합 법규와의 완전한 일관성을 요구한다.

또한, EU 기본권 헌장과 데이터 보호, 소비자 보호, 차별 금지 및 성평등에 관한 기존의 유럽 연합 2차 입법을 통해서도 일관성이 보장된다. 본 제안은 유럽 일반 개인정보 보호법(Regulation (EU) 2016/679)과 법 집행 지침(Directive (EU) 2016/680)을 침해하지 않으며, 특정한 고위험 AI 시스템의 설계, 개발, 사용에 적용되는 일련의 조화 법령과 원격 생체 인식 시스템의 특정한 사용에 대한 제한으로 이를 보완한다. 나아가, 본 제안은 특히 AI 시스템의 개발에 사용되는 데이터세트의 설계 및 품질과 관련하여 알고리즘에 의한 차별의 위험을 최소화하는 것을 목표로 하는 특정 요구사항과 AI 시스템의 수명주기 전반에 걸친 테스트, 위험 관리, 기록 및 인간의 감독에 대한 의무를 통해 차별 금지에 관한 기존의 유럽 연합 법규를 보완한다. 본 제안은 유럽 연합 경쟁법의 적용을 침해하지 않는다.

제품의 안전 구성요소인 고위험 AI 시스템과 관련하여, 본 제안은 일관성을 보장하고, 중복을 피하고, 추가적 부담을 최소화하기 위해 기존의 부문별 안전 법규에 통합될 것이다. 특히, 새로운 입법 프레임워크(New Legislative Framework, NLF)가 적용되는 제품(예: 기계류, 의료 기기, 장난감)의 고위험 AI 시스템과 관련하여, 본 제안에 제시된 AI 시스템에 대한 요구사항은 관련 NLF에 따른 기존 적합성 평가 절차의 일부로 점검을 받을 것이다. 요구사항들의 상호작용과 관련하여, AI 시스템에 특유한 안전 위험에는 본 제안의 요구사항이 적용되지만 NLF는 최종 제품의 전반적 안전을 보장하는 것을 목표로 하며 따라서 AI 시스템을 최종 제품에 안전하게 통합하는 데 대한 요구사항을 포함할 수 있다. 본 제안과 같은 날 채택된 기계류 규정(Machinery Regulation)에 대한 제안은 이러한 접근방식을 충실히 반영한다. 전통적 접근방식(Old Approach) 법규가 적용되는 제품(예: 항공, 자동차)의 AI 시스템에 대해서는 본 제안이 직접 적용되지 않는다. 하지만 그러한 법규에 따른 관련 이행 또는 위임 입법을 채택할 때는 본 제안에 제시된 고위험 AI 시스템에 대한 사전(ex-ante) 필수 요구사항을 고려해야 할 것이다.

규제 대상인 신용 기관이 제공하거나 사용하는 AI 시스템과 관련하여, AI 시스템이 신용 기관의 내부 지배구조를 통해 어느 정도 암암리에 규제되는 경우 본 제안과 유럽 연합의 금융 서비스 법규에 따른 의무의 일관된 집행을 보장하기 위해 유럽 연합 금융 서비스 법규의 감독을 책임지는 기관을 본 제안의 요구사항을 감독하는 관할 기관으로 지명해야 한다. 일관성을 더욱 강화하기 위해, 적합성 평가 절차와 본 제안에 따른 제공자의 절차적 의무 중 일부가 신용 기관의 활동에 대한 접근과 건전성 감독에 관한 Directive 2013/36/EU[14]에 따른 절차에 통합된다.

[14] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 27.6.2013, p. 338–436.

This proposal is also consistent with the applicable Union legislation on services, including on intermediary services regulated by the e-Commerce Directive 2000/31/EC[15] and the Commission's recent proposal for the Digital Services Act (DSA)[16].

In relation to AI systems that are components of large-scale IT systems in the Area of Freedom, Security and Justice managed by the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), the proposal will not apply to those AI systems that have been placed on the market or put into service before one year has elapsed from the date of application of this Regulation, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

1.3. Consistency with other Union policies

The proposal is part of a wider comprehensive package of measures that address problems posed by the development and use of AI, as examined in the White Paper on AI. Consistency and complementarity is therefore ensured with other ongoing or planned initiatives of the Commission that also aim to address those problems, including the revision of sectoral product legislation (e.g. the Machinery Directive, the General Product Safety Directive) and initiatives that address liability issues related to new technologies, including AI systems. Those initiatives will build on and complement this proposal in order to bring legal clarity and foster the development of an ecosystem of trust in AI in Europe.

The proposal is also coherent with the Commission's overall digital strategy in its contribution to promoting technology that works for people, one of the three main pillars of the policy orientation and objectives announced in the Communication 'Shaping Europe's digital future'[17]. It lays down a coherent, effective and proportionate framework to ensure AI is developed in ways that respect people's rights and earn their trust, making Europe fit for the digital age and turning the next ten years into the **Digital Decade**[18].

Furthermore, the promotion of AI-driven innovation is closely linked to the **Data Governance Act**[19]**,** the **Open Data Directive**[20] and other initiatives under **the EU strategy for data**[21], which will establish trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality.

The proposal also strengthens significantly the Union's role to help shape global norms and standards and promote trustworthy AI that is consistent with Union values and interests. It provides the Union with a powerful basis to engage further with its external partners, including third countries, and at international fora on issues relating to AI.

---

15 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

16 See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

17 Communication from the Commission, Shaping Europe's Digital Future, COM/2020/67 final.

18 2030 Digital Compass: the European way for the Digital Decade.

19 Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

21 Commission Communication, A European strategy for data COM/2020/66 final.

본 제안은 또한 e-Commerce Directive 2000/31/EC[15]와 디지털 서비스법(Digital Services Act, DSA)에 대한 유럽연합 집행위원회의 최근 제안[16]에 의해 규제되는 중개업을 포함한 서비스에 대한 해당 유럽 연합 법규와 일치한다.

대규모 IT 시스템의 운영 관리를 위한 유럽 연합 기구(eu-LISA)가 관리하는 자유 안전 사법 지대(Area of Freedom, Security and Justice)에서 대규모 IT 시스템의 구성요소인 AI 시스템과 관련하여, 본 제안은 본 규정(Regulation)의 적용일로부터 1년이 경과하기 전에 시장에 출시되었거나 서비스를 개시한 AI 시스템에는 적용되지 않는다. 단, 해당 법규의 교체 또는 수정으로 인해 관련 AI 시스템의 설계 또는 원래 목적이 현저하게 변경된 경우는 예외로 한다.

1.3. 다른 유럽 연합 정책과의 일관성

본 제안은 인공 지능 백서에서 검토한 바와 같이 AI의 개발 및 사용으로 인해 제기되는 문제를 해결하기 위한 조치를 망라한 종합 패키지의 일부이다. 따라서 역시 그러한 문제를 해결하기 위해 유럽연합 집행위원회에서 진행 또는 계획 중인, 부문별 제품 법규(예: Machinery Directive, General Product Safety Directive)의 개정 및 AI 시스템을 포함한 신기술과 관련된 책임 문제를 다루는 이니셔티브를 포함한 다른 이니셔티브와의 일관성과 보완성이 보장된다. 이러한 이니셔티브는 법적 명확성을 제고하고 유럽에서 AI에 대한 신뢰 에코시스템의 개발을 촉진하기 위해 본 제안을 확충·보완한다.

본 제안은 또한 유럽연합 집행위원회가 커뮤니케이션(Communication) '유럽의 디지털 미래 구축(Shaping Europe's digital future)'[17]에서 발표한 3대 정책 방향 및 목표 가운데 하나인 사람을 위해 봉사하는 기술을 촉진한다는 점에서 유럽연합 집행위원회의 전반적 디지털 전략에 부합한다. 본 제안은 AI가 사람들의 권리를 존중하고 사람들의 신뢰를 얻는 방식으로 개발되어 유럽을 디지털 시대에 적합하게 변모시키고 향후 10년을 **디지털 10년(Digital Decade)**[18]으로 만들 수 게 해주는 일관성 있고 효과적이며 균형 잡힌 프레임워크를 규정한다.

나아가, AI 중심의 혁신을 촉진하는 일은 **데이터 거버넌스법(Data Governance Act)**[19], **오픈 데이터 지침(Open Data Directive)**[20], 및 **EU 데이터 전략(EU strategy for data)**[21]에 따른 기타 이니셔티브와 긴밀히 연관되어 있다. 이로써 품질 높은 데이터 중심 AI 모델의 개발에 필수적인 데이터의 재사용과 공유 및 풀링을 위한 신뢰성 있는 메커니즘과 서비스가 확립될 것이다.

아울러 본 제안은 글로벌 규범과 표준을 제정하고 유럽 연합의 가치와 이익에 부합하는 신뢰할 수 있는 AI를 촉진하는 유럽 연합의 역할을 크게 강화한다. 본 제안은 유럽 연합이 제3국을 포함한 외부 파트너들과 더욱 활발하게 교류하고 AI와 관련된 문제를 다루는 국제 포럼에 적극적으로 참여할 수 있는 강력한 토대를 제공한다.

---

15 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

16 참조: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final.

17 Communication from the Commission, Shaping Europe's Digital Future, COM/2020/67 final.

18 2030 Digital Compass: the European way for the Digital Decade.

19 Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

20 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

21 Commission Communication, A European strategy for data COM/2020/66 final.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

The legal basis for the proposal is in the first place Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures to ensure the establishment and functioning of the internal market.

This proposal constitutes a core part of the EU digital single market strategy. The primary objective of this proposal is to ensure the proper functioning of the internal market by setting harmonised rules in particular on the development, placing on the Union market and the use of products and services making use of AI technologies or provided as stand-alone AI systems. Some Member States are already considering national rules to ensure that AI is safe and is developed and used in compliance with fundamental rights obligations. This will likely lead to two main problems: i) a fragmentation of the internal market on essential elements regarding in particular the requirements for the AI products and services, their marketing, their use, the liability and the supervision by public authorities, and ii) the substantial diminishment of legal certainty for both providers and users of AI systems on how existing and new rules will apply to those systems in the Union. Given the wide circulation of products and services across borders, these two problems can be best solved through EU harmonizing legislation.

Indeed, the proposal defines common mandatory requirements applicable to the design and development of certain AI systems before they are placed on the market that will be further operationalised through harmonised technical standards. The proposal also addresses the situation after AI systems have been placed on the market by harmonising the way in which ex-post controls are conducted.

In addition, considering that this proposal contains certain specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU.

2.2. Subsidiarity (for non-exclusive competence)

The nature of AI, which often relies on large and varied datasets and which may be embedded in any product or service circulating freely within the internal market, entails that the objectives of this proposal cannot be effectively achieved by Member States alone. Furthermore, an emerging patchwork of potentially divergent national rules will hamper the seamless circulation of products and services related to AI systems across the EU and will be ineffective in ensuring the safety and protection of fundamental rights and Union values across the different Member States. National approaches in addressing the problems will only create additional legal uncertainty and barriers, and will slow market uptake of AI.

The objectives of this proposal can be better achieved at Union level to avoid a further fragmentation of the Single Market into potentially contradictory national frameworks preventing the free circulation of goods and services embedding AI. A solid European regulatory framework for trustworthy AI will also ensure a level playing field and protect all people, while strengthening Europe's competitiveness and industrial basis in AI. Only common action at Union level can also protect the Union's digital sovereignty and leverage its tools and regulatory powers to shape global rules and standards.

2. 법적 근거, 보충성 및 비례성

2.1. 법적 근거

본 제안의 법적 근거는 첫째로 역내 시장의 설립과 기능을 보장하는 조치의 채택을 규정한 유럽 연합의 기능에 관한 조약(TFEU) 제114조에 있다.

본 제안은 'EU 디지털 단일 시장 전략'의 핵심 부분을 구성한다. 본 제안의 주된 목표는 특히 AI 기술을 사용하거나 독립형 AI 시스템으로 제공되는 제품과 서비스의 개발, EU 시장 출시, 사용에 관한 조화 규칙을 제정함으로써 역내 시장의 올바른 기능을 보장하는 것이다. 일부 회원국은 이미 AI가 안전하고 기본권 의무를 준수하는 방식으로 개발·사용되도록 보장하는 국가 규칙을 고려하고 있다. 이는 두 가지 주요한 문제를 초래할 가능성이 있다: i) AI 제품 및 서비스의 마케팅, 사용, 그리고 공공 기관의 감독과 책임 등에 대한 요구사항과 관련한 핵심 요소들에 따라 역내 시장이 파편화하는 문제, ii) AI 시스템의 제공자와 사용자 모두에게, 유럽 연합에서 기존의 규칙과 새로운 규칙이 그러한 시스템에 어떻게 적용될 것인지에 대한 법적 확실성이 크게 낮아지는 문제가 그것이다. 제품과 서비스가 국경을 넘어 널리 유통되는 점을 감안할 때, 이 두 가지 문제는 EU의 조화 입법(harmonizing legislation)을 통해 가장 효과적으로 해결할 수 있다.

본 제안은 특정 AI 시스템이 출시되기 전 단계에서 설계와 개발에 적용되는 일반적 필수 요건을 정의한다. 이는 조화 기술 표준을 통해 추가로 정비된다. 본 제안은 또한 사후 관리가 이루어지는 방식을 조화함으로써 AI 시스템이 출시된 후의 상황에 대비한다.

이와 더불어, 본 제안에 개인 데이터의 처리와 관련된 개인의 보호에 관한 특정 규칙, 특히 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식을 위해 AI 시스템을 사용하는 데 대한 제한이 포함되는 점을 감안할 때, 그러한 특정 규칙이 관련되는 한 이 규정을 TFEU 제16조에 기초하는 것이 적절하다.

2.2. (비 독점적 권한을 위한) 보충성

흔히 규모가 크고 다양한 데이터세트에 의존하고 역내 시장에서 자유로이 유통되는 어떤 제품 또는 서비스에나 임베드될 수 있는 AI의 성격 때문에 회원국 단독으로는 본 제안의 목표를 효과적으로 달성할 수 없다. 뿐만 아니라, 제각각 일치하지 않는 새로운 국가 규칙들은 AI 시스템과 관련된 제품과 서비스가 EU 전역에서 매끄럽게 유통되는 데 방해가 되고 다양한 회원국 사이에서 기본권과 유럽 연합 가치를 보호하는 데 효과적이지 못할 것이다. 국가 단위의 문제 해결 방식은 단지 법적 불확실성과 장벽을 가중시키고 AI의 시장 진입을 늦출 것이다.

본 제안의 목표는 유럽 연합 수준에서 보다 효과적으로 달성할 수 있다. 단일 시장이 모순된 국가 프레임워크로 파편화되어 AI가 임베드된 상품과 서비스의 자유로운 유통을 막는 것을 방지해야 한다. 또한, 신뢰할 수 있는 AI를 위한 견고한 유럽 규제 프레임워크는 공평한 경쟁의 장을 보장하고 모든 사람을 보호하는 한편 유럽의 경쟁력과 AI의 산업 기반을 강화시켜 줄 것이다. 오로지 유럽 연합 수준의 공동 행동을 통해서만 유럽 연합의 디지털 주권을 보호하고, 그 도구와 규제 역량을 활용하여 글로벌 규칙 및 표준을 제정할 수 있다.

2.3. Proportionality

The proposal builds on existing legal frameworks and is proportionate and necessary to achieve its objectives, since it follows a risk-based approach and imposes regulatory burdens only when an AI system is likely to pose high risks to fundamental rights and safety. For other, non-high-risk AI systems, only very limited transparency obligations are imposed, for example in terms of the provision of information to flag the use of an AI system when interacting with humans. For high-risk AI systems, the requirements of high quality data, documentation and traceability, transparency, human oversight, accuracy and robustness, are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI and that are not covered by other existing legal frameworks. Harmonised standards and supporting guidance and compliance tools will assist providers and users in complying with the requirements laid down by the proposal and minimise their costs. The costs incurred by operators are proportionate to the objectives achieved and the economic and reputational benefits that operators can expect from this proposal.

2.4. Choice of the instrument

The choice of a regulation as a legal instrument is justified by the need for a uniform application of the new rules, such as definition of AI, the prohibition of certain harmful AI- enabled practices and the classification of certain AI systems. The direct applicability of a Regulation, in accordance with Article 288 TFEU, will reduce legal fragmentation and facilitate the development of a single market for lawful, safe and trustworthy AI systems. It will do so, in particular, by introducing a harmonised set of core requirements with regard to AI systems classified as high-risk and obligations for providers and users of those systems, improving the protection of fundamental rights and providing legal certainty for operators and consumers alike.

At the same time, the provisions of the regulation are not overly prescriptive and leave room for different levels of Member State action for elements that do not undermine the objectives of the initiative, in particular the internal organisation of the market surveillance system and the uptake of measures to foster innovation.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

3.1. Stakeholder consultation

This proposal is the result of extensive consultation with all major stakeholders, in which the general principles and minimum standards for consultation of interested parties by the Commission were applied.

An **online public consultation** was launched on 19 February 2020 along with the publication of the White Paper on Artificial Intelligence and ran until 14 June 2020. The objective of that consultation was to collect views and opinions on the White Paper. It targeted all interested stakeholders from the public and private sectors, including governments, local authorities, commercial and non-commercial organisations, social partners, experts, academics and citizens. After analysing all the responses received, the Commission published a summary outcome and the individual responses on its website[22].

In total, 1215 contributions were received, of which 352 were from companies or business organisations/associations, 406 from individuals (92%individuals from EU), 152 on behalf of

[22] See all consultation results here.

2.3. 비례성

본 제안은 기존의 법적 프레임워크에 기반을 두고 위험 기반 접근법을 따르며 AI 시스템이 기본권과 안전에 높은 위험을 초래할 가능성이 있는 경우에만 규제 부담을 부과하므로 목표 달성에 비례적·필수적이다. 기타 비 고위험 AI 시스템의 경우, 이를테면 인간과 상호 작용할 때 AI 시스템의 사용을 플래깅하기 위한 정보의 제공이라는 맥락에서 매우 제한적인 투명성 의무가 부과된다. 고위험 AI 시스템의 경우, 고품질 데이터, 기록 및 추적 가능성, 투명성, 인간의 감독, 정확성, 견고성 등의 요구사항은 AI에 의해 제기되고 기존의 다른 법적 프레임워크에 적용되지 않는 기본권과 안전에 대한 위험을 완화하는 데 꼭 필요하다. 조화 표준과 이를 뒷받침하는 지침 및 준수 도구는 제공자와 사용자가 본 제안에 제시된 요구사항을 준수하는 데 도움을 주고 그에 따른 비용을 최소화시켜 줄 것이다. 운영자가 부담하는 비용은 달성한 목표와 운영자가 본 제안에서 기대할 수 있는 경제적 이익과 평판의 혜택에 비례한다.

2.4. 수단의 선택

법적 수단으로서 규정의 선택은 AI의 정의, 유해한 AI 사용 관행의 금지, 특정 AI 시스템의 분류와 같은 새로운 규칙을 일률적으로 적용해야 할 필요성에 의해 정당화된다. TFEU 제288조에 따라 규정(Regulation)을 직접 적용할 수 있다면 법적 파편화를 완화하고 적법하고 안전하며 신뢰할 수 있는 AI 시스템을 위한 단일 시장의 개발을 촉진할 수 있을 것이다. 이는 특히, 고위험으로 분류되는 AI 시스템과 관련된 핵심 요구사항과 그러한 시스템의 제공자 및 사용자에게 부과되는 일련의 조화 의무를 도입하여 기본권의 보호를 개선하고 운영자와 소비자 모두를 위해 법적 확실성을 제공함으로써 실현될 수 있다.

이와 동시에, 규정의 조항들은 지나치게 권위적이지 않으며, 특히 시장 감시 시스템의 내부 조직과 혁신을 촉진하기 위한 조치의 채택 등 이니셔티브의 목표를 저해하지 않는 요소들에 대해 회원국들이 다양한 수준의 조치를 취할 수 있는 여지를 남긴다.

3. 사후 평가, 이해관계자 협의 및 영향 평가의 결과

3.1. 이해관계자 협의

본 제안은 유럽연합 집행위원회와 모든 주요 이해관계자 간의 방대한 협의에 따른 결과물이며, 이 과정에서 이해관계자들과의 협의를 위한 일반 원칙과 최소 기준이 적용되었다.

2020년 2월 19일에 인공 지능 백서의 발표와 더불어 **온라인 공개 협의**가 시작되고 2020년 6월 14일까지 계속되었다. 이 협의의 목적은 백서에 대한 의견을 수렴하는 것이었다. 협의는 정부, 지방 당국, 영리/비영리 단체, 사회적 파트너, 전문가, 학계, 시민 등을 망라한 공공/민간 부문의 모든 이해관계자를 대상으로 이루어졌다. 위원회는 수집한 모든 응답을 분석한 후 요약 결과와 개별 응답을 자체 웹사이트에 발표했다[22].

총 1,215건의 응답이 접수되었으며, 이 가운데 352건은 기업 또는 사업자 단체/협회, 406건은 개인(92%는 EU 시민), 152건은 학술/연구 기관, 73건은 공공 단체로부터 수집한 것이다. 시민 사회의 목소리는

22 여기서 모든 협의 결과 보기.

academic/research institutions, and 73 from public authorities. Civil society's voices were represented by 160 respondents (among which 9 consumers' organisations, 129 non-governmental organisations and 22 trade unions), 72 respondents contributed as 'others'. Of the 352 business and industry representatives, 222 were companies and business representatives, 41.5% of which were micro, small and medium-sized enterprises. The rest were business associations. Overall, 84% of business and industry replies came from the EU-27. Depending on the question, between 81 and 598 of the respondents used the free text option to insert comments. Over 450 position papers were submitted through the EU Survey website, either in addition to questionnaire answers (over 400) or as stand-alone contributions (over 50).

Overall, there is a general agreement amongst stakeholders on a need for action. A large majority of stakeholders agree that legislative gaps exist or that new legislation is needed. However, several stakeholders warn the Commission to avoid duplication, conflicting obligations and overregulation. There were many comments underlining the importance of a technology neutral and proportionate regulatory framework.

Stakeholders mostly requested a narrow, clear and precise definition for AI. Stakeholders also highlighted that besides the clarification of the term of AI, it is important to define 'risk', 'high-risk', 'low-risk', 'remote biometric identification' and 'harm'.

Most of the respondents are explicitly in favour of the risk-based approach. Using a risk-based framework was considered a better option than blanket regulation of all AI systems. The types of risks and threats should be based on a sector-by-sector and case-by-case approach. Risks also should be calculated taking into account the impact on rights and safety.

Regulatory sandboxes could be very useful for the promotion of AI and are welcomed by certain stakeholders, especially the Business Associations.

Among those who formulated their opinion on the enforcement models, more than 50%, especially from the business associations, were in favour of a combination of an ex-ante risk self-assessment and an ex-post enforcement for high-risk AI systems.

3.2. Collection and use of expertise

The proposal builds on two years of analysis and close involvement of stakeholders, including academics, businesses, social partners, non-governmental organisations, Member States and citizens. The preparatory work started in 2018 with the setting up of a **High-Level Expert Group on AI (HLEG)** which had an inclusive and broad composition of 52 well-known experts tasked to advise the Commission on the implementation of the Commission's Strategy on Artificial Intelligence. In April 2019, the Commission supported[23] the key requirements set out in the HLEG ethics guidelines for Trustworthy AI[24], which had been revised to take into account more than 500 submissions from stakeholders. The key requirements reflect a widespread and common approach, as evidenced by a plethora of ethical codes and principles developed by many private and public organisations in Europe and beyond, that AI development and use should be guided by certain essential value-oriented principles. The Assessment List for Trustworthy Artificial Intelligence (ALTAI)[25] made those requirements operational in a piloting process with over 350 organisations.

[23] European Commission, *Building Trust in Human-Centric Artificial Intelligence*, COM(2019) 168.
[24] HLEG, *Ethics Guidelines for Trustworthy AI*, 2019.
[25] HLEG, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020.

160명의 응답자에 의해 대변되었으며(이 가운데 9건은 소비자 단체, 129건은 비정부 조직, 22건은 노동조합), 72명의 응답자가 '기타'로 참여했다. 352건의 비즈니스 및 산업 대표자들 가운데 222건은 기업 및 비즈니스 대표자였으며, 이 중 41.5%는 소상공인과 중소기업, 나머지는 사업자 협회였다. 전체적으로 비즈니스 및 산업 대표자 응답의 84%가 EU 27개국에서 수집되었다. 질문에 따라 81~598명의 응답자가 자유 텍스트(free text) 옵션을 사용하여 의견을 기입했다. 450건이 넘는 성명서(position paper)가 설문 응답에 추가하거나(400건 이상) 별도의 기고문 형태로(50건 이상) EU Survey 웹사이트를 통해 제출되었다.

전반적으로 볼 때, 이해관계자들 간 행동의 필요성에 대한 일반적 합의가 이루어지고 있다. 대다수의 이해관계자가 입법 격차가 존재하거나 새로운 입법이 필요하다는 데 동의한다. 하지만 몇몇 이해관계자는 유럽연합 집행위원회에 대해 중복과 의무 상충, 과잉 규제를 방지할 것을 경고한다. 또한 기술 중립적이고 균형 잡힌 규제 프레임워크의 중요성을 강조하는 의견이 많았다.

이해관계자들은 대부분 AI에 대해 좁고 명확하고 정확한 정의를 요구했다. 이들은 또한 AI라는 용어를 명확하게 설명하는 것과 더불어, '위험(risk)', '고위험(high-risk)', '저위험(low-risk)', '원격 생체 인식(remote biometric identification)', '피해(harm)' 등의 개념을 정의하는 것이 중요하다고 강조했다.

대부분의 응답자는 위험 기반 접근법을 명확히 지지했다. 모든 AI 시스템을 일괄적으로 규제하는 것보다 위험 기반 프레임워크를 사용하는 것이 더 나은 옵션으로 간주되었다. 위험과 위협의 유형은 부문별, 사례별 접근법을 근거로 분류해야 한다. 또한, 위험은 권리와 안전에 미치는 영향을 고려해야 계산해야 한다.

규제 샌드박스는 AI의 촉진에 매우 유용할 수 있으며 특정 이해관계자, 특히 사업자 협회의 환영을 받았다.

집행 모델에 대한 의견을 개진한 응답자 가운데 50% 이상(특히 사업자 협회에서)이 고위험 AI 시스템에 대한 사전 위험 자체 평가와 사후 집행의 조합을 지지했다.

3.2. 전문 지식의 수집 및 사용

본 제안은 2년간의 분석과 학계, 기업, 소셜 파트너, 비정부 단체, 회원국, 시민 등 이해관계자들의 긴밀한 참여를 바탕으로 이루어졌다. 2018년, 유럽연합 집행위원회의 인공 지능 전략 시행에 대해 자문하는 52인의 유명 전문가들로 폭넓게 구성된 **AI에 관한 고위급 전문가 그룹(High-Level Expert Group, HLEG)**을 설립하여 준비 작업에 착수했다. 2019년 4월, 위원회는 이해관계자들이 제출한 500건 이상의 의견을 고려하여 개정된 신뢰할 수 있는 AI를 위한 HLEG 윤리 가이드라인[24]에 명시된 핵심 요구사항을 지지했다[23]. 이러한 요구사항은 유럽과 기타 지역에서 여러 민간/공공 단체들이 개발한 수많은 윤리 규범 및 원칙들을 통해 확인된바, AI의 개발과 사용은 확고한 가치 지향적 원칙에 의해 지도되어야 한다는 광범위하고 일반적인 접근법을 반영한다. 신뢰할 수 있는 인공지능을 위한 평가 리스트(Assessment List for Trustworthy Artificial Intelligence, ALTAI)[25]는 350개 이상의 조직이 참여한 파일럿 프로세스에서 이러한 요구사항을 적용할 수 있도록 해주었다.

---

23 European Commission, *Building Trust in Human-Centric Artificial Intelligence*, COM(2019) 168.
24 HLEG, *Ethics Guidelines for Trustworthy AI*, 2019.
25 HLEG, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020.

In addition, the **AI Alliance**[26] was formed as a platform for approximately 4000 stakeholders to debate the technological and societal implications of AI, culminating in a yearly AI Assembly.

The **White Paper** on AI further developed this inclusive approach, inciting comments from more than 1250 stakeholders, including over 450 additional position papers. As a result, the Commission published an Inception Impact Assessment, which in turn attracted more than 130 comments[27]. **Additional stakeholder workshops and events** were also organised the results of which support the analysis in the impact assessment and the policy choices made in this proposal[28]. An **external study** was also procured to feed into the impact assessment.

3.3. Impact assessment

In line with its "Better Regulation" policy, the Commission conducted an impact assessment for this proposal examined by the Commission's Regulatory Scrutiny Board. A meeting with the Regulatory Scrutiny Board was held on 16 December 2020, which was followed by a negative opinion. After substantial revision of the impact assessment to address the comments and a resubmission of the impact assessment, the Regulatory Scrutiny Board issued a positive opinion on 21 March 2021. The opinions of the Regulatory Scrutiny Board, the recommendations and an explanation of how they have been taken into account are presented in Annex 1 of the impact assessment.

The Commission examined different policy options to achieve the general objective of the proposal, which is to **ensure the proper functioning of the single market** by creating the conditions for the development and use of trustworthy AI in the Union.

Four policy options of different degrees of regulatory intervention were assessed:

- **Option 1**: EU legislative instrument setting up a voluntary labelling scheme;
- **Option 2**: a sectoral, "ad-hoc" approach;
- **Option 3**: Horizontal EU legislative instrument following a proportionate risk-based approach;
- **Option 3+**: Horizontal EU legislative instrument following a proportionate risk-based approach + codes of conduct for non-high-risk AI systems;
- **Option 4**: Horizontal EU legislative instrument establishing mandatory requirements for all AI systems, irrespective of the risk they pose.

According to the Commission's established methodology, each policy option was evaluated against economic and societal impacts, with a particular focus on impacts on fundamental rights. The preferred option is option 3+, a regulatory framework for high-risk AI systems only, with the possibility for all providers of non-high-risk AI systems to follow a code of conduct. The requirements will concern data, documentation and traceability, provision of information and transparency, human oversight and robustness and accuracy and would be mandatory for high-risk AI systems. Companies that introduced codes of conduct for other AI systems would do so voluntarily.

---

[26] The AI Alliance is a multi-stakeholder forum launched in June 2018, AI Alliance https://ec.europa.eu/digital-single-market/en/european-ai-alliance

[27] European Commission, *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.*

[28] For details of all the consultations that have been carried out see Annex 2 of the impact assessment

이와 더불어, 약 4000명의 이해관계자가 AI의 기술적·사회적 함의에 대해 토론하는 플랫폼 역할을 하는 **AI Alliance**[26]를 결성하고, 해마다 AI Assembly를 열기로 했다.

인공 지능 백서는 이 포괄적 접근법을 더욱 발전시켜, 1,250명 이상의 이해관계자들로부터 의견을 수렴했다(450건이 넘는 추가 성명서 포함). 그 결과, 유럽연합 집행위원회는 다시 130건 이상의 의견을 수렴한 초기 영향 평가(Inception Impact Assessment)를 발표했다[27]. 아울러, 본 제안에서 이루어진 영향 평가의 분석과 정책 선택을 뒷받침하기 위한 **추가적 이해관계자 워크숍 및 이벤트**가 조직되었다[28]. 이와 함께 영향 평가에 반영할 **외부 연구**를 의뢰했다.

3.3. 영향 평가

유럽연합 집행위원회는 "더 나은 규제(Better Regulation)" 정책에 따라 규제 검토 위원회(Regulatory Scrutiny Board)를 중심으로 본 제안에 대한 영향 평가를 수행했다. 2020년 12월 16일 규제 조사 위원회의 회의가 열리고, 이어서 부정적 의견이 개진되었다. 규제 검토 위원회는 의견을 수렴하여 영향 평가를 대폭 수정해서 다시 제출한 후 2021년 3월 21일에 긍정적 의견을 발표했다. 규제 검토 위원회의 의견과 권고사항, 그리고 이들이 어떻게 반영되었는지에 대한 설명이 영향 평가의 부속서 1에 제시되어 있다.

유럽연합 집행위원회는 유럽 연합에서 신뢰할 수 있는 AI의 개발과 사용을 위한 조건을 창출하여 **단일 시장의 올바른 기능을 보장한다**는 본 제안의 일반적 목표를 달성하기 위한 다양한 정책 옵션을 검토했다.

서로 다른 수준의 규제 개입을 수반하는 4개 정책 옵션이 평가되었다.

- **옵션 1**: 자발적 레이블링 체계를 정립하는 EU 법규
- **옵션 2**: 부문별 "임의적(ad-hoc)" 접근법
- **옵션 3**: 균형 잡힌 위험 기반 접근법에 따른 수평적 EU 법규
- **옵션 3+**: 균형 잡힌 위험 기반 접근법에 따른 수평적 EU 법규 + 비 고위험 AI 시스템을 위한 행동 지침
- **옵션 4**: 수반되는 위험과 관계없이 모든 AI 시스템에 대한 필수 요건을 규정하는 수평적 EU 법규.

유럽연합 집행위원회의 검증된 방법론에 따라, 기본권에 미치는 영향에 특히 초점을 맞추어 경제적·사회적 영향을 기준으로 각 정책 옵션을 평가했다. 우선적으로 고려되는 옵션은 옵션 3+이다. 이는 고위험 AI 시스템에만 적용되는 규제 프레임워크이지만, 모든 비 고위험 AI 시스템 제공자들이 행동 지침을 따를 가능성이 있다. 요구사항은 데이터, 기록 및 추적 가능성, 정보 제공, 투명성, 인간의 감독, 견고성, 정확성 등에 관한 것이며 고위험 AI 시스템의 필수 요건이 될 것이다. 다른 AI 시스템에 대한 행동 지침을 도입한 기업들은 이를 자발적으로 이행할 할 것이다.

---

[26] AI Alliance는 2018년 6월에 출범한 다중 이해관계자 포럼이다. https://ec.europa.eu/digital-single-market/en/european-ai-alliance

[27] European Commission, *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence.*

[28] 수행된 모든 협의의 세부 사항은 영향 평가의 부속서 2 참조.

The preferred option was considered suitable to address in the most effective way the objectives of this proposal. By requiring a restricted yet effective set of actions from AI developers and users, the preferred option limits the risks of violation of fundamental rights and safety of people and foster effective supervision and enforcement, by targeting the requirements only to systems where there is a high risk that such violations could occur. As a result, that option keeps compliance costs to a minimum, thus avoiding an unnecessary slowing of uptake due to higher prices and compliance costs. In order to address possible disadvantages for SMEs, this option includes several provisions to support their compliance and reduce their costs, including creation of regulatory sandboxes and obligation to consider SMEs interests when setting fees related to conformity assessment.

The preferred option will increase people's trust in AI, companies will gain in legal certainty, and Member States will see no reason to take unilateral action that could fragment the single market. As a result of higher demand due to higher trust, more available offers due to legal certainty, and the absence of obstacles to cross-border movement of AI systems, the single market for AI will likely flourish. The European Union will continue to develop a fast- growing AI ecosystem of innovative services and products embedding AI technology or stand-alone AI systems, resulting in increased digital autonomy.

Businesses or public authorities that develop or use AI applications that constitute a high risk for the safety or fundamental rights of citizens would have to comply with specific requirements and obligations. Compliance with these requirements would imply costs amounting to approximately EUR € 6000 to EUR € 7000 for the supply of an average high- risk AI system of around EUR € 170000 by 2025. For AI users, there would also be the annual cost for the time spent on ensuring human oversight where this is appropriate, depending on the use case. Those have been estimated at approximately EUR € 5000 to EUR € 8000 per year. Verification costs could amount to another EUR € 3000 to EUR € 7500 for suppliers of high-risk AI. Businesses or public authorities that develop or use any AI applications not classified as high risk would only have minimal obligations of information. However, they could choose to join others and together adopt a code of conduct to follow suitable requirements, and to ensure that their AI systems are trustworthy. In such a case, costs would be at most as high as for high-risk AI systems, but most probably lower.

The impacts of the policy options on different categories of stakeholders (economic operators/ business; conformity assessment bodies, standardisation bodies and other public bodies; individuals/citizens; researchers) are explained in detail in Annex 3 of the Impact assessment supporting this proposal.

3.4. Regulatory fitness and simplification

This proposal lays down obligation that will apply to providers and users of high-risk AI systems. For providers who develop and place such systems on the Union market, it will create legal certainty and ensure that no obstacle to the cross-border provision of AI-related services and products emerge. For companies using AI, it will promote trust among their customers. For national public administrations, it will promote public trust in the use of AI and strengthen enforcement mechanisms (by introducing a European coordination mechanism, providing for appropriate capacities, and facilitating audits of the AI systems with new requirements for documentation, traceability and transparency). Moreover, the framework will envisage specific measures supporting innovation, including regulatory sandboxes and specific measures supporting small-scale users and providers of high-risk AI systems to comply with the new rules.

The proposal also specifically aims at strengthening Europe's competitiveness and industrial basis in AI. Full consistency is ensured with existing sectoral Union legislation applicable to

우선 옵션은 본 제안의 목표를 가장 효과적으로 달성하는 데 적합한 것으로 간주되었다. 우선 옵션은 AI 개발자와 사용자에 대해 제한적이면서도 효과적인 일련의 행동을 요구함으로써 사람들의 기본권과 안전을 침해할 위험을 억제하고 그러한 침해가 발생할 위험이 큰 시스템에만 요구사항을 적용함으로써 효과적인 감독과 집행을 촉진한다. 그 결과, 이 옵션은 준수 비용을 최소한으로 유지하여 높은 비용으로 인해 시행이 불필요하게 지체되는 것을 방지한다. 이 옵션은 중소기업이 겪을 수 있는 불이익을 해소하기 위해, 적합성 평가와 관련된 수수료를 설정할 때 중소기업의 이해를 고려하는 의무와 규제 샌드박스의 도입을 포함하여 규정 준수를 지원하고 비용을 경감하는 몇 가지 조항을 포함한다.

우선 옵션은 AI에 대한 사람들의 신뢰를 제고하고, 기업들은 법적 확실성을 획득할 것이며, 회원국들은 단일 시장을 파편화시킬 수 있는 일방적 조치를 취할 이유를 찾지 못할 것이다. 신뢰 제고로 인해 높아진 수요, 법적 확실성으로 인해 더 저렴해진 오퍼, AI 시스템의 국가간 이동을 방해하는 장애물 제거 등에 따른 결과로 AI를 위한 단일 시장이 번성할 가능성이 높다. 유럽 연합은 AI 기술이 임베드된 혁신적 제품/서비스 또는 독립형 AI 시스템으로 이루어진 빠르게 성장하는 AI 에코시스템을 계속 개발할 것이다.

시민의 안전 또는 기본권에 대한 고위험을 구성하는 AI 애플리케이션을 개발하거나 사용하는 기업 또는 공공 기관은 특정한 요구사항과 의무를 준수해야 할 것이다. 이러한 요구사항을 준수하는 기업은 2025년까지 약 EUR € 170000에 달하는 평균 고위험 AI 시스템의 공급에 대해 약 EUR € 6000 ~ EUR € 7000에 이르는 비용을 초래할 것이다. AI 사용자의 경우에도 사용 사례에 따라 적절한 경우 인간의 감독을 보장하는 데 소요되는 시간과 비용이 초래될 것이다. 이는 연간 약 EUR € 5000 ~ EUR € 8000로 추산되었다. 고위험 AI의 공급자에 대한 추가적 검증 비용은 EUR € 3000 ~ EUR € 7500에 이를 수 있다. 고위험으로 분류되지 않은 AI 애플리케이션을 개발하거나 사용하는 기업 또는 공공 기관은 단지 최소한의 정보 의무만 지게 될 것이다. 하지만, 이들은 타기업/기관과 공동으로 적절한 요구사항에 따르는 행동 지침을 채택하고 각자의 AI 시스템에 대한 신뢰성을 보장해야 할 수 있다. 그러한 경우, 비용은 많아 봐야 고위험 AI 시스템과 비슷하고 대부분은 낮을 것이다.

정책 옵션이 다양한 범주의 이해관계자(경제 운영자/기업, 적합성 평가 기관, 표준화 기구 및 기타 공공 단체, 개인/시민, 연구자 등)에 미치는 영향에 대해서는 본 제안을 뒷받침하는 영향 평가의 부속서 3에서 상세히 설명한다.

3.4. 규제 적합성 및 간소화

본 제안은 고위험 AI 시스템의 제공자와 사용자에게 적용되는 의무를 규정한다. 본 제안은 그러한 시스템을 개발하여 유럽 연합 시장에 출시하는 제공자를 위해 법적 확실성을 확보하고 AI 관련 제품/서비스의 국가간 유통에 어떠한 장애물도 발생하지 않을 것을 보장한다. AI를 사용하는 기업을 위해서는 고객들 사이에 신뢰를 증진할 것이다. 국가 행정을 위해서는 AI의 사용에 대한 공중의 신뢰를 증진하고 (새로운 기록, 추적 가능성, 투명성 요구사항을 통해 AI 시스템의 적절한 기능을 규정하고 감사를 촉진하는 유럽 조정 체계를 도입함으로써) 집행 체계를 강화할 것이다. 나아가 이 프레임워크는 고위험 AI 시스템의 소규모 사용자 및 제공자들이 새로운 규칙을 준수할 수 있도록 지원하는 특정 조치와 규제 샌드박스를 포함하여, 혁신을 뒷받침하는 특정 조치들을 모색할 것이다.

본 제안은 특히 유럽의 경쟁력과 AI의 산업 기반을 강화하는 것을 목표로 한다. 새로운 규칙의 명확성을 높이고 집행을 간소화하는, (예컨대 제품과 서비스의) AI 시스템에

AI systems (e.g. on products and services) that will bring further clarity and simplify the enforcement of the new rules.

3.5. Fundamental rights

The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter'). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach. With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Article 1), respect for private life and protection of personal data (Articles 7 and 8), non- discrimination (Article 21) and equality between women and men (Article 23). It aims to prevent a chilling effect on the rights to freedom of expression (Article 11) and freedom of assembly (Article 12), to ensure protection of the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Articles 47 and 48), as well as the general principle of good administration. Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Article 31), a high level of consumer protection (Article 28), the rights of the child (Article 24) and the integration of persons with disabilities (Article 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Article 37) is also relevant, including in relation to the health and safety of people. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimising the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary. In case infringements of fundamental rights still happen, effective redress for affected persons will be made possible by ensuring transparency and traceability of the AI systems coupled with strong ex post controls.

This proposal imposes some restrictions on the freedom to conduct business (Article 16) and the freedom of art and science (Article 13) to ensure compliance with overriding reasons of public interest such as health, safety, consumer protection and the protection of other fundamental rights ('responsible innovation') when high-risk AI technology is developed and used. Those restrictions are proportionate and limited to the minimum necessary to prevent and mitigate serious safety risks and likely infringements of fundamental rights.

The increased transparency obligations will also not disproportionately affect the right to protection of intellectual property (Article 17(2)), since they will be limited only to the minimum necessary information for individuals to exercise their right to an effective remedy and to the necessary transparency towards supervision and enforcement authorities, in line with their mandates. Any disclosure of information will be carried out in compliance with relevant legislation in the field, including Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. When public authorities and notified bodies need to be given access to confidential information or source code to examine compliance with substantial obligations, they are placed under binding confidentiality obligations.

4. BUDGETARY IMPLICATIONS

Member States will have to designate supervisory authorities in charge of implementing the legislative requirements. Their supervisory function could build on existing arrangements, for

적용되는 기존의 부문별 유럽 연합 법규와의 일관성이 완벽하게 보장된다.

3.5. 기본권

AI의 여러 가지 특성(불투명성, 복잡성, 데이터에 의존성, 자율적 작동 등)은 EU 기본권 헌장("헌장")에 명시된 기본권에 악영향을 미칠 수 있다. 본 제안은 이러한 기본권을 높은 수준으로 보호하고 명확히 정의된 위험 기반 접근법을 통해 위험의 다양한 근원을 파악하고자 한다. 본 제안은 신뢰할 수 있는 AI를 위한 일련의 요구사항과 가치 사슬의 모든 참여자에게 부과되는 균형 잡힌 의무를 통해 헌장이 보장하는 다음과 같은 권리의 보호를 강화·촉진할 것이다: 인간의 존엄성에 대한 권리(제1조), 사생활 존중 및 개인 데이터 보호(제7 및 8조), 차별 금지(제21조), 남녀 평등(제23조). 본 제안은 표현의 자유(제11조) 및 집회의 자유(제12조)에 대한 위축 효과를 방지하고, 효과적인 구제 수단 및 공정한 재판에 대한 권리, 무죄 추정의 원칙과 방어권(제47 및 48조), 및 좋은 행정의 일반 원칙을 보호하고자 한다. 나아가, 특정 영역에 적용되는 본 제안은 공평하고 공정한 노동 조건에 대한 노동자의 권리(제31조), 높은 수준의 소비자 보호(제28조), 아동의 권리(제24조), 장애인의 일관성(제26조) 등 여러 특수 집단의 권리에 긍정적 영향을 미칠 것이다. 높은 수준의 환경 보호와 환경 품질의 개선에 대한 권리(제37조) 역시 중요하며, 여기에는 사람의 건강 및 안전과 관련된 권리 포함한다. 사전 검사, 위험 관리 및 인간의 감독에 대한 의무는 또한 교육 및 훈련, 고용, 중요한 서비스, 법 집행 및 사법 등의 핵심 영역에서 AI를 활용한 잘못되거나 편향된 의사결정의 위험을 최소화함으로써 다른 기본권의 존중을 촉진할 것이다. 기본권 침해가 여전히 발생하는 경우, 강력한 사후 관리와 더불어 AI 시스템의 투명성과 추적 가능성을 보장함으로써 피해자의 효과적인 구제가 가능하게 될 것이다.

본 제안은 고위험 AI 기술을 개발하고 사용할 때 건강, 안전, 소비자 보호 및 기타 기본권의 보호 등 공익의 최우선 가치를 준수하기 위해('책임 있는 혁신') 기업의 자유(제16조) 및 학문과 예술의 자유(제13조)에 일부 제한을 둔다. 이러한 제한은 비례적이며 중대한 안전 위험과 기본권의 침해를 예방·완화하는 데 필요한 최소한도로 제한된다.

투명성 강화 의무는 개인이 효과적인 구제의 권리를 행사하는 데 필요한 최소한의 정보와 감독 및 집행 기관에 대해 그들의 권한에 따라 요구되는 투명성으로만 제한될 것이므로 지적 재산 보호권(제17(2)조)에 불균형한 영향을 주지 않을 것이다. 모든 정보 공개는 비공개 노하우 및 비즈니스 정보(영업 비밀)를 불법 취득, 사용 및 공개로부터 보호하는 데 관한 Directive 2016/943을 포함한 관련 분야의 법규를 준수하여 수행될 것이다. 공공 기관과 인증 기관(notified body)이 중요한 의무의 준수 여부를 조사하기 위해 기밀 정보 또는 소스 코드에 접근할 필요가 있는 경우에는 이들에게 구속력 있는 비밀 유지 의무가 부과된다.

4. 재정적 함의

회원국은 법적 요구사항을 시행할 감독 기관을 지명해야 한다. 이들의 감독 기능은 예컨대 적합성 평가 기관 또는 시장 감시와 관련된 기존의 제도를 활용할 수 있으나, 충분한 전문기술과 인적

example regarding conformity assessment bodies or market surveillance, but would require sufficient technological expertise and human and financial resources. Depending on the pre-existing structure in each Member State, this could amount to 1 to 25 Full Time Equivalents per Member State.

A detailed overview of the costs involved is provided in the 'financial statement' linked to this proposal.

5. OTHER ELEMENTS

5.1. Implementation plans and monitoring, evaluation and reporting arrangements

Providing for a robust monitoring and evaluation mechanism is crucial to ensure that the proposal will be effective in achieving its specific objectives. The Commission will be in charge of monitoring the effects of the proposal. It will establish a system for registering stand-alone high-risk AI applications in a public EU-wide database. This registration will also enable competent authorities, users and other interested people to verify if the high-risk AI system complies with the requirements laid down in the proposal and to exercise enhanced oversight over those AI systems posing high risks to fundamental rights. To feed this database, AI providers will be obliged to provide meaningful information about their systems and the conformity assessment carried out on those systems.

Moreover, AI providers will be obliged to inform national competent authorities about serious incidents or malfunctioning that constitute a breach of fundamental rights obligations as soon as they become aware of them, as well as any recalls or withdrawals of AI systems from the market. National competent authorities will then investigate the incidents/or malfunctioning, collect all the necessary information and regularly transmit it to the Commission with adequate metadata. The Commission will complement this information on the incidents by a comprehensive analysis of the overall market for AI.

The Commission will publish a report evaluating and reviewing the proposed AI framework five years following the date on which it becomes applicable.

5.2. Detailed explanation of the specific provisions of the proposal

5.2.1. SCOPE AND DEFINITIONS (TITLE I)

Title I defines the subject matter of the regulation and the scope of application of the new rules that cover the placing on the market, putting into service and use of AI systems. It also sets out the definitions used throughout the instrument. The definition of AI system in the legal framework aims to be as technology neutral and future proof as possible, taking into account the fast technological and market developments related to AI. In order to provide the needed legal certainty, Title I is complemented by Annex I, which contains a detailed list of approaches and techniques for the development of AI to be adapted by the Commission in line with new technological developments. Key participants across the AI value chain are also clearly defined such as providers and users of AI systems that cover both public and private operators to ensure a level playing field.

5.2.2. PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES (TITLE II)

Title II establishes a list of prohibited AI. The regulation follows a risk-based approach, differentiating between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. The list of prohibited practices in Title II comprises all those AI systems whose use is considered unacceptable as contravening Union values, for instance by violating fundamental rights. The prohibitions covers practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit

자원 및 재원을 요구할 것이다. 각 회원국의 기존 구조에 따라 이는 회원국당 1~25명의 상근 상당 인력(Full Time Equivalents, FTE)에 이를 수 있다.

관련 비용의 상세한 내역은 본 제안에 링크된 '재정 설명서(financial statement)'에서 확인할 수 있다.

5. 기타 요소

5.1. 시행 계획과 모니터링, 평가 및 보고 체계

견고한 모니터링 및 평가 체계는 제안이 목표를 효과적으로 달성하는 데 매우 중요하다. 유럽연합 집행위원회는 제안의 효과를 모니터링하는 일을 책임진다. 위원회는 독립형 고위험 AI 애플리케이션을 전 EU 공용 데이터베이스에 등록하기 위한 시스템을 수립할 것이다. 이 등록은 또한 관할 기관과 사용자 및 기타 이해관계자로 하여금 고위험 AI 시스템이 제안에 명시된 요구사항을 준수하는지 여부를 확인하고 기본권에 고위험을 초래하는 AI 시스템에 대한 감독을 강화할 수 있게 해준다. 이 데이터베이스를 구성하기 위해 AI 제공자는 각자의 시스템과 해당 시스템에 대해 수행된 적합성 평가에 관한 유의미한 정보를 이 데이터베이스에 제공해야 한다.

나아가 AI 제공자는 기본권 의무의 위반을 구성하는 중대한 사건 또는 오작동을 인지하는 경우 즉시, 그리고 AI 시스템을 리콜하거나 시장에서 회수하는 경우 이를 국가 관할 기관에 통지해야 한다. 이어서 국가 관할 기관은 사건 또는 오작동을 조사하고, 필요한 모든 정보를 수집하고, 이를 적절한 메타데이터와 함께 위원회에 정기적으로 전송한다. 위원회는 AI 시장 전반에 대한 종합적 분석을 통해 이러한 사건에 관한 정보를 보완한다.

유럽연합 집행위원회는 제안된 AI 프레임워크를 평가·검토하는 보고서를 그것이 적용되는 날짜로부터 5년 후에 공개한다.

5.2. 본 제안의 특정 조항에 대한 상세한 설명

5.2.1. 범위 및 정의(제1편)

제1편(Title I)은 규정의 주제들과 AI 시스템의 출시, 서비스 개시 및 사용을 망라하는 새로운 규칙의 적용 범위를 정의한다. 아울러 문서 전반에 걸쳐 사용되는 정의들을 제시한다. 법적 프레임워크 내에서 AI 시스템의 정의는 AI와 관련된 기술과 시장의 급속한 발전을 고려하여 가능한 한 기술 중립적이고 미래 지향적(future-proof)인 관점을 견지한다. 필요한 법적 확실성을 확보하기 위해, 제1편은 새로운 기술 발전에 발맞추어 유럽연합 집행위원회가 채택하는 AI의 개발을 위한 접근법과 기법의 상세한 목록을 포함하는 부속서 I에 의해 보완된다. 이와 더불어, 공평한 경쟁의 장을 보장하기 위해 공공/민간 운영자들을 망라한 AI 시스템의 제공자와 사용자 등, AI 가치 사슬을 포괄하는 주요 참여자들이 명확히 정의된다.

5.2.2. 금지되는 인공 지능 관행(제2편)

제2편(Title II)은 금지되는 AI의 목록을 제시한다. 규정은 (i) 용납할 수 없는 위험, (ii) 높은 위험, (iii) 낮은 위험 또는 최소한의 위험을 초래하는 AI의 사용을 구분하는 위험 기반 접근법을 따른다. 제2편의 금지되는 관행 목록에는 예컨대 기본권을 침해하는 등 유럽 연합의 가치에 위배되어 용납할 수 없는 것으로 간주되는 모든 AI 시스템의 사용이 포함된다. 금지 대상에는 의식을 벗어난 식역하 기법을 통해 사람들을 조종하거나, 아동이나 장애인과 같은 취약 집단의 취약성을 이용하여

vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm. Other manipulative or exploitative practices affecting adults that might be facilitated by AI systems could be covered by the existing data protection, consumer protection and digital service legislation that guarantee that natural persons are properly informed and have free choice not to be subject to profiling or other practices that might affect their behaviour. The proposal also prohibits AI-based social scoring for general purposes done by public authorities. Finally, the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

5.2.3. HIGH-RISK AI SYSTEMS (TITLE III)

Title III contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. In line with a risk-based approach, those high-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used.

Chapter 1 of Title III sets the classification rules and identifies two main categories of high-risk AI systems:

- AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;
- other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III.

This list of high-risk AI systems in Annex III contains a limited number of AI systems whose risks have already materialised or are likely to materialise in the near future. To ensure that the regulation can be adjusted to emerging uses and applications of AI, the Commission may expand the list of high-risk AI systems used within certain pre-defined areas, by applying a set of criteria and risk assessment methodology.

Chapter 2 sets out the legal requirements for high-risk AI systems in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security. The proposed minimum requirements are already state-of-the-art for many diligent operators and the result of two years of preparatory work, derived from the Ethics Guidelines of the HLEG[29], piloted by more than 350 organisations[30]. They are also largely consistent with other international recommendations and principles, which ensures that the proposed AI framework is compatible with those adopted by the EU's international trade partners. The precise technical solutions to achieve compliance with those requirements may be provided by standards or by other technical specifications or otherwise be developed in accordance with general engineering or scientific knowledge at the discretion of the provider of the AI system. This flexibility is particularly important, because it allows providers of AI systems to choose the

[29] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019.

[30] They were also endorsed by the Commission in its 2019 Communication on human-centric approach to AI.

정신적·신체적 피해를 초래하는 방식으로 그들의 행동을 현저히 왜곡할 잠재성이 큰 관행들이 포함된다. AI 시스템에 의해 촉발될 수 있는 성인에게 피해를 주는 기타 조작 또는 착취 관행은 자연인이 그들의 행동에 영향을 미칠 수 있는 프로파일링 또는 기타 관행에 연루되지 않도록 적절한 통지를 받고 자유로운 선택을 할 수 있도록 보장하는 기존의 데이터 보호, 소비자 보호 및 디지털 서비스 법규를 통해 처리할 수 있다. 본 제안은 또한 공공 기관이 수행하는 일반적 목적의 AI 기반 소셜 스코어링을 금지한다. 끝으로, 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 것도 특정한 제한적 예외가 적용되지 않는 한 금지된다.

5.2.3. 고위험 AI 시스템(제3편)

제3편(Title III)은 자연인의 건강과 안전 또는 기본권에 고위험을 초래하는 AI 시스템에 대한 특정 규칙을 포함한다. 위험 기반 접근법에 따라, 이러한 고위험 AI 시스템은 특정한 필수 요건을 준수하고 사전 적합성 평가를 받는 것을 조건으로 유럽 시장에서 허용된다. AI 시스템을 고위험으로 분류하는 일은 기존의 제품 안전 법규에 따라 AI 시스템의 의도된 목적을 근거로 이루어진다. 따라서 고위험 분류는 AI 시스템이 수행하는 기능뿐 아니라 해당 시스템을 사용하는 구체적 목적과 방식에 의해서도 좌우된다.

제3편 제1장은 분류 규칙을 설정하고 고위험 AI 시스템의 두 가지 주요 범주를 규정한다.

- 제3자 사전 적합성 평가를 받는 제품의 안전 구성요소로 사용되는 AI 시스템
- 부속서 III에 명시된 기본권에 영향을 미치는 기타 독립형 AI 시스템.

부속서 III의 고위험 AI 시스템 목록에는 이미 위험이 구체화되거나 가까운 미래에 구체화될 가능성이 있는 제한된 수의 AI 시스템이 포함된다. 유럽연합 집행위원회는 AI의 새로운 사용 및 애플리케이션에 맞추어 규정을 조정할 수 있도록 보장하기 위해, 일련의 기준과 위험 평가 방법론을 적용하여 사전 정의된 특정 영역 내에서 사용되는 고위험 AI 시스템의 목록을 확장할 수 있다.

제2장은 데이터 및 데이터 거버넌스, 문서 및 기록 유지, 투명성 및 사용자에 대한 정보 제공, 인간의 감독, 견고성, 정확성, 보안 등과 관련된 고위험 AI 시스템에 대한 법적 요구사항을 명시한다. 제안된 최소 요건은 HLEG의 윤리 가이드라인[29]에서 파생되고 350개 이상의 조직이 선도한 2년에 걸친 준비 작업의 결과물이며[30], 다수의 성실한 운영자들에게는 이미 최신 트렌드가 되고 있다. 이는 또한 제안된 AI 프레임워크가 EU의 국제 무역 파트너들이 채택한 프레임워크와 양립할 수 있도록 보장하는 다른 국제 권고사항 및 원칙들과 대체로 일치한다. 이러한 요구사항을 준수하는 정확한 기술 솔루션은 표준 또는 기타 기술 규격에 의해 제공되거나 AI 시스템 제공자의 재량에 따라 일반적인 공학 또는 과학 지식을 토대로 개발될 수 있다. 이러한 유연성은 AI 시스템 제공자가 이 분야의 최신 트렌드와 기술적·과학적 진보를 고려하여 각자의 요구사항을 충족하는 방식을

---

29 High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019.

30 이는 또한 AI에 대한 인간 중심 접근법에 관한 2019 Communication에서 유럽연합 집행위원회에 의해 지지되었다.

way to meet their requirements, taking into account the state-of-the-art and technological and scientific progress in this field.

Chapter 3 places a clear set of horizontal obligations on providers of high-risk AI systems. Proportionate obligations are also placed on users and other participants across the AI value chain (e.g., importers, distributors, authorized representatives).

Chapter 4 sets the framework for notified bodies to be involved as independent third parties in conformity assessment procedures, while Chapter 5 explains in detail the conformity assessment procedures to be followed for each type of high-risk AI system. The conformity assessment approach aims to minimise the burden for economic operators as well as for notified bodies, whose capacity needs to be progressively ramped up over time. AI systems intended to be used as safety components of products that are regulated under the New Legislative Framework legislation (e.g. machinery, toys, medical devices, etc.) will be subject to the same ex-ante and ex-post compliance and enforcement mechanisms of the products of which they are a component. The key difference is that the ex-ante and ex-post mechanisms will ensure compliance not only with the requirements established by sectorial legislation, but also with the requirements established by this regulation.

As regards stand-alone high-risk AI systems that are referred to in Annex III, a new compliance and enforcement system will be established. This follows the model of the New Legislative Framework legislation implemented through internal control checks by the providers with the exception of remote biometric identification systems that would be subject to third party conformity assessment. A comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement, could be an effective and reasonable solution for those systems, given the early phase of the regulatory intervention and the fact the AI sector is very innovative and expertise for auditing is only now being accumulated. An assessment through internal checks for 'stand-alone' high-risk AI systems would require a full, effective and properly documented ex ante compliance with all requirements of the regulation and compliance with robust quality and risk management systems and post-market monitoring. After the provider has performed the relevant conformity assessment, it should register those stand-alone high-risk AI systems in an EU database that will be managed by the Commission to increase public transparency and oversight and strengthen ex post supervision by competent authorities. By contrast, for reasons of consistency with the existing product safety legislation, the conformity assessments of AI systems that are safety components of products will follow a system with third party conformity assessment procedures already established under the relevant sectoral product safety legislation. New ex ante re-assessments of the conformity will be needed in case of substantial modifications to the AI systems (and notably changes which go beyond what is pre-determined by the provider in its technical documentation and checked at the moment of the ex-ante conformity assessment).

5.2.4. TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (TITLE IV)

Title IV concerns certain AI systems to take account of the specific risks of manipulation they pose. Transparency obligations will apply for systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes'). When persons interact with an AI system or their emotions or characteristics are recognised through automated means, people must be informed of that circumstance. If an AI system is used to generate or manipulate image, audio or video content that appreciably resembles authentic content, there should be an obligation to disclose that the content is generated through automated means, subject to

선택할 수 있도록 해주기 때문에 특히 중요하다.

제3장은 고위험 AI 시스템의 제공자에게 명확한 일련의 수평적 의무를 부과한다. 아울러 사용자와 AI 가치 사슬 전반에 걸친 다른 참여자들(가령 수입업자, 유통업자, 공인 대리인 등)에게도 비례적인 의무가 부과된다.

제4장은 적합성 평가 절차에 독립 제3자로 관여하는 인증 기관을 위한 프레임워크를 설정하고, 제5장은 각 유형의 고위험 AI 시스템에 대해 수행하는 적합성 평가 절차에 대해 상세히 설명한다. 적합성 평가 접근법의 목표는 장기간에 걸쳐 점진적으로 역량을 강화해야 하는 경제 운영자와 인증 기관의 부담을 최소화하는 것이다. 새로운 입법 프레임워크(NLF)에 따라 규제되는 제품의 안전 구성요소로 사용되는 AI 시스템(예: 기계류, 장난감, 의료 기기 등)에는 그것이 구성하는 제품과 동일한 사전/사후 준수 및 집행 체계가 적용된다. 주요한 차이점은 사전/사후 메커니즘이 부문별 법규에 의해 수립된 요구사항뿐 아니라 이 규정에 의해 수립된 요구사항의 준수도 보장한다는 점이다.

부속서 III에 언급된 독립형 고위험 AI 시스템에 대해 새로운 준수 및 집행 시스템이 확립될 것이다. 이는 제공자의 내부 관리 점검을 통해 시행되는 새로운 입법 프레임워크(NLF)의 모델을 따른다. 단, 제3자 적합성 평가를 받는 원격 생체 인식 시스템은 예외이다. 규제 개입이 초기 단계에 머물러 있고 AI 부문이 매우 혁신적이며 감사를 위한 전문지식이 충분히 축적된 지 않은 점을 감안할 때, 내부 점검을 통한 종합적 사전 적합성 평가와 강력한 사후 집행을 결합하면 그러한 시스템을 위한 효과적이고 합리적인 솔루션이 될 수 있다. '독립형' 고위험 AI 시스템에 대한 내부 점검을 통한 평가는 규정의 모든 요구사항을 사전에 철저히 효과적으로 준수·기록하고, 엄격한 품질 및 위험 관리 시스템과 출시 후 모니터링을 준수할 것을 요구한다. 제공자는 관련 적합성 평가를 수행한 후, 공공 투명성 및 감독을 보장하고 관할 기관의 사후 감독을 강화하기 위해 유럽연합 집행위원회가 관리하는 EU 데이터베이스에 해당 독립형 고위험 AI 시스템을 등록해야 한다. 이와 대조적으로, 제품의 안전 구성요소인 AI 시스템의 적합성 평가는 기존 제품 안전 법규와의 일관성을 이유로 관련 부문별 제품 안전 법규에 따라 이미 확립된 제3자 적합성 평가 절차를 따른다. AI 시스템이 상당히 변경되는 경우(특히 제공자가 기술 문서에서 사전 확인하고 사전 적합성 평가 시 점검한 것을 넘어서는 변경) 새로운 사전 적합성 재평가가 필요할 것이다.

5.2.4. 특정 AI 시스템에 대한 투명성 의무(제4편)

제4편(Title IV)은 특정 AI 시스템이 초래하는 조작의 위험을 다룬다. 투명성 의무는 (i) 인간과 상호작용하거나, (ii) 생체 데이터를 근거로 감정 상태를 탐지하거나 (사회적) 범주와의 연관성을 파악하는 데 사용되거나, (iii) 콘텐츠를 생성 또는 조작하는 ('딥 페이크') 시스템에 적용된다. 사람들이 AI 시스템과 상호 작용하거나 자동화된 수단을 통해 그들의 감정 또는 특성이 인식되는 경우에는 반드시 당사자에게 그러한 상황을 통지해야 한다. AI 시스템이 진본 콘텐츠와 눈에 띄게 유사한 이미지, 오디오 또는 비디오 콘텐츠를 생성하거나 조작하는 데 사용되는 경우, 콘텐츠가 자동화된 수단을 통해 생성된다는 사실을 공개할 의무를 부과해야 한다. 단, 합법적 목적(법 집행, 표현의 자유 등)을 위한 경우는 예외로 한다. 이는 사람들이 정보에 근거한 선택을 내리거나

exceptions for legitimate purposes (law enforcement, freedom of expression). This allows persons to make informed choices or step back from a given situation.

5.2.5. MEASURES IN SUPPORT OF INNOVATION (TITLE V)

Title V contributes to the objective to create a legal framework that is innovation-friendly, future-proof and resilient to disruption. To that end, it encourages national competent authorities to set up regulatory sandboxes and sets a basic framework in terms of governance, supervision and liability. AI regulatory sandboxes establish a controlled environment to test innovative technologies for a limited time on the basis of a testing plan agreed with the competent authorities. Title V also contains measures to reduce the regulatory burden on SMEs and start-ups.

5.2.6. GOVERNANCE AND IMPLEMENTATION (TITLES VI, VII AND VII)

Title VI sets up the governance systems at Union and national level. At Union level, the proposal establishes a European Artificial Intelligence Board (the 'Board'), composed of representatives from the Member States and the Commission. The Board will facilitate a smooth, effective and harmonised implementation of this regulation by contributing to the effective cooperation of the national supervisory authorities and the Commission and providing advice and expertise to the Commission. It will also collect and share best practices among the Member States.

At national level, Member States will have to designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of the regulation. The European Data Protection Supervisor will act as the competent authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of this regulation.

Title VII aims to facilitate the monitoring work of the Commission and national authorities through the establishment of an EU-wide database for stand-alone high-risk AI systems with mainly fundamental rights implications. The database will be operated by the Commission and provided with data by the providers of the AI systems, who will be required to register their systems before placing them on the market or otherwise putting them into service.

Title VIII sets out the monitoring and reporting obligations for providers of AI systems with regard to post-market monitoring and reporting and investigating on AI-related incidents and malfunctioning. Market surveillance authorities would also control the market and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market. Market surveillance authorities would have all powers under Regulation (EU) 2019/1020 on market surveillance. Ex-post enforcement should ensure that once the AI system has been put on the market, public authorities have the powers and resources to intervene in case AI systems generate unexpected risks, which warrant rapid action. They will also monitor compliance of operators with their relevant obligations under the regulation. The proposal does not foresee the automatic creation of any additional bodies or authorities at Member State level. Member States may therefore appoint (and draw upon the expertise of) existing sectorial authorities, who would be entrusted also with the powers to monitor and enforce the provisions of the regulation.

All this is without prejudice to the existing system and allocation of powers of ex-post enforcement of obligations regarding fundamental rights in the Member States. When necessary for their mandate, existing supervision and enforcement authorities will also have the power to request and access any documentation maintained following this regulation and, where needed, request market surveillance authorities to organise testing of the high-risk AI system through technical means.

주어진 상황에서 한 걸음 물러나 생각할 수 있게 해준다.

5.2.5. 혁신을 지원하는 조치(제5편)

제5편(Title V)은 혁신 친화적이고 미래 지향적이며(future-proof) 회복력 있는 법적 프레임워크를 구축한다는 목표에 기여한다. 이러한 목표를 달성하기 위해, 국가 관할 기관에 대해 규제 샌드박스를 설정하고 거버넌스, 감독 및 책임에 관한 기본 프레임워크를 구축할 것을 장려한다. AI 규제 샌드박스는 관할 기관과 합의한 테스트 계획을 토대로 제한된 시간 동안 혁신 기술을 테스트할 수 있는 통제 환경을 구축한다. 제5편은 또한 중소기업과 스타트업에 대한 규제 부담을 완화하기 위한 조치를 포함한다.

5.2.6. 거버넌스 및 시행(제6, 7, 8편)

제6편(Title VI)은 유럽 연합 및 국가 수준에서 거버넌스 시스템을 구축한다. 유럽 연합 수준에서, 본 제안은 회원국과 유럽연합 집행위원회의 대표들로 구성된 유럽 인공지능 위원회('위원회')를 설립한다. 위원회는 국가 감독 기관과 유럽연합 집행위원회의 효과적인 협력에 기여하고 유럽연합 집행위원회에 조언과 전문지식을 제공함으로써 이 규정의 원활하고 효과적이며 조화된 시행을 촉진한다. 아울러 회원국 사이의 모범 사례를 수집하고 공유한다.

국가 수준에서, 회원국은 하나 이상의 국가 관할 기관을 지명하고, 규정의 적용과 시행을 감독하기 위한 목적으로 그 가운데에서 국가 감독 기관을 지명해야 한다. 유럽 데이터 보호 감독관(European Data Protection Supervisor)은 유럽 연합 기관, 기구, 단체가 이 규정의 범위 내에 속할 경우 이를 감독하는 관할 기관 역할을 한다.

제7편(Title VII)은 기본권에 영향을 미치는 독립형 고위험 AI 시스템에 대한 전 EU 데이터베이스를 구축하여 유럽연합 집행위원회와 국가 기구의 모니터링 작업을 촉진하는 것을 목표로 한다. 이 데이터베이스는 유럽연합 집행위원회가 운영하고 AI 시스템의 제공자가 데이터를 제공한다. 제공자는 시스템을 출시하거나 서비스를 개시하기 전에 시스템을 등록해야 한다.

제8편(Title VIII)은 AI 시스템의 제공자에 대해 출시 후 모니터링 및 보고, 그리고 AI 관련 사건 및 오작동에 대한 조사와 관련한 모니터링 및 보고 의무를 명시한다. 또한, 시장 감시 기관은 시장을 통제하고 이미 출시된 모든 고위험 AI 시스템에 대한 의무 및 요구사항의 준수 여부를 조사한다. 시장 감시 기관은 Regulation (EU) 2019/1020에 따라 시장 감시에 대한 모든 권한을 가진다. 사후 집행은 AI 시스템이 출시된 후 신속한 조치를 요하는 예기치 않은 위험을 초래할 경우 공공 기관이 개입할 수 있는 권한과 자원을 확보하도록 보장해야 한다. 이들은 또한 운영자가 규정에 따른 관련 의무를 준수하는지 여부를 모니터한다. 본 제안은 회원국 수준에서 추가 기구 또는 기관이 자동으로 설립될 것으로 예견하지 않는다. 따라서 회원국은 기존의 부문별 기관을 임명하여 규정의 조항들을 모니터하고 집행할 권한을 위임하고 그 전문지식을 활용해야 한다.

이 모든 내용은 회원국의 기존 시스템을 침해하지 않으며 기본권과 관련된 의무를 사후 집행할 권한의 할당을 침해하지 않는다. 기존의 감독 및 집행 기관 역시 그들의 임무를 위해 필요할 경우 이 규정에 따라 유지되는 문서를 요구하고 접근할 권한을 가지며, 필요한 경우 시장 감시 기관에 대해 기술적 수단을 통한 고위험 AI 시스템의 테스트를 조직할 것을 요구할 권한을 가진다.

5.2.7. CODES OF CONDUCT (TITLE IX)

Title IX creates a framework for the creation of codes of conduct, which aim to encourage providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems (as laid out in Title III). Providers of non-high-risk AI systems may create and implement the codes of conduct themselves. Those codes may also include voluntary commitments related, for example, to environmental sustainability, accessibility for persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of development teams.

5.2.8. FINAL PROVISIONS (TITLES X, XI AND XII)

Title X emphasizes the obligation of all parties to respect the confidentiality of information and data and sets out rules for the exchange of information obtained during the implementation of the regulation. Title X also includes measures to ensure the effective implementation of the regulation through effective, proportionate, and dissuasive penalties for infringements of the provisions.

Title XI sets out rules for the exercise of delegation and implementing powers. The proposal empowers the Commission to adopt, where appropriate, implementing acts to ensure uniform application of the regulation or delegated acts to update or complement the lists in Annexes I to VII.

Title XII contains an obligation for the Commission to assess regularly the need for an update of Annex III and to prepare regular reports on the evaluation and review of the regulation. It also lays down final provisions, including a differentiated transitional period for the initial date of the applicability of the regulation to facilitate the smooth implementation for all parties concerned.

5.2.7. 행동 지침(제9편)

제9편(Title IX)은 비 고위험 AI 시스템의 제공자가 (제3편에 명시된) 고위험 AI 시스템에 대한 필수 요건을 자발적으로 적용하도록 장려하는 행동 지침을 규정하기 위한 프레임워크를 제안한다. 비 고위험 AI 시스템의 제공자는 스스로 행동 지침을 제정하고 시행할 수 있다. 이러한 지침에는 예컨대 환경의 지속가능성, 장애인의 접근성, AI 시스템의 설계와 개발에 대한 이해관계자의 참여, 개발 팀의 다양성 등과 관련된 자발적 약속이 포함될 수 있다.

5.2.8. 최종 조항(제10, 11, 12편)

제10편(Title X)은 정보와 데이터의 기밀을 유지해야 할 모든 당사자의 의무를 강조하고 규정을 시행하는 과정에서 획득한 정보의 교환에 관한 규칙을 제정한다. 제10편은 또한 규정의 위반에 대한 효과적이고 비례적이며 억제적인 처벌을 통한 규정의 효과적 시행을 보장하기 위한 조치들을 포함한다.

제11편(Title XI)은 위임 및 실행 권한의 행사에 관한 규칙을 제정한다. 본 제안은 유럽연합 집행위원회에 대해 적절한 경우 규정의 균일한 적용을 보장하기 위한 실행 규정(implementing act) 또는 부속서 I~VII의 목록들을 업데이트하거나 보안하기 위한 위임 규정(delegated act)을 채택할 권한을 부여한다.

제12편(Title XII)은 부속서 III을 업데이트할 필요가 있는지 정기적으로 평가하고 규정의 평가와 검토에 관한 정기 보고서를 작성할 유럽연합 집행위원회의 의무를 포함한다. 이와 더불어, 모든 관계 당사자를 위해 원활한 시행을 촉진하기 위해 규정의 적용 개시일에 대한 차별화된 과도 기간을 포함한 최종 조항을 명시한다.

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[31],

Having regard to the opinion of the Committee of the Regions[32],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) Artificial intelligence systems (AI systems) can be easily deployed in multiple sectors of the economy and society, including cross border, and circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured, while divergences hampering the free circulation of AI systems and related products and services within the internal market should be prevented, by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning

[31] OJ C […], […], p. […].
[32] OJ C […], […], p. […].

2021/0106 (COD)

인공 지능에 관한 조화 규칙(인공지능법) 제정 및 특정 유럽 연합 법규 개정을 위한 유럽 의회 및 유럽 이사회의 규정(Regulation) 제안

유럽 의회 및 유럽 연합 이사회는,

유럽 연합의 기능에 관한 조약, 특히 제16조 및 제114조를 고려하고,

유럽연합 집행위원회의 제안을 고려하여,

각국 의회에 입법 초안을 전달한 후,

유럽 경제 사회 위원회의 의견을 고려하고[31],

지역 위원회의 의견을 고려하여[32],

일반적인 입법 절차에 따라,

다음을 고려하여 본 규정을 채택하였다.

(1) 본 규정(Regulation)의 목적은 특히 유럽 연합의 가치에 부합하는 인공 지능의 개발, 마케팅, 사용을 위한 통일된 법적 프레임워크를 구축함으로써 역내 시장의 기능을 개선하는 것이다. 본 규정은 건강, 안전, 기본권의 수준 높은 보호를 비롯한 여러 가지 공익의 최우선 가치를 추구하며, AI 기반 상품 및 서비스의 자유로운 국가간 이동을 보장하여 본 규정에 의해 명시적으로 허가되지 않은 한 회원국들이 AI 시스템의 개발, 마케팅, 사용을 제한하는 것을 방지한다.

(2) 인공 지능 시스템(AI 시스템)은 경제 및 사회의 여러 부문에 손쉽게 배포되고 국가간 및 유럽 연합 전반에 걸쳐 유통될 수 있다. 일부 회원국은 인공 지능이 기본권을 준수하여 안전하게 개발·사용되도록 보장하는 국가 규칙을 채택하려는 움직임을 보이고 있다. 서로 다른 국가 규칙들은 역내 시장의 파편화를 불러오고 AI 시스템을 개발·사용하는 운영자를 위한 법적 확실성을 저해할 수 있다. 따라서 유럽 연합 전역에 걸쳐 일관되고 높은 수준의 보호를 보장하는 한편, 유럽 연합의 기능에 관한 조약(TFEU) 제114조를 근거로 운영자에 대해 균일한 의무를 규정하고 공익의 최우선 가치와 시민의 권리에 대해 균일한 보호를 보장함으로써 역내 시장 내에서 AI 시스템과 관련 제품 및 서비스의 자유로운 유통을 방해하는 불일치를 방지해야 한다. 본 규정에 개인 데이터의 처리와 관련된 개인의 보호에 관한 특정 규칙, 특히 법 집행의 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식을 위해 AI 시스템을 사용하는 데 대한 제한이 포함되는 점을 감안할 때,

[31] OJ C […], […], p. […].
[32] OJ C […], […], p. […].

restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(3) Artificial intelligence is a fast evolving family of technologies that can contribute to a wide array of economic and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of artificial intelligence can provide key competitive advantages to companies and support socially and environmentally beneficial outcomes, for example in healthcare, farming, education and training, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, and climate change mitigation and adaptation.

(4) At the same time, depending on the circumstances regarding its specific application and use, artificial intelligence may generate risks and cause harm to public interests and rights that are protected by Union law. Such harm might be material or immaterial.

(5) A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. By laying down those rules, this Regulation supports the objective of the Union of being a global leader in the development of secure, trustworthy and ethical artificial intelligence, as stated by the European Council[33], and it ensures the protection of ethical principles, as specifically requested by the European Parliament[34].

(6) The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension. AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to–date in the light of market and technological

---

33 European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

34 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

본 규정을 TFEU 제16조에 기초하는 것이 적절하다. 그러한 특정 규칙과 TFEU 제16조의 원용에 비추어 유럽 데이터 보호 이사회(European Data Protection Board)와 협의하는 것이 바람직하다.

(3) 인공 지능은 산업과 사회 활동의 전 영역에 걸쳐 광범위한 경제적·사회적 편익에 기여할 수 있는 빠르게 진화하는 기술이다. 인공 지능의 사용은 예측을 개선하고, 운영과 자원 할당을 최적화하고, 개인과 조직이 사용할 수 있는 디지털 솔루션을 개인화함으로써 기업에 주요한 경쟁 우위를 제공하고, 보건 의료, 농업, 교육 및 훈련, 인프라 관리, 에너지, 수송 및 물류, 공공 서비스, 안보, 사법, 자원 및 에너지 효율, 기후 변화 완화 및 적응 등의 분야에서 사회적·환경적으로 유익한 결과를 이끌어낼 수 있다.

(4) 그와 동시에, 구체적인 적용 및 사용과 관련된 상황에 따라 인공 지능은 유럽 연합법에 의해 보호되는 공익에 위험과 피해를 초래할 수 있다. 이러한 피해는 물질적일 수도 있고 정신적일 수도 있다.

(5) 따라서, 역내 시장에서 건강과 안전 등 공익의 보호와 유럽 연합법에 의해 인정·보호되는 기본권의 보호를 높은 수준으로 충족하는 인공 지능의 개발, 사용, 수용을 촉진하기 위해서는 인공 지능에 대한 조화 규칙을 제정하는 유럽 연합의 법적 프레임워크가 필요하다. 이러한 목표를 달성하려면, AI 시스템의 출시 및 서비스 개시와 관련한 규칙을 제정하여 원활한 역내 시장의 기능을 보장하고 그러한 시스템이 상품과 서비스의 자유로운 이동에 따른 혜택을 누릴 수 있도록 해야 한다. 그러한 규칙을 제정함으로써, 본 규정은 유럽 이사회가 명시하는 안전하고 신뢰할 수 있으며 윤리적인 인공 지능의 개발에서 글로벌 리더가 된다는 유럽 연합의 목표[33]를 지원하고, 유럽 의회가 명시적으로 요청한 윤리 원칙의 보호[34]를 보장한다.

(6) 법적 확실성을 보장하는 동시에 미래의 기술 개발에 대비한 유연성을 제공하기 위해서는 AI 시스템의 개념이 명확히 정의되어야 한다. 정의는 소프트웨어의 주요 기능 특성, 특히 인간이 정의한 일련의 목표를 위해 물리적 또는 디지털 차원에서 시스템이 상호 작용하는 환경에 영향을 주는 콘텐츠, 예측, 권고 또는 결정과 같은 아웃풋을 생성할 수 있는 능력에 근거해야 한다. AI 시스템은 다양한 수준의 자율성을 가지고 운용되도록 설계될 수 있으며 시스템이 제품에 물리적으로 임베드(내장)되어 있는지 또는 임베드되지 않은(비내장) 상태로 제품의 기능을 수행하는지 여부에 관계없이 독립형으로 사용되거나 제품의 구성요소로 사용될 수 있다. AI 시스템의 정의는 그 개발에 사용되는 기법과 접근법의 목록으로 보완되어야 하며, 목록을 수정하기 위한 유럽연합 집행위원회 위임 규정을 채택하여 시장과 기술의 발전에 따라 목록을

[33] European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

[34] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

developments through the adoption of delegated acts by the Commission to amend that list.

(7) The notion of biometric data used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council[35], Article 3(18) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[36] and Article 3(13) of Directive (EU) 2016/680 of the European Parliament and of the Council[37].

(8) The notion of remote biometric identification system as used in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used. Considering their different characteristics and manners in which they are used, as well as the different risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

(9) For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a

---

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

36 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)

37 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) (OJ L 119, 4.5.2016, p. 89).

최신으로 유지해야 한다.

(7) 본 규정에서 사용되는 생체 인식 데이터의 개념은 유럽 의회 및 유럽 이사회의 Regulation (EU) 2016/679 제4(14)조[35], 유럽 의회 및 유럽 이사회의 Regulation (EU) 2018/1725 제3(18)조[36] 및 유럽 의회 및 유럽 이사회의 Directive (EU) 2016/680 제3(13)조[37]에 정의된 생체 인식 데이터의 개념과 일치하도록 해석되어야 한다.

(8) 본 규정에서 사용되는 원격 생체 인식 시스템의 개념은 사용되는 기술, 프로세스 또는 생체 인식 데이터의 유형에 관계없이 특정인의 생체 인식 데이터를 참조 데이터베이스에 포함된 생체 인식 데이터와 비교하여 원거리에 있는 자연인을 식별하는 AI 시스템으로서, 대상인이 존재하고 식별할 수 있는지 여부에 대한 사전 지식 없이 기능적으로 정의되어야 한다. 그 다양한 특성과 사용되는 방식, 그리고 수반되는 다양한 위험을 감안하여 '실시간(real-time)' 및 '사후(post)' 원격 생체 인식 시스템 간의 구분이 이루어져야 한다. '실시간' 시스템의 경우 생체 인식 데이터의 수집, 비교, 식별이 모두 즉각적, 거의 즉각적 또는 어떠한 경우에도 큰 지연 없이 이루어진다. 이 점에서, 사소한 지연을 허용함으로써 해당 AI 시스템의 '실시간' 사용에 대한 본 규정의 규칙들을 회피할 수 있는 여지가 없어야 한다. '실시간' 시스템은 예컨대 카메라 또는 기타 유사한 기능의 장치에 의해 생성된 비디오 영상과 같은 'live' 또는 'near-live' 자료의 사용을 수반한다. 이와 대조적으로, '사후(post)' 시스템의 경우에는 생체 인식 데이터가 이미 수집되어 있고 상당한 지연 후에야 비교와 식별이 이루어진다. 이는 당사자와 관련하여 시스템을 사용하기 전에 폐쇄 회로(CC) TV 카메라 또는 개인 장치에 의해 생성된 사진 또는 비디오 영상과 같은 자료를 수반한다.

(9) 본 규정의 목적을 위해, 공개적으로 접근 가능한 공간(publicly accessible space)은 문제의 장소가 개인 소유인지 공공 소유인지 여부와 관계없이 일반인이 접근할 수 있는 물리적 장소를 가리키는 것으로 이해되어야 한다. 따라서 가정, 비공개 클럽, 사무소, 창고, 공장 등과 같이 당사자가 특별히 초대되거나 허가된 경우 외에는 성격상 사적이고 보통 법 집행 기관을 포함한 제3자가 자유롭게 접근할 수 없는 장소는 이 개념에 포함되지 않는다. 온라인 공간은 물리적 공간이 아니므로 역시 여기에 포함되지 않는다. 하지만, 공간에 접근하기 위한 특정 조건이 적용될 수 있다는 단순한 사실만으로 본 규정의 의미 내에서

---

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

36 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39)

37 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) (OJ L 119, 4.5.2016, p. 89).

particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by- case basis, having regard to the specificities of the individual situation at hand.

(10) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to users of AI systems established within the Union.

(11) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are neither placed on the market, nor put into service, nor used in the Union. This is the case for example of an operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk and whose effects impact natural persons located in the Union. In those circumstances, the AI system used by the operator outside the Union could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union. Nonetheless, to take into account existing arrangements and special needs for cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of international agreements concluded at national or European level for law enforcement and judicial cooperation with the Union or with its Member States. Such agreements have been concluded bilaterally between Member States and third countries or between the European Union, Europol and other EU agencies and third countries and international organisations.

(12) This Regulation should also apply to Union institutions, offices, bodies and agencies when acting as a provider or user of an AI system. AI systems exclusively developed or used for military purposes should be excluded from the scope of this Regulation where that use falls under the exclusive remit of the Common Foreign and Security Policy regulated under Title V of the Treaty on the European Union (TEU). This Regulation should be without prejudice to the provisions regarding the liability of intermediary service providers set out in Directive 2000/31/EC of the European Parliament and of the Council [as amended by the Digital Services Act].

(13) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common normative standards for all high-risk AI systems should be established. Those standards should be consistent with the Charter of fundamental rights of the European Union (the Charter) and should be non-discriminatory and in line with the Union's international trade commitments.

공간이 공개적으로 접근 불가능하다는 것을 의미하지는 않는다. 따라서 거리, 정부 건물의 관련 부분 및 대부분의 교통 인프라와 같은 공공 장소에 더하여, 영화관, 극장, 상점, 쇼핑 센터 등의 공간도 보통 공개적으로 접근 가능하다. 하지만, 주어진 공간이 공개적으로 접근 가능한지 여부는 당면한 개별 상황의 특수성을 고려하여 사례별로 결정되어야 한다.

(10) 유럽 연합 전역에 걸쳐 공평한 경쟁의 장과 개인의 권리 및 자유의 효과적인 보호를 보장하기 위해, 본 규정에 의해 제정되는 규칙은 AI 시스템 제공자에게 그들이 유럽 연합 내에서 또는 제3국에서 설립되었는지 여부에 관계없이 비차별적으로 적용되어야 하며, 유럽 연합 내에서 설립된 AI 시스템 사용자에게 적용되어야 한다.

(11) 특정 AI 시스템은 유럽 연합에서 출시, 서비스 개시 또는 사용되지 않는 경우라도 그 디지털 성격에 비추어 본 규정의 범위 내에 속해야 한다. 이는 예컨대 유럽 연합에서 설립된 운영자가 고위험으로 분류되는 AI 시스템이 수행하고 유럽 연합에 소재한 자연인에게 영향을 미치는 활동과 관련된 특정 서비스를 유럽 연합 외부에서 설립된 운영자에게 계약하는 경우에 해당한다. 그러한 상황에서 유럽 연합 외부의 운영자가 사용하는 AI 시스템은 유럽 연합에서 적법하게 수집되고 전송된 데이터를 처리할 수 있으며, 해당 AI 시스템이 유럽 연합에서 출시, 서비스 개시 또는 사용되지 않는 경우라도 그러한 처리에 따른 해당 AI 시스템의 결과물을 계약하는 유럽 연합의 운용자에게 제공할 수 있다. 본 규정의 회피를 방지하고 유럽 연합에 소재한 자연인을 효과적으로 보호하기 위해, 제3국에서 설립된 시스템이 산출한 결과물이 유럽 연합에서 사용되는 경우에 한하여 본 규정은 해당 AI 시스템의 제공자와 사용자에게도 적용되어야 한다. 그럼에도 불구하고, 정보와 증거를 교환하는 외국 파트너와의 협력을 위한 기존의 협약과 특수한 요구를 고려하여, 본 규정은 유럽 연합 또는 그 회원국과의 법 집행 및 사법적 협력을 위해 국가 또는 유럽 수준에서 체결된 국제 협정의 프레임워크에서 활동하는 제3국의 공공 기관과 국제 기구에는 적용되지 않아야 한다. 그러한 협정은 회원국과 제3국 간 또는 유럽 연합, 유로폴 및 기타 EU 기관과 제3국 및 국제 기구 간에 쌍무적으로 체결되었다.

(12) 이 규정은 또한 AI 시스템의 제공자 또는 사용자 역할을 하는 유럽 연합 기관, 국/청, 기구, 단체에도 적용되어야 한다. 오로지 군사 목적으로 개발되거나 사용되는 AI 시스템은 그러한 사용이 유럽 연합 조약(Treaty on the European Union, TEU)의 제5편에 따라 규제되는 공통 외교 안보 정책(Common Foreign and Security Policy)의 독점 소관에 속하는 경우 본 규정의 범위에서 제외되어야 한다. 본 규정은 유럽 의회 및 유럽 이사회의 Directive 2000/31/EC[디지털 서비스법에 의해 개정]에 명시된 중개 서비스 제공자의 책임과 관련한 조항을 침해하지 않아야 한다.

(13) 건강, 안전 및 기본권과 관련된 공익의 일관되고 높은 수준의 보호를 보장하기 위해 모든 고위험 AI 시스템에 대한 공통 규범 표준을 확립해야 한다. 이러한 표준은 유럽 연합 기본권 헌장(헌장)과 일치하고 비차별적이며 유럽 연합의 국제 거래 규약을 따라야 한다.

(14) In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

(15) Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.

(16) The placing on the market, putting into service or use of certain AI systems intended to distort human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the intention to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. The intention may not be presumed if the distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user. Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research.

(17) AI systems providing social scoring of natural persons for general purpose by public authorities or on their behalf may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify the trustworthiness of natural persons based on their social behaviour in multiple contexts or known or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. Such AI systems should be therefore prohibited.

(18) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in 'real-time' carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.

(19) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in three exhaustively listed and narrowly defined situations, where

(14) AI 시스템에 대해 비례적이고 효과적이며 구속력 있는 규칙을 도입하기 위해서는 명확히 정의된 위험 기반 접근법을 따라야 한다. 이러한 접근법은 AI 시스템이 초래할 수 있는 위험의 강도와 범위에 맞추어 규칙의 유형과 내용을 조정해야 한다. 따라서 특정한 인공지능 관행을 금지하고, 고위험 AI 시스템에 대한 요구사항과 관련 운영자에 대한 의무를 규정하고, 특정 AI 시스템에 대한 투명성 의무를 규정하는 것이 필요하다.

(15) 인공 지능을 사용하면 여러 가지 편익을 얻을 수 있지만, 또 한편으로는 이 기술이 오용되어 조작, 착취, 사회 통제를 위한 새롭고 강력한 도구가 될 수도 있다. 이러한 관행은 특히 인간의 존엄, 자유, 평등, 민주주의, 법치주의, 그리고 차별 금지, 개인정보보호, 아동의 권리를 포함한 기본권을 존중하는 유럽 연합의 가치에 위배되기 때문에 유해하며 금지되어야 한다.

(16) 인간의 행동을 왜곡하여 신체적·정신적 피해를 초래할 가능성이 있는 특정 AI 시스템의 출시, 서비스 개시 또는 사용은 금지되어야 한다. 이러한 AI 시스템은 개인이 인식할 수 없는 식역하 구성요소를 배포하거나 미성년자와 고령자, 신체 또는 정신 장애인의 취약성을 이용한다. 이들은 개인의 행동을 중대하게 왜곡하여 당사자 또는 타인에게 피해를 입히려는 의도를 가진다. 하지만 인간 행동의 왜곡이 제공자 또는 사용자의 통제를 벗어난 AI 시스템에 외적 요인에서 비롯되는 경우에는 그러한 의도를 추정할 수 없다. 이러한 AI 시스템과 관련된 합법적 목적에 관한 연구가 자연인을 피해에 노출시키는 인간-기계 관계에서 AI 시스템의 사용하는 경우에 해당하지 않고 과학 연구에 대해 인정되는 윤리 기준에 따라 수행되는 경우 그러한 연구가 금지에 의해 억제되어서는 안 된다.

(17) 공공 기관에 의해 또는 그를 대신하여 일반적 목적으로 자연인의 소셜 스코어링을 제공하는 AI 시스템은 차별적 결과와 특정 집단의 배제를 초래할 수 있다. 이는 존엄성과 차별 금지에 대한 권리 및 평등과 정의의 가치에 위배될 수 있다. 이러한 AI 시스템은 다양한 맥락에서 자연인의 사회적 행동 또는 알려지거나 예측되는 개인적 특성을 토대로 그의 신뢰성을 평가하거나 분류한다. 이러한 AI 시스템을 통해 획득한 소셜 스코어는 데이터가 처음 생성되거나 수집된 맥락과 무관한 사회적 맥락에서 자연인 또는 전체 집단을 차별 또는 홀대하거나, 그 사회적 행동의 중대성에 비례하지 않거나 정당하지 않은 방식으로 홀대하는 결과를 낳을 수 있다. 따라서 이러한 AI 시스템은 금지되어야 한다.

(18) 법 집행 목적으로 공개적으로 접근 가능한 공간에서 자연인의 '실시간' 원격 생체 인식에 AI 시스템을 사용하는 것은, 그것이 주민 대부분의 사생활에 영향을 주고, 끊임없이 감시당하는 느낌을 촉발하고, 집회의 자유를 비롯한 기본권의 행사를 간접적으로 억제할 수 있는 경우 당사자의 권리와 자유를 특히 침해하는 것으로 간주된다. 뿐만 아니라, '실시간'으로 운용되는 이러한 시스템의 사용과 관련된 영향의 직접성과 추후 확인 또는 시정의 기회가 제한되는 점은 법 집행 활동에 따른 대상자의 권리 및 자유에 대한 위험을 고조시킨다.

(19) 따라서 법 집행 목적으로 이러한 시스템을 사용하는 것은 금지되어야 한다. 단, 그 중요성이 위험을 능가하는 상당한 공익을 성취하기 위해 사용이 절대적으로 필요한, 빠짐없이

the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for potential victims of crime, including missing children; certain threats to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[38] if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State. Such threshold for the custodial sentence or detention order in accordance with national law contributes to ensure that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, of the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA, some are in practice likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification will foreseeably be necessary and proportionate to highly varying degrees for the practical pursuit of the detection, localisation, identification or prosecution of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences.

(20) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to appropriate limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.

(21) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should in principle be obtained prior to the use, except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In such situations of urgency, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations seek to obtain an authorisation as soon as possible, whilst providing the reasons for not having been able to request it earlier.

(22) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State in question has decided to expressly provide for the possibility to authorise such use in its

[38] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

열거되고 좁게 정의된 세 가지 상황은 예외로 한다. 이러한 상황은 다음과 같다: 실종된 아동을 포함한 범죄의 잠재적 피해자를 수색하는 경우; 자연인의 생명 또는 신체적 안전에 대한 특정한 위협 또는 테러 공격의 위협; Council Framework Decision 2002/584/JHA[38]에 언급된 범죄 행위의 범인 또는 용의자 탐지, 소재 파악, 식별 또는 기소. 단, 관련 회원국에서 이러한 범죄 행위를 3년 이상의 최대 기간 동안 구금형 또는 구금 명령으로 처벌 가능하고 그와 같이 동 회원국의 법률에 정의된 경우에 한한다. 국가 법률에 따른 구금형 또는 구금 명령의 이러한 한계치는 해당 범죄 행위가 '실시간' 원격 생체 인식 시스템의 사용을 정당화하기에 충분히 심각할 것을 보장하는 데 일조한다. 나아가, Council Framework Decision 2002/584/JHA에 열거된 32개의 범죄 행위 가운데 일부는, '실시간' 원격 생체 인식에 대한 원용이 열거된 다양한 범죄 행위의 범인 또는 용의자 탐지, 소재 파악, 식별 또는 기소에 필요하고 매우 다양한 수준에서 비례적일 것으로 예측된다는 점에서, 그리고 가능한 피해 또는 부정적 결과의 중대성, 개연성 및 규모의 차이를 고려할 때, 실제로 다른 것보다 더 중요할 가능성이 있다.

(20) 또한 이러한 시스템이 책임감 있고 균형 잡힌 방식으로 사용되도록 보장하기 위해서는, 상기한 빠짐없이 열거되고 좁게 정의된 세 가지 상황 각각에 대해, 특히 요구를 유발하는 상황의 성격과 그러한 사용이 모든 관계자의 권리와 자유에 미치는 결과, 그리고 사용과 더불어 제공되는 보호 수단 및 조건과 관련하여 특정 요소가 고려되어야 한다는 점을 확실히 명시하는 것이 중요하다. 이와 더불어, 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 데 대해서는, 특히 위협, 피해자 또는 가해자에 관한 증거 또는 징후와 관련하여, 시간과 공간에 적절한 제한이 부과되어야 한다. 개인들의 참조 데이터베이스는 위에 언급한 세 가지 상황에서 각각의 사용 사례에 적절해야 한다.

(21) 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 각각의 경우에 대해 회원국 사법 기관 또는 독립 행정 기관의 명시적이고 구체적인 허가를 받아야 한다. 이러한 허가는 원칙적으로 사용 전에 획득해야 한다. 단, 적절한 절차에 따라 정당화되는 긴급 상황, 즉 문제의 시스템을 사용해야 할 필요성이 긴급하여 사용을 개시하기 전에 허가를 획득하는 것이 실질적·객관적으로 불가능한 상황은 예외로 한다. 이러한 긴급 상황에서, 사용은 절대적으로 필요한 최소한도로 제한되고 국가 법률이 규정하고 법 집행 기관이 자체적으로 각각의 긴급 사용 사례의 맥락에서 명시하는 적절한 보호 수단 및 조건이 적용되어야 한다. 아울러, 그러한 상황에서 법 집행 기관은 가능한 한 신속히 허가를 획득하고 더 빨리 허가를 요청할 수 없었던 이유를 밝혀야 한다.

(22) 나아가, 본 규정이 설정한 완전한 프레임워크 내에서 문제의 회원국이 국내 법의 세칙에 그러한 사용을 허가할 수 있음을 명시하는 경우에 한해서만 본 규정에 따라 회원국의 영토에서 그러한 시스템을 사용할 수 있다는 것을

[38] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation.

(23) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should only be possible in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In this context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive 2016/680. However, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to it.

(24) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, including where those systems are used by competent authorities in publicly accessible spaces for other purposes than law enforcement, should continue to comply with all requirements resulting from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680, as applicable.

(25) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), point (d), (2) and (3) of this Regulation adopted on the basis of Article 16 of the TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 of the TFEU.

(26) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and TFEU, Denmark is not bound by rules laid down in Article 5(1), point (d), (2) and (3) of this Regulation adopted on the basis of Article 16 of the TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

규정하는 것이 적절하다. 따라서 회원국은 본 규정에 따라 자유롭게 그러한 가능성을 전폭적으로 규정하거나, 또는 단지 본 규정에서 확인된 허가된 사용을 정당화할 수 있는 일부 목표와 관련해서만 그러한 가능성을 규정할 수 있다.

(23) 법 집행 목적으로 공개적으로 접근 가능한 공간에서 자연인의 '실시간' 원격 생체 인식을 위해 AI 시스템을 사용하는 것은 필연적으로 생체 인식 데이터의 처리를 수반한다. TFEU 제16조에 의거하여 특정한 예외를 제외하고 그러한 사용을 금지하는 본 규정의 규칙은 Directive (EU) 2016/680 제10조에 포함된 생체 인식 데이터의 처리에 관한 규칙과 관련하여 *특별법(lex specialis)*으로 적용되어야 하며, 따라서 관련 생체 인식 데이터의 사용 및 처리를 철저하게 규제해야 한다. 따라서 그러한 사용 및 처리는 오직 본 규정에 의해 설정된 프레임워크와 부합하는 경우에 한해서만 가능해야 하며, 해당 프레임워크를 벗어나서, 법 집행 목적으로 행동하는 관할 기관이 Directive (EU) 2016/680 제10조에 열거된 근거 하에 그와 관련하여 시스템을 사용하고 데이터를 처리할 수 있는 여지가 없어야 한다. 이러한 맥락에서, 본 규정은 Directive 2016/680 제8조에 따른 개인 데이터의 처리를 위한 법적 근거를 제공하기 위한 것이 아니다. 단, 관할 기관을 포함하여, 법 집행 이외의 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 것은 본 규정에 의해 설정된 법 집행 목적의 사용과 관련한 특정 프레임워크에 포함될 수 없다. 따라서 법 집행 이외의 목적으로 사용할 경우 본 규정 및 그에 효력을 부여할 수 있는 적용 가능한 국내 법의 세칙에 따른 허가 요건항이 적용되지 않는다.

(24) 관할 기관이 법 집행 이외의 목적으로 공개적으로 접근 가능한 공간에서 해당 시스템을 사용하는 경우를 포함하여, 본 규정이 적용되는 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 경우 외에, 생체 인식을 위한 AI 시스템 사용에 수반되는 생체 인식 데이터 및 기타 개인 데이터의 처리는 상황에 따라 Regulation (EU) 2016/679 제9(1)조, Regulation (EU) 2018/1725 제10(1)조 및 Directive (EU) 2016/680 제10조에서 비롯되는 모든 요구사항을 계속 준수해야 한다.

(25) TEU와 TFEU에 부속된, 자유 안전 사법 지대와 관련한 영국과 아일랜드의 지위에 관한 Protocol No 21 제6a조에 따라, 아일랜드는 회원국이 TFEU 제3부 제5편 제4장 또는 제5장의 범위 내에 속하는 활동을 수행할 때 개인 데이터를 처리하는 데 관한 TFEU 제16조를 근거로 채택된 본 규정의 제5(1)조 (d)항, (2) 및 (3)조에 명시된 규칙에 구속되지 않으며, TFEU 제16조를 근거로 명시된 조항의 준수를 요구하는, 범죄 문제에 대한 사법 협력 또는 경찰 협력의 형태를 지배하는 규칙에 구속되지 않는다.

(26) TEU와 TFEU에 부속된, 덴마크의 지위에 관한 Protocol No 22 제2조 및 2a조에 따라, 덴마크는 회원국이 TFEU 제3부 제5편 제4장 또는 제5장의 범위 내에 속하는 활동을 수행할 때 개인 데이터를 처리하는 데 관한 TFEU 제16조를 근거로 채택된 본 규정의 제5(1)조 (d)항, (2) 및 (3)조에 명시된 규칙에 구속되거나 그 적용을 받지 않는다.

(27) High-risk AI systems should only be placed on the Union market or put into service if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any.

(28) AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as components of products. Consistently with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, and non-discrimination, consumer protection, workers' rights, rights of persons with disabilities, right to an effective remedy and to a fair trial, right of defence and the presumption of innocence, right to good administration. In addition to those rights, it is important to highlight that children have specific rights as enshrined in Article 24 of the EU Charter and in the United Nations Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.

(29) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council[39], Regulation (EU) No 167/2013 of the European Parliament and of the Council[40], Regulation (EU) No 168/2013 of the European Parliament and of the Council[41], Directive 2014/90/EU of

[39] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

[40] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

[41] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

(27) 고위험 AI 시스템은 특정한 필수 요건을 준수하는 경우에만 유럽 연합 시장에 출시 또는 서비스 개시되어야 한다. 이러한 요건은 유럽 연합에서 이용 가능하거나 그 결과물이 유럽 연합에서 사용되는 고위험 AI 시스템이 유럽 연합법에 의해 인정되고 보호되는 유럽 연합의 중요한 공익에 용납할 수 없는 위험을 초래하지 않도록 보장해야 한다. 고위험으로 식별된 AI 시스템은 유럽 연합 시민의 건강, 안전 및 기본권에 중대한 피해를 주는 시스템으로 제한되어야 하며 이러한 제한은 국제 무역에 대한 잠재적 제약(있을 경우)을 최소화한다.

(28) AI 시스템은 특히 그러한 시스템이 제품의 구성요소로 작동할 경우 개인의 건강과 안전에 부정적 결과를 초래할 수 있다. 역내 시장에서 제품의 자유로운 이동을 촉진하고 오직 안전하고 규정을 준수하는 제품만이 출시되도록 보장하기 위한 유럽 연합 조화 법령의 목표에 따라, AI 시스템을 포함한 디지털 구성요소로 인해 제품 전체에 의해 초래될 수 있는 안전 위험을 적절히 방지·완화하는 것이 중요하다. 예를 들어, 자동 로봇은 제조, 활동 보조, 간병 등 다양하고 복잡한 환경에서 안전하게 작동하고 기능을 수행할 수 있어야 한다. 마찬가지로, 생명과 건강에 대한 우려가 특히 높은 의료 부문에서 점점 정교해지는 진단 시스템과 인간의 결정을 돕는 시스템은 신뢰할 수 있고 정확해야 한다. AI 시스템을 고위험으로 분류할 때는 AI 시스템이 헌장에 의해 보호되는 기본권에 미치는 부정적 영향의 정도가 특히 중요하다. 그러한 권리에는 인간의 존엄성, 사생활과 가족 생활의 존중, 개인 데이터의 보호, 표현과 정보의 자유, 집회와 결사의 자유, 차별 금지, 소비자 보호, 노동자의 권리, 장애인의 권리, 효과적인 구제 및 공정한 재판에 대한 권리, 방어권 및 무죄 추정의 원칙, 좋은 행정에 대한 권리 등이 포함된다. 그러한 권리에 더하여, 아동은 아동의 취약성을 고려하고 그들의 행복에 필요한 보호와 보살핌을 제공할 것을 요구하는 EU 헌장 제24조와 UN 아동 권리 협약(디지털 환경에 관한 UNCRC General Comment No. 25에 추가로 상술)에 명시된 특정한 권리를 가진다는 데 유의할 필요가 있다. 개인의 건강 및 안전과 관련된 것을 포함하여 AI 시스템이 초래할 수 있는 피해의 심각성을 평가할 때는 헌장에 명시되고 유럽 연합 정책에 구현된 높은 수준의 환경 보호에 대한 기본권 역시 고려되어야 한다.

(29) 제품 또는 시스템의 안전 구성요소이거나, 그 자체가 유럽 의회 및 유럽 이사회 Regulation (EC) No 300/2008[39], 유럽 의회 및 유럽 이사회 Regulation (EU) No 167/2013[40], 유럽 의회 및 유럽 이사회 Regulation (EU) No 168/2013[41], 유럽 의회 및 유럽 이사회

[39] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

[40] Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

[41] Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

the European Parliament and of the Council[42], Directive (EU) 2016/797 of the European Parliament and of the Council[43], Regulation (EU) 2018/858 of the European Parliament and of the Council[44], Regulation (EU) 2018/1139 of the European Parliament and of the Council[45], and Regulation (EU) 2019/2144 of the European Parliament and of the Council[46], it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant future delegated or implementing acts on the basis of those acts.

(30) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonisation legislation, it is appropriate to classify them as high-risk under this Regulation if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.

(31) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered 'high-risk' under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is notably the case for Regulation (EU) 2017/745 of the European Parliament and of the

---

42 Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

43 Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

44 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

45 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

46 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

Directive 2014/90/EU[42], 유럽 의회 및 유럽 이사회 Directive (EU) 2016/797[43], 유럽 의회 및 유럽 이사회 Regulation (EU) 2018/858[44], 유럽 의회 및 유럽 이사회 Regulation (EU) 2018/1139[45], 유럽 의회 및 유럽 이사회 Regulation (EU) 2019/2144[46] 등의 범위 내에 속하는 제품 또는 시스템인 고위험 AI 시스템과 관련하여, 유럽연합 집행위원회가 해당 규정(act)을 근거로 향후에 관련된 위임 또는 실행 규정(act)을 채택할 때, 각 부문의 기술 및 규제 규격을 근거로 기존의 거버넌스, 적합성 평가 및 집행 메커니즘과 그에 대해 확립된 권한에 개입하지 않고 본 규정에 명시된 고위험 AI 시스템에 대한 필수 요건을 고려하도록 보장하기 위해 해당 규정(act)을 개정하는 것이 적절하다.

(30) 제품 또는 시스템의 안전 구성요소이거나, 그 자체가 특정한 유럽 연합 조화 법령의 범위 내에 속하는 제품인 고위험 AI 시스템과 관련하여, 문제의 제품이 해당 유럽 연합 조화 법령에 따라 제3자 적합성 평가 기관의 적합성 평가 절차를 거치는 경우 이를 본 규정에 따른 고위험으로 분류하는 것이 적절하다. 특히, 그러한 제품은 기계류, 장난감, 리프트, 폭발 위험 환경에서 사용하는 장비 및 보호 시스템, 무선 장치, 압력 장치, 레저 선박 장비, 삭도 설비, 가스 기기, 의료 기기, 체외 진단 의료 기기 등이다.

(31) 본 규정에 따라 특정 AI 시스템을 고위험으로 분류한다고 해서 반드시 AI 시스템이 안전 구성요소인 제품 또는 제품으로서 AI 시스템 자체가 제품에 적용되는 유럽 연합 조화 법령에 명시된 기준에 따라 '고위험'으로 간주되는 것을 의미하지는 않는다. 이는 특히 중간위험 및 고위험 제품에 대한 제3자 적합성 평가를 규정한 유럽 의회 및 유럽 이사회

---

42 Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

43 Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

44 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

45 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

46 Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

Council[47] and Regulation (EU) 2017/746 of the European Parliament and of the Council[48], where a third-party conformity assessment is provided for medium-risk and high-risk products.

(32) As regards stand-alone AI systems, meaning high-risk AI systems other than those that are safety components of products, or which are themselves products, it is appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in the Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems.

(33) Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities. Therefore, 'real-time' and 'post' remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight.

(34) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

(35) AI systems used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.

(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects and livelihoods of these persons. Relevant work-related contractual relationships should involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Such persons should in principle not be considered users within the meaning of this Regulation. Throughout the recruitment process and in the

---

47 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

48 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

Regulation (EU) 2017/745[47] 및 유럽 의회 및 유럽 이사회 Regulation (EU) 2017/746[48]의 경우에 해당한다.

(32) 단독형 AI 시스템, 즉 제품의 안전 구성요소가 아니거나 그 자체가 제품인 고위험 AI 시스템과 관련하여, 원래의 목적에 비추어 가능한 피해의 심각성과 발생할 확률을 고려할 때 그것이 개인의 건강과 안전 또는 기본권에 피해를 줄 위험이 높고 본 규정에 명시된 구체적으로 사전 정의된 여러 영역에서 사용되는 경우 이를 고위험으로 분류하는 것이 적절하다. 이러한 시스템의 식별은 고위험 AI 시스템의 향후 수정을 위해 예상되는 것과 동일한 방법론과 기준을 따른다.

(33) 자연인의 원격 생체 인식에 사용되는 AI 시스템의 기술적 부정확성은 편향된 결과로 이어지고 차별적 효과를 수반할 수 있다. 이는 특히 연령, 만족, 성별, 장애 등의 문제와 관련된다. 따라서 '실시간' 및 '사후' 원격 생체 인식 시스템은 고위험으로 분류되어야 한다. 이들이 초래하는 위험에 비추어, 두 가지 유형의 원격 생체 인식 시스템 모두 로깅 기능과 인간의 감독에 관한 특정 요구사항을 충족해야 한다.

(34) 중요한 인프라의 관리 및 운영과 관련하여, 도로 교통, 수도, 가스, 난방, 전기 등에 고장이나 오작동이 발생할 경우 사람들의 생명과 건강에 대규모의 위험을 초래하고 일상적인 사회·경제 활동의 수행에 큰 혼란을 일으킬 수 있으므로 그 관리와 운영을 위한 안전 구성요소로 사용되는 AI 시스템을 고위험으로 분류하는 것이 적절하다.

(35) 교육 또는 직업 훈련에서, 특히 교육 기관과 직업 훈련 기관에 대한 접근을 결정하거나 교육의 일부 또는 전제 조건으로 개인을 테스트·평가하는 데 사용되는 AI 시스템은 개인의 삶에서 교육과 직업의 경로를 결정하고 따라서 생계를 유지하는 능력에 영향을 미칠 수 있으므로 고위험으로 간주되어야 한다. 이러한 시스템이 부적절하게 설계되고 사용될 경우 교육 및 훈련에 대한 권리와 차별당하지 않을 권리를 침해하고 차별의 역사적 패턴을 영속화할 수 있다.

(36) 고용, 노무 관리, 자영업에 대한 접근, 특히 인력의 채용과 선발, 승진과 해고에 대한 결정, 업무 할당, 모니터링 또는 업무 관련 계약 관계에서 개인의 평가 등에 사용되는 AI 시스템 역시 당사자들의 미래 직업 전망과 생계에 현저한 영향을 미칠 수 있으므로 고위험으로 분류되어야 한다. 업무 관련 계약 관계에는 2021년 유럽연합 집행위원회 업무 프로그램(Commission Work Programme 2021)에 언급된 플랫폼을 통해 서비스를 제공하는 사람들과 직원들이 참여해야 한다. 이러한 사람들은 원칙적으로 본 규정의 의미 내에서 사용자로 간주되지 않는다. 채용 과정 전반에 걸쳐, 그리고 업무 관련 계약 관계에서 사람들의 평가, 승진, 유지 측면에서 이러한 시스템은 예컨대 여성, 연령 집단, 장애인,

---

47 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1).

48 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of these persons may also impact their rights to data protection and privacy.

(37) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts. Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by small-scale providers for their own use. Natural persons applying for or receiving public assistance benefits and services from public authorities are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non- discrimination, human dignity or an effective remedy. Those systems should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

(38) Actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high quality data, does not meet adequate requirements in terms of its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities in question and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by law

인종/민족 또는 성적 지향에 따른 차별의 역사적 패턴을 영속화할 수 있다. 이러한 사람들의 업무 수행과 행동을 모니터하는 데 사용되는 AI 시스템 역시 개인정보보호에 대한 그들의 권리에 영향을 미칠 수 있다.

(37) AI 시스템의 사용에 대해 특별한 고려가 필요한 또 다른 영역으로, 사람들이 사회에 적극적으로 참여하거나 생활 수준을 개선하는 데 필수적인 민간/공공 서비스 및 편익에 대한 접근과 향유를 들 수 있다. 특히, 자연인의 신용 평점 또는 신뢰성을 평가하는 데 사용되는 AI 시스템은 금융 자원 또는 주택, 전기, 통신 등 필수 서비스에 대한 접근 여부를 결정하므로 고위험 AI 시스템으로 분류되어야 한다. 이러한 목적으로 사용되는 AI 시스템은 개인 또는 집단의 차별로 이어질 수 있고, 예컨대 인종/민족, 장애, 연령, 성적 지향 등에 따른 차별의 역사적 패턴을 영속화하거나 새로운 형태의 차별 효과를 유발할 수 있다. 소규모 제공자가 신뢰성 및 신용 평가 목적의 AI 시스템을 자체적인 용도로 서비스 개시(put into service)하는 경우에는, 영향의 매우 제한적인 규모와 시장에서 가용한 대안을 고려하여 면제하는 것이 적절하다. 공공 부조와 공공 기관의 서비스를 신청하거나 받는 자연인은 일반적으로 그러한 보조금과 서비스에 의존하며 담당 기관에 대해 취약한 위치에 놓인다. 담당 기관이 그러한 보조금과 서비스를 거절, 삭감, 취소 또는 환수해야 할지 여부를 결정하는 데 AI 시스템을 사용하는 경우, 이는 개인의 생계에 중대한 영향을 미칠 수 있고 사회적 보호, 차별 금지, 인간적 존엄성, 효과적 구제 등에 대한 권리를 비롯한 기본권을 침해할 수 있다. 따라서 이러한 시스템은 고위험으로 분류되어야 한다. 그럼에도 불구하고 본 규정은, 법인과 자연인에게 고위험을 초래하지 않는 적법하고 안전한 AI 시스템의 폭넓은 사용으로 혜택을 입을 수 있는 행정 분야에서 혁신적인 접근법의 개발과 사용을 방해해서는 안 된다. 끝으로, 응급 처치(Emergency First Response) 서비스의 파견 또는 그 우선순위를 설정하는 데 사용되는 AI 시스템 역시 개인의 생명과 건강 및 재산을 지키는 데 매우 중요한 상황에서 의사결정을 내리므로 고위험으로 분류되어야 한다.

(38) AI 시스템의 사용을 수반하는 법 집행 기관의 행동은 높은 수준의 권력 불균형을 수반하며, 자연인의 감시, 체포 또는 자유 박탈로 이어지거나 헌장에서 보장하는 기본권에 그 밖의 부작용을 초래할 수 있다. 특히, AI 시스템이 고품질 데이터를 통해 학습되지 않거나, 정확성 또는 견고성 측면에서 적절한 요구사항을 충족하지 않거나, 출시 또는 서비스 개시되기 전에 적절히 설계·테스트되지 않을 경우, 차별적이거나 부정확하거나 부당한 방식으로 사람을 식별해 낼 수 있다. 뿐만 아니라 이러한 AI 시스템이 충분히 투명하고 설명 가능하고 기록되지 않을 경우, 효과적 구제와 공정한 재판에 대한 권리 및 방어권과 무죄 추정의 원칙 등 중요한 절차적 기본권의 행사를 방해할 있다. 따라서 부정적 영향을 방지하고, 공공의 신뢰를 유지하고, 책무성과 효과적 구제를 보장하기 위해 정확성, 신뢰성, 투명성이 특히 중요한 법 집행 맥락에서 사용되는 다수의 AI 시스템을 고위험으로 분류하는 것이 적절하다. 해당 활동의 성격과 그에 관련된 위험에 비추어, 이러한 고위험 AI 시스템에는

enforcement authorities for individual risk assessments, polygraphs and similar tools or to detect the emotional state of natural person, to detect 'deep fakes', for the evaluation of the reliability of evidence in criminal proceedings, for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons, or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences, as well as for crime analytics regarding natural persons. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.

(39) AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non- discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council[49], the Regulation (EC) No 810/2009 of the European Parliament and of the Council[50] and other relevant legislation.

(40) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts. Such qualification should not extend, however, to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks or allocation of resources.

---

[49] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

[50] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

법 집행 기관이 개인 위험 평가, 거짓말 탐지기 및 유사한 도구를 사용한 자연인의 감정 상태 탐지, '딥 페이크' 탐지, 형사 소송에서 증거의 신뢰성 평가, 자연인 프로파일링에 근거한 실제적·잠재적 범죄 행위의 발생 또는 재발 예측 또는 자연인 및 집단의 성격 특성 또는 과거 범죄 행위 평가, 범죄 행위 탐지, 수사 또는 기소 과정의 프로파일링, 자연인에 대한 범죄 분석 등에 사용하는 특정한 AI 시스템이 포함되어야 한다. 세무 및 관세 당국이 행정 절차에 사용하는 AI 시스템은 사법 당국이 범죄 행위의 예방, 탐지, 수사, 기소의 목적으로 사용하는 고위험 AI 시스템으로 간주되어서는 안 된다.

(39) 이주, 망명 및 출입국 관리에 사용되는 AI 시스템은 특히 취약한 위치에 놓여 있고 관할 공공 기관의 조치에 따른 결과에 의존하는 사람들에게 영향을 미친다. 그러므로 이러한 맥락에서 사용되는 AI 시스템의 정확성, 비차별적 성격 및 투명성은 영향을 받는 사람의 기본권 존중, 특히 자유로운 이동, 차별 금지, 사생활과 개인 데이터의 보호, 국제적 보호 및 좋은 행정을 보장하는 데 특히 중요하다. 따라서 이주, 망명 및 출입국 관리 분야의 관할 공공 기관이 거짓말 탐지기 및 유사한 도구를 사용한 자연인의 감정 상태 탐지, 회원국의 영토에 진입하거나 비자 또는 망명을 신청하는 자연인이 초래하는 위험의 평가, 자연인이 제출한 문서의 진위 확인, 지위를 신청하는 자연인의 자격을 확인하기 위해 망명, 비자, 체류 허가 신청을 심사하고 불만 사항을 처리하는 관할 공공 기관의 업무 지원 등을 위해 사용하는 AI 시스템을 고위험으로 분류하는 것이 적절하다. 본 규정이 적용되는 이주, 망명 및 출입국 관리 분야의 AI 시스템은 유럽 의회 및 유럽 이사회 Directive 2013/32/EU[49], 유럽 의회 및 유럽 이사회 Regulation (EC) No 810/2009[50] 및 기타 관련 법규에 명시된 절차적 요건을 준수해야 한다.

(40) 사법 행정과 민주주의 프로세스를 위한 특정 AI 시스템은 민주주의, 법치주의, 개인의 자유, 효과적인 구제와 공정한 재판의 권리 등에 중대한 영향을 미칠 가능성이 있으므로 고위험으로 분류되어야 한다. 특히 잠재적 편향, 오류, 불투명의 위험을 해소하기 위해, 사법 당국이 사실과 법률을 연구·해석하고 법률을 구체적 사실에 적용하는 데 도움을 주는 AI 시스템을 고위험으로 분류하는 것이 적절하다. 하지만 이러한 분류를 예컨대 사법 판결, 문서, 데이터의 익명화 또는 가명화, 직원들 간의 의사소통, 행정 업무, 자원 할당 등의 개별 사례에서 실제 사법 행정에 영향을 주지 않는 순수하게 보조적인 행정 활동을 위한 AI 시스템으로 확장해서는 안 된다.

---

49 Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).

50 Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

(41) The fact that an AI system is classified as high risk under this Regulation should not be interpreted as indicating that the use of the system is necessarily lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant.

(42) To mitigate the risks from high-risk AI systems placed or otherwise put into service on the Union market for users and affected persons, certain mandatory requirements should apply, taking into account the intended purpose of the use of the system and according to the risk management system to be established by the provider.

(43) Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

(44) High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices. Training, validation and testing data sets should be sufficiently relevant, representative and free of errors and complete in view of the intended purpose of the system. They should also have the appropriate statistical properties, including as regards the persons or groups of persons on which the high-risk AI system is intended to be used. In particular, training, validation and testing data sets should take into account, to the extent required in the light of their intended purpose, the features, characteristics or elements that are particular to the specific geographical, behavioural or functional setting or context within which the AI system is intended to be used. In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers shouldbe able to process also special categories of personal data, as a matter of substantial public interest, in order to ensure the bias monitoring, detection and correction in relation to high-risk AI systems.

(45) For the development of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as digital innovation hubs, testing experimentation facilities and researchers, should be able to access and use high quality datasets within their respective fields of activities which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of artificial intelligence algorithms on those datasets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities,

(41) 본 규정에 따라 AI 시스템이 고위험으로 분류된다는 사실은 시스템의 사용이 예컨대 개인 데이터 보호, 거짓말 탐지기 및 유사한 도구 또는 기타 시스템을 사용한 자연인의 감정 상태 탐지 등에 관한 유럽 연합법의 다른 규정 또는 유럽 연합법과 양립되는 국가 법률 하에서 적법하다는 것을 나타내는 것으로 해석되어서는 안 된다. 그러한 사용은 오로지 헌장과 2차 유럽 연합법 및 국가 법률의 관련 규정에서 비롯되는 요구사항에 따라 이루어져야 한다. 본 규정은 적절한 경우 특수한 범주의 개인 데이터를 포함한 개인 데이터의 처리를 위한 법적 근거를 제공하는 것으로 이해되어서는 안 된다.

(42) 유럽 연합 시장에서 출시되거나 서비스 개시되는 고위험 AI 시스템에 따른 위험을 완화하기 위해, 시스템의 사용 목적을 고려하고 제공자가 수립하는 위험 관리 시스템에 따라 특정한 필수 요건이 적용되어야 한다.

(43) 요구사항은 사용되는 데이터세트의 품질, 기술 문서 및 기록 유지, 투명성 및 사용자에 대한 정보 제공, 인간의 감독, 견고성, 정확성, 사이버 보안 등과 관련된 고위험 AI 시스템에 적용되어야 한다. 이러한 요구사항은 시스템의 원래 목적에 비추어 건강, 안전 및 기본권에 대한 위험을 효과적으로 완화하는 데 필요하며, 이보다 약한 다른 무역 제한 조치가 합리적으로 가용하지 않으므로 무역에 대한 부당한 제한을 방지한다.

(44) 고위험 AI 시스템이 의도한 대로 안전하게 기능을 수행하고 유럽 연합법이 금지하는 차별의 원천이 되지 않도록 보장하기 위해서는, 특히 모델의 학습을 수반하는 기법이 사용되는 경우 높은 데이터 품질을 확보하는 것이 AI 시스템의 성능에 필수적이다. 높은 품질의 학습, 검증, 테스트 데이터세트는 적절한 데이터 거버넌스 및 관리 체계의 시행을 요구한다. 학습, 검증, 테스트 데이터세트는 충분히 관련성과 대표성이 있고, 오류가 없고, 시스템의 원래 목적에 비추어 완전해야 한다. 이는 또한 고위험 AI 시스템을 사용하게 될 개인 또는 집단에 관한 것을 포함하여 적절한 통계적 속성을 보유해야 한다. 특히, 학습, 검증, 테스트 데이터세트는 원래의 목적에 비추어 요구되는 한에서 AI 시스템이 사용되는 특정한 지리적, 행동적, 기능적 환경 또는 맥락에 특유한 특성 또는 요소를 고려해야 한다. AI 시스템의 편향성에 비롯되는 차별로부터 타인의 권리를 보호하기 위해서는 제공자가 고위험 AI 시스템과 관련된 편향성 모니터링, 탐지, 시정을 보장하기 위한 실질적 공익의 문제로 특별한 범주의 개인 데이터를 처리할 수 있어야 한다.

(45) 고위험 AI 시스템의 개발을 위해서는 제공자, 인증 기관 및 디지털 혁신 허브, 테스트/실험 시설, 연구자 등 기타 관련 실체를 포함한 특정 행위자가 본 규정과 관련된 각자의 활동 분야 내에서 고품질 데이터세트를 접근하고 사용할 수 있어야 한다. 유럽연합 집행위원회가 설립한 유럽 공동 데이터 공간(European common data spaces)과 공익을 위한 기업간 및 정부와의 데이터 공유는 AI 시스템의 학습, 검증, 테스트를 위한 고품질 데이터를 신뢰할 수 있고 책임 있고 비차별적인 방식으로 접근하는 데 중요하다. 일례로 보건 분야에서 유럽 보건 데이터 공간(European health data space)은 개인정보를 보호하고, 안전하며, 시기 적절하고 투명하며, 신뢰할 수 있는 방식으로, 그리고 적절한 제도적 거버넌스를 통해, 보건 데이터에 대한 비차별적 접근과 그러한 데이터세트에 대한 인공 지능 알고리즘의 학습을 촉진할 것이다. 데이터에 대한 접근을

including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

(46) Having information on how high-risk AI systems have been developed and how they perform throughout their lifecycle is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date.

(47) To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.

(48) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.

(49) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art. The level of accuracy and accuracy metrics should be communicated to the users.

(50) The technical robustness is a key requirement for high-risk AI systems. They should be resilient against risks connected to the limitations of the system (e.g. errors, faults, inconsistencies, unexpected situations) as well as against malicious actions that may compromise the security of the AI system and result in harmful or otherwise undesirable behaviour. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

(51) Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

제공하거나 지원하는 부분별 기관을 포함한 관련 관할 기관 역시 AI 시스템의 학습, 검증, 테스트를 위한 고품질 데이터의 제공을 지원할 수 있다.

(46) 본 규정에 따른 요구사항의 준수 여부를 확인하기 위해서는 고위험 AI 시스템이 어떻게 개발되고 라이프사이클 전반에 걸쳐 어떻게 작동하는지에 관한 정보를 확보하는 것이 필수적이다. 이는 AI 시스템이 관련 요구사항을 준수하는지 여부를 평가하는 데 필요한 정보를 포함하는 기술 문서와 기록의 보존을 요구한다. 이러한 정보에는 시스템의 일반적 특성과 기능 및 제약, 사용되는 알고리즘, 데이터, 학습, 테스트 및 검증 프로세스, 그리고 위험 관리 시스템에 관한 문서 기록 등이 포함되어야 한다. 기술 문서는 최신으로 유지되어야 한다.

(47) 특정 AI 시스템을 자연인이 이해할 수 없거나 너무 복잡하게 만들 수 있는 불투명성을 해소하기 위해, 고위험 AI 시스템에 대해 일정 수준의 투명성이 요구된다. 사용자는 시스템 아웃풋을 해석하고 적절히 사용할 수 있어야 한다. 따라서 고위험 AI 시스템에는 관련 문서와 사용 지침이 수반되어야 하며 기본권 침해 및 차별의 위험과 관련된 것을 포함한 간결하고 명확한 정보가 수반되어야 한다.

(48) 고위험 AI 시스템은 자연인이 그 기능을 감독할 수 있는 방식으로 설계되고 개발되어야 한다. 이러한 목적을 위해 시스템 제공자는 시스템이 출시되거나 서비스 개시되기 전에 적절한 인간의 감독 수단을 확보해야 한다. 특히 그러한 수단은 시스템이 스스로 재정의할 수 없게 만드는 내부 작동의 제약이 있어야 하며, 인간 운영자에 응답을 받도록 보장하고, 감독 임무를 부여받은 자연인이 그러한 임무를 수행하는 데 필요한 교육과 권한을 제공해야 한다.

(49) 고위험 AI 시스템은 라이프사이클 전반에 걸쳐 일관성 있게 작동해야 하며, 일반적으로 인정되는 첨단 기술에 따라 적절한 수준의 정확성, 견고성 및 사이버 보안 기준을 충족해야 한다. 정확성 수준과 정확성 척도를 사용자에게 고지해야 한다.

(50) 기술적 견고성은 고위험 AI 시스템을 위한 핵심적 요구사항이다. 이는 시스템의 제약(오류, 고장, 비일관성, 예기치 않은 상황 등)과 관련된 위험과, AI 시스템의 보안을 훼손하고 유해하거나 바람직하지 않은 작동을 초래할 수 있는 악의적 행위에 대해 복원력을 가져야 한다. 이러한 위험에 제대로 대처하지 못하면, 예컨대 AI 시스템이 잘못된 결정을 내리거나 편향된 결과를 산출하여 안전을 저해하거나 기본권에 부정적 효과를 미칠 수 있다.

(51) 사이버 보안은 AI 시스템의 취약성을 이용하여 그 사용, 기능, 작동을 변경하거나 보안 속성을 훼손하려는 악의적 제3자의 시도에 대해 시스템이 복원력을 가지도록 보장하는 데 중요한 역할을 한다. AI 시스템에 대한 사이버 공격은 학습 데이터세트(예: 데이터 오염), 학습된 모델(예: 적대적 공격), 또는 AI 시스템의 디지털 자산 또는 기본 ICT 인프라의 취약성 이용 등 AI 특유의 자산을 활용할 수 있다. 따라서, 위험에 적합한 수준의 사이버 보안을 보장하려면 고위험 AI 시스템의 제공자가 기본 ICT 인프라를 고려하여 적합한 조치를 취해야 한다.

(52) As part of Union harmonisation legislation, rules applicable to the placing on the market, putting into service and use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council[51] setting out the requirements for accreditation and the market surveillance of products, Decision No 768/2008/EC of the European Parliament and of the Council[52] on a common framework for the marketing of products and Regulation (EU) 2019/1020 of the European Parliament and of the Council[53] on market surveillance and compliance of products ('New Legislative Framework for the marketing of products').

(53) It is appropriate that a specific natural or legal person, defined as the provider, takes the responsibility for the placing on the market or putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

(54) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority in question.

(55) Where a high-risk AI system that is a safety component of a product which is covered by a relevant New Legislative Framework sectorial legislation is not placed on the market or put into service independently from the product, the manufacturer of the final product as defined under the relevant New Legislative Framework legislation should comply with the obligations of the provider established in this Regulation and notably ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

(56) To enable enforcement of this Regulation and create a level-playing field for operators, and taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative established in the Union.

(57) In line with New Legislative Framework principles, specific obligations for relevant economic operators, such as importers and distributors, should be set to ensure legal certainty and facilitate regulatory compliance by those relevant operators.

---

51 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

52 Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

53 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169, 25.6.2019, p. 1–44).

(52) 유럽 연합 조화 법령의 일부로, 제품의 인가(accreditation) 및 시장 감시를 위한 요구사항을 명시한 유럽 의회 및 유럽 이사회 Regulation (EC) No 765/2008[51], 제품의 마케팅을 위한 공동 프레임워크에 관한 유럽 의회 및 유럽 이사회 Decision No 768/2008/EC[52], 제품의 시장 감시 및 규정 준수에 관한 유럽 의회 및 유럽 이사회 Regulation (EU) 2019/1020[53]('제품의 마케팅을 위한 새로운 입법 프레임워크(NLF)') 등과 일치하는 고위험 AI 시스템의 출시, 서비스 개시 및 사용에 적용되는 규칙이 제정되어야 한다.

(53) 제공자가 정의하는 특정 자연인 또는 법인이 시스템을 설계하거나 개발했는지 여부에 관계없이 고위험 AI 시스템의 출시 또는 서비스 개시에 대해 책임을 지는 것이 적절하다.

(54) 제공자는 견실한 품질 관리 시스템을 구축하고, 필요한 적합성 평가 절차를 확립하고, 관련 문서를 작성하고, 견실한 출시 후 모니터링 시스템을 구축해야 한다. 자체적으로 사용하기 위해 고위험 AI 시스템을 서비스 개시(put into service)하는 공공 기관은 부문의 특수성과 당 기관의 권한 및 조직을 고려하여 국가 또는 지역 수준에서 채택하는 품질 관리 시스템의 일부로 품질 관리 시스템을 위한 규칙을 채택하고 시행할 수 있다.

(55) 관련 NLF 부분별 법규가 적용되는 제품의 안전 구성요소인 고위험 AI 시스템이 제품과 독립적으로 출시 또는 서비스 개시되지 않는 경우, 관련 NLF 법규에 따라 정의되는 최종 제품의 제조업체는 본 규정에 명시된 제공자의 의무를 준수하고 최종 제품에 임베드된 AI 시스템이 본 규정의 요구사항을 준수하도록 보장해야 한다.

(56) 디지털 제품이 제공되는 다양한 형태를 고려할 때, 본 규정의 집행을 지원하고 운영자들을 위해 공평한 경쟁의 장을 확립하기 위해, 어떠한 경우에도 유럽 연합에 소재하는 사람이 AI 시스템의 규정 준수에 관한 모든 필수 정보를 당국에 제공할 수 있도록 보장하는 것이 중요하다. 따라서, 수입업자를 확인할 수 없는 경우 유럽 연합 외부에서 설립된 제공자는 AI 시스템을 유럽 연합에 제공하기 전에 서면 위임(written mandate)을 통해 유럽 연합에 소재하는 공인 대리인을 임명해야 한다.

(57) NLF 원칙에 따라, 법적 확실성을 보장하고 관련 운영자의 규제 준수를 촉진하기 위해 수입업자와 유통업자를 비롯한 관련 운영자에 대한 구체적 의무가 명시되어야 한다.

---

51 Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

52 Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

53 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169, 25.6.2019, p. 1–44).

(58) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regard the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for users. Users should in particular use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate.

(59) It is appropriate to envisage that the user of the AI system should be the natural or legal person, public authority, agency or other body under whose authority the AI system is operated except where the use is made in the course of a personal non- professional activity.

(60) In the light of the complexity of the artificial intelligence value chain, relevant third parties, notably the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services, should cooperate, as appropriate, with providers and users to enable their compliance with the obligations under this Regulation and with competent authorities established under this Regulation.

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council[54] should be a means for providers to demonstrate conformity with the requirements of this Regulation. However, the Commission could adopt common technical specifications in areas where no harmonised standards exist or where they are insufficient.

(62) In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

(63) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation following the New Legislative Framework approach, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already foreseen under that legislation. The applicability of the requirements of this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant specific New Legislative Framework legislation. This approach is fully reflected in the interplay between this Regulation and the [Machinery Regulation]. While safety risks of AI systems ensuring safety functions in machinery are addressed by the requirements of this Regulation, certain specific requirements in the [Machinery Regulation] will ensure the safe integration of the AI system into the overall machinery, so as not to compromise the safety of the machinery as a whole.

---

[54] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(58) 실제 환경에서 AI 시스템의 성능을 적절히 모니터링할 필요성을 포함하여, AI 시스템의 성격 및 그 사용과 관련된 안전 및 기본권에 대한 위험을 감안할 때, 사용자에 대한 구체적 책임을 명시하는 것이 적절하다. 사용자는 특히 사용 지침에 따라 고위험 AI 시스템을 사용해야 하며, AI 시스템의 기능에 대한 모니터링 및 기록 유지와 관련된 그 밖의 특정한 의무가 규정되어야 한다.

(59) AI 시스템이 개인의 비전문적 활동에 사용되는 경우를 제외하고, AI 시스템의 사용자가 그 권한에 따라 AI 시스템이 운영되는 자연인 또는 법인, 공공 기관, 기구 또는 기타 단체일 것으로 예상하는 것이 타당하다.

(60) 인공 지능 가치 사슬의 복잡성에 비추어, 관련 제3자, 특히 소프트웨어, 소프트웨어 도구 및 구성요소, 사전 학습된 모델 및 데이터의 판매와 공급에 관여하는 제3자 또는 네트워크 서비스 제공자는 적절한 경우 본 규정에 따른 의무 준수를 보장하기 위해 제공자 및 사용자들과 협력하고 본 규정에 따라 설립된 관할 당국과도 협력해야 한다.

(61) 표준화는 본 규정의 준수를 보장하기 위해 제공자에게 기술 솔루션을 제공하는 데 핵심적인 역할을 수행해야 한다. 유럽 의회 및 유럽 이사회 Regulation (EU) No 1025/2012[54]에 정의된 조화 표준의 준수는 제공자가 본 규정의 요구사항에 따른다는 것을 입증하는 수단이 되어야 한다. 단, 유럽연합 집행위원회는 조화 표준이 존재하지 않거나 불충분한 분야에서 공통 기술 규격을 채택할 수 있다.

(62) 고위험 AI 시스템에 대해 높은 수준의 신뢰성을 보장하기 위해, 시스템을 출시 또는 서비스 개시하기 전에 적합성 평가를 실시해야 한다.

(63) 운영자의 부담을 최소화하고 가능한 중복을 방지하기 위해, NLF 접근법에 따른 기존의 유럽 연합 조화 법령이 적용되는 제품과 관련된 고위험 AI 시스템에 대해, 해당 법규에 따라 이미 예정된 적합성 평가의 일부로 해당 AI 시스템이 본 규정의 요구사항을 준수하는지 여부를 평가하는 것이 적절하다. 그러므로 본 규정의 요구사항이 적용된다는 사실이 관련 NLF 법규에 따른 적합성 평가의 특정한 논리, 방법론 또는 일반적 구조에 영향을 주어서는 안 된다. 이 접근법은 본 규정과 [기계류 규정(Machinery Regulation)] 간의 상호작용에 충분히 반영된다. 기계류의 안전 기능을 보장하는 AI 시스템의 안전 위험은 본 규정의 요구사항에 의해 해소되지만, [기계류 규정]의 특정 요구사항은 AI 시스템이 기계류에 안전하게 통합되어 기계류 전체의 안전을 훼손하지 않도록 보장한다.

---

54 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

The [Machinery Regulation] applies the same definition of AI system as this Regulation.

(64) Given the more extensive experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

(65) In order to carry out third-party conformity assessment for AI systems intended to be used for the remote biometric identification of persons, notified bodies should be designated under this Regulation by the national competent authorities, provided they are compliant with a set of requirements, notably on independence, competence and absence of conflicts of interests.

(66) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that an AI system undergoes a new conformity assessment whenever a change occurs which may affect the compliance of the system with this Regulation or when the intended purpose of the system changes. In addition, as regards AI systems which continue to 'learn' after being placed on the market or put into service (i.e. they automatically adapt how functions are carried out), it is necessary to provide rules establishing that changes to the algorithm and its performance that have been pre-determined by the provider and assessed at the moment of the conformity assessment should not constitute a substantial modification.

(67) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

(68) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons and the protection of industrial and commercial property, Member States could authorise the placing on the market or putting into service of AI systems which have not undergone a conformity assessment.

(69) In order to facilitate the work of the Commission and the Member States in the artificial intelligence field as well as to increase the transparency towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, should be required to register their high-risk AI system in a EU database, to be established and managed by the Commission. The Commission should be the controller of that database, in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the

[기계류 규정]은 AI 시스템에 대해 본 규정과 동일한 정의를 적용한다.

(64) 제품 안전 분야에서 전문 프리마켓 인증자(pre-market certifier)의 풍부한 경험과 수반되는 위험의 다양한 성격을 감안할 때, 적어도 본 규정을 적용하는 초기 단계에는 제품과 관련된 것 이외의 고위험 AI 시스템에 대한 제3자 적합성 평가의 적용 범위를 제한하는 것이 적절하다. 따라서, 그러한 시스템의 적합성 평가는 원칙적으로 제공자가 자기 책임 하에 수행해야 한다. 단, 인증 기관이 적합성 평가에 관여할 것으로 예상되는, 개인의 원격 생체 인식에 사용되는 AI 시스템은 (그것이 금지되지 않는 한) 예외로 한다.

(65) 개인의 원격 생체 인식에 사용할 AI 시스템에 대한 제3자 적합성 평가를 수행하기 위해, 국가 관할 당국은 본 규정에 따라 인증 기관을 지명해야 한다. 단, 동 인증 기관은 특히 독립성, 권한 및 이해 충돌의 부재에 관한 일련의 요구사항을 준수해야 한다.

(66) 유럽 연합 조화 법령에 의해 규제되는 제품의 상당한 개조에 대해 일반적으로 확립된 개념에 따라, 시스템의 본 규정 준수에 영향을 줄 수 있는 변경이 발생하거나 시스템의 원래 목적이 변경될 경우 AI 시스템에 대해 새로운 적합성 평가를 실시하는 것이 적절하다. 이와 더불어, 출시 또는 서비스 개시된 후에도 '학습'을 계속하는(즉, 기능이 수행되는 방식에 자동으로 적응하는) AI 시스템과 관련하여, 제공자에 의해 사전 결정되고 적합성 평가 시에 평가된 알고리즘과 성능의 변경이 상당한 개조를 구성하지 않는다는 점을 명시하는 규칙을 제공할 필요가 있다.

(67) 고위험 AI 시스템은 역내 시장 내에서 자유로이 이동할 수 있도록 본 규정의 준수를 나타내는 CE 마크를 부착해야 한다. 회원국은 본 규정에 명시된 요구사항을 준수하고 CE 마크를 부착한 고위험 AI 시스템의 출시 또는 서비스 개시에 부당한 장애를 초래해서는 안 된다.

(68) 특정한 조건 하에서는 개인의 건강과 안전 및 사회 전체를 위해 혁신적인 기술을 신속하게 도입하는 것이 중요할 수 있다. 따라서, 공공 안전 또는 자연인의 생명과 건강의 보호 및 산업 및 상업용 재산의 보호를 요하는 예외적 상황에서는 회원국이 적합성 평가를 거치지 않은 AI 시스템의 출시 또는 서비스 개시를 허가할 수 있도록 하는 것이 적절하다.

(69) 인공 지능 분야에서 유럽연합 집행위원회와 회원국의 업무를 촉진하고 일반에 대한 투명성을 증대하기 위해, 기존 유럽 연합 조화 법령의 범위 내에 속하는 제품과 관련된 것을 제외한 고위험 AI 시스템의 제공자는 각자의 유럽연합 집행위원회가 구축하고 관리하는 EU 데이터베이스에 고위험 AI 시스템을 등록해야 한다.

Council[55]. In order to ensure the full functionality of the database, when deployed, the procedure for setting the database should include the elaboration of functional specifications by the Commission and an independent audit report.

(70) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, natural persons should be notified when they are exposed to an emotion recognition system or a biometric categorisation system. Such information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin.

(71) Artificial intelligence is a rapidly developing family of technologies that requires novel forms of regulatory oversight and a safe space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that is innovation-friendly, future- proof and resilient to disruption, national competent authorities from one or more Member States should be encouraged to establish artificial intelligence regulatory sandboxes to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service.

(72) The objectives of the regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and Member States legislation; to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, and to accelerate access to markets, including by removing barriers for small and medium enterprises (SMEs) and start-ups. To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. This Regulation should provide the legal basis for the use of personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, in line with Article 6(4) of Regulation (EU) 2016/679, and Article 6 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) of Directive (EU) 2016/680. Participants in the sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting

[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

유럽연합 집행위원회는 유럽 의회 및 유럽 이사회 Regulation (EU) 2018/1725[55]에 따라 상기한 데이터베이스의 관리자(controller)가 되어야 한다. 데이터베이스의 완전한 기능을 보장하기 위해, 데이터베이스를 설정하는 절차에 유럽연합 집행위원회가 작성한 기능 명세서와 독립 감사 보고서가 포함되어야 한다.

(70) 자연인과 상호 작용하거나 콘텐츠를 생성하도록 의도된 특정 AI 시스템은 고위험으로 분류되는지 여부에 관계없이 특정한 가장(impersonation) 또는 기만의 위험을 초래할 수 있다. 따라서 특정 상황에서는 고위험 AI 시스템에 대한 요구사항과 의무를 침해함이 없이, 이러한 시스템의 사용에 대해 특정한 투명성 의무를 부과해야 한다. 특히, 사용의 맥락과 상황으로 미루어 명백한 경우를 제외하고, 자연인이 AI 시스템과 상호 작용하는 경우 이를 당사자에게 고지해야 한다. 나아가, 자연인이 감정 인식 시스템 또는 생체 인식 분류 시스템에 노출되는 경우 이를 당사자에게 고지해야 한다. 이러한 정보 및 고지는 장애인이 접근 가능한 형식으로 제공되어야 한다. 아울러, AI 시스템을 사용하여 기존의 사람, 장소 또는 사건과 현저히 유사하고 마치 진본처럼 보이는 이미지, 오디오 또는 비디오 콘텐츠를 생성하거나 조작하는 사용자는 인공 지능 아웃풋에 적절한 라벨을 표시하고 그 인공적 기원을 밝힘으로써 해당 콘텐츠가 인공적으로 생성 또는 조작되었음을 공개해야 한다.

(71) 인공 지능은 빠르게 발전하는 기술로서, 책임 있는 혁신을 보장하고 적절한 보호 장치 및 위험 완화 수단을 통합하는 새로운 형태의 규제 감독과 안전한 실험 공간을 필요로 한다. 혁신 친화적이고 미래 지향적이며 유사시 복원력이 있는 법적 프레임워크를 보장하기 위해, 하나 이상 회원국의 국가 관할 당국에 대해 이러한 시스템이 출시 또는 서비스 개시되기 전에 엄격한 규제 감독 하에 혁신적인 AI 시스템의 개발과 테스트를 촉진하기 위한 인공 지능 규제 샌드박스를 설정할 것을 장려해야 한다.

(72) 규제 샌드박스의 목적은 혁신적인 AI 시스템이 본 규정과 유럽 연합 및 회원국의 기타 관련 법규를 준수하도록 보장하기 위해 개발 및 프리마케팅(pre-marketing) 단계에 통제된 실험 및 테스트 환경을 구축함으로써 AI의 혁신을 촉진하고, 혁신자들을 위해 법적 확실성을 보장하고, AI 사용에 따른 기회, 위험, 영향에 대한 관할 당국의 이해와 감독을 강화하고, 중소기업과 스타트업을 위해 장벽을 제거하는 일을 포함하여 시장에 대한 접근을 가속화하는 것이 되어야 한다. 유럽 연합 전역에 걸친 균일한 시행과 규모의 경제를 보장하기 위해, 규제 샌드박스의 시행을 위한 공통 규칙과 샌드박스의 감독에 관여하는 기관들 간의 협력을 위한 프레임워크를 확립하는 것이 바람직하다. 본 규정은 Regulation (EU) 2016/679 제6(4)조, Regulation (EU) 2018/1725 제6조에 따라 Directive (EU) 2016/680 제4(2)조를 침해함이 없이, 다른 목적으로 수집한 개인 데이터를 AI 규제 샌드박스 내에서 공익을 위해 특정 AI 시스템을 개발하는 데 사용할 수 있는 법적 근거를 제공해야 한다. 샌드박스의 참여자들은 적절한 보호 수단을 보장하고 관할 당국과 협력해야 한다. 여기에는 그들의 지도에 따르고, 샌드박스 내에서의 개발

[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

expeditiously and in good faith to mitigate any high-risks to safety and fundamental rights that may arise during the development and experimentation in the sandbox. The conduct of the participants in the sandbox should be taken into account when competent authorities decide whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680.

(73) In order to promote and protect innovation, it is important that the interests of small-scale providers and users of AI systems are taken into particular account. To this objective, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Moreover, the specific interests and needs of small-scale providers shall be taken into account when Notified Bodies set conformity assessment fees. Translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, notably those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross- border users.

(74) In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers and notified bodies with their obligations under this Regulation, the AI-on demand platform, the European Digital Innovation Hubs and the Testing and Experimentation Facilities established by the Commission and the Member States at national or EU level should possibly contribute to the implementation of this Regulation. Within their respective mission and fields of competence, they may provide in particular technical and scientific support to providers and notified bodies.

(75) It is appropriate that the Commission facilitates, to the extent possible, access to Testing and Experimentation Facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is notably the case for expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

(76) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation, including on technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to and assisting the Commission on specific questions related to artificial intelligence.

(77) Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority.

(78) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the

및 실험 과정에서 발생할 수 있는 안전과 기본권에 대한 고위험을 완화하기 위해 신속하고 성실하게 행동하는 일이 포함된다. 샌드박스에서 참여자가 취하는 행동은 관할 기관이 Regulation 2016/679 제83(2)조 및 Directive 2016/680 제57조에 따른 과징금을 부과할지 여부를 결정할 때 고려되어야 한다.

(73) 혁신을 촉진하고 보호하기 위해서는 소규모 AI 시스템 제공자 및 사용자의 이익을 특별히 고려하는 것이 중요하다. 이러한 목적을 위해 회원국들은 그러한 운영자들을 대상으로 인식 제고와 정보 전달을 포함한 이니셔티브를 개발해야 한다. 나아가, 인증 기관이 적합성 평가 수수료를 책정할 때 소규모 제공자의 이익과 요구를 고려해야 한다. 의무적인 문서 기록 및 당국과의 의사소통과 관련된 번역 비용은 특히 규모가 작은 제공자와 기타 운영자에게 상당한 부담을 줄 수 있다. 회원국은 관련 제공자의 문서 기록 및 의사소통을 위해 그들이 결정하고 수락하는 언어의 하나가 가능한 최대 수의 국가간 사용자에 의해 널리 이해되는 언어가 되도록 보장해야 한다.

(74) 정보와 전문지식의 부족에서 비롯되는 시행에 대한 위험을 최소화하고 제공자와 인증 기관이 본 규정에 따른 의무를 준수하도록 촉진하기 위해, AI 온디맨드 플랫폼과 유럽 디지털 혁신 허브(European Digital Innovation Hubs) 및 유럽연합 집행위원회와 회원국이 국가 또는 EU 수준에서 설립한 테스트 및 실험 시설은 가능한 한 본 규정의 시행에 기여해야 한다. 이들은 각자의 사명과 권한 분야에서 특별한 과학 및 기술 지원을 제공자와 인증 기관에 제공할 수 있다.

(75) 유럽연합 집행위원회가 가능한 한에서, 관련 유럽 연합 조화 법령에 의거하여 설립되거나 인가되고 동 유럽 연합 조화 법령이 적용되는 제품 또는 장치의 적합성 평가 맥락에서 과업을 이행하는 기구, 그룹 또는 실험실에 대해 테스트 및 실험 시설의 접근을 허용하는 것이 바람직하다. 이는 특히 Regulation (EU) 2017/745 및 Regulation (EU) 2017/746에 따른 의료 기기 분야의 전문가 패널(expert panels), 전문 실험실(expert laboratories) 및 표준 실험실(reference laboratories)에 해당된다.

(76) 본 규정의 원활하고 효과적이며 조화된 시행을 촉진하기 위해 유럽 인공지능 위원회(European Artificial Intelligence Board)를 설립해야 한다. 이 위원회는 본 규정에 명시된 요구사항과 관련된 기술 규격 또는 기존 표준을 포함하여 본 규정의 시행과 관련된 문제에 대해 의견, 권고, 조언 또는 지침을 제공하고 인공 지능과 관련된 특정 문제에 대해 유럽연합 집행위원회에 자문·조력하는 등 여러 가지 자문 업무를 책임져야 한다.

(77) 회원국은 본 규정의 적용과 집행에 핵심적인 역할을 담당한다. 이 점에서 각 회원국은 본 규정의 적용과 시행을 감독하는 목적으로 하나 이상의 국가 관할 당국을 지명해야 한다. 회원국 측에서 조직의 효율성을 증대하고 일반 대중과 회원국 및 유럽 연합 수준의 다른 상대와 접촉하는 공식 연락 지점을 설정하기 위해, 각 회원국에서 하나의 국가 기관을 국가 감독 기관으로 지명해야 한다.

(78) 고위험 AI 시스템의 제공자가 각자의 시스템과 설계 및 개발 프로세스를 개선하기 위해 고위험 AI 시스템의 사용에 관한 경험을 참작하거나 시기 적절한

design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents or any breaches to national and Union law protecting fundamental rights resulting from the use of their AI systems.

(79) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Where necessary for their mandate, national public authorities or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation.

(80) Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the authorities responsible for the supervision and enforcement of the financial services legislation, including where applicable the European Central Bank, should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU of the European Parliament and of the Council[56], it is also appropriate to integrate the conformity assessment procedure and some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on users of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU.

(81) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of trustworthy artificial intelligence in the Union. Providers of non-high-risk AI systems should be encouraged to create codes of conduct intended to foster the voluntary application of the mandatory requirements applicable to high-risk AI systems. Providers should also be encouraged to apply on a voluntary basis additional requirements related, for example, to environmental sustainability, accessibility to persons with disability, stakeholders' participation in the design and development of AI systems, and diversity of the development teams. The Commission may develop initiatives, including of a sectorial

[56] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

방식으로 가능한 시정 조치를 취할 수 있도록 보장하기 위해, 모든 제공자는 출시 후 모니터링 시스템을 구축해야 한다. 이 시스템은 또한 출시 또는 서비스 개시된 후에도 계속해서 '학습'하는 AI 시스템에서 발생할 수 있는 위험이 적시에 효율적으로 해소될 수 있도록 보장하는 데도 중요하다. 이러한 맥락에서, 제공자는 AI 시스템의 사용에서 비롯되는 중대한 사건 또는 기본권을 보호하는 국가 및 유럽 연합 법규의 위반을 관련 당국에 보고하는 시스템을 구축해야 한다.

(79) 유럽 연합 조화 법령인 본 규정에 명시된 요구사항과 의무의 적절하고 효과적인 집행을 보장하기 위해, Regulation (EU) 2019/1020에 의해 수립된 시장 감시 및 제품의 준수를 위한 시스템이 전면적으로 적용되어야 한다. 그 권한을 위해 필요한 경우, 평등 기구를 포함하여 기본권을 보호하는 유럽 연합법의 적용을 감독하는 국가 공공 기관 또는 기구 역시 본 규정에 따라 작성된 모든 문서 기록에 접근할 수 있어야 한다.

(80) 금융 서비스에 관한 유럽 연합 법규에는 AI 시스템을 사용하는 경우를 포함하여 해당 서비스를 제공하는 과정에서 규제 대상 금융 기관에 적용되는 내부 거버넌스 및 위험 관리 규칙 및 요구사항이 포함된다. 본 규정과 유럽 연합 금융 서비스 법규의 관련 규칙 및 요구사항에 따른 의무의 일관성 있는 적용과 집행을 보장하기 위해, 적절한 경우 유럽 중앙은행을 포함하여 금융 서비스 법규의 감독과 집행을 책임지는 기관이, 규제와 감독을 받는 금융 기관이 제공하거나 사용하는 AI 시스템과 관련하여, 시장 감시 활동을 포함한 본 규정의 시행을 감독하는 목적을 위한 관할 당국으로 지명되어야 한다. 본 규정과 유럽 의회 및 유럽 이사회 Directive 2013/36/EU[56]에 따라 규제되는 신용 기관에 적용되는 규칙 간의 일관성을 더욱 향상시키기 위해, 적합성 평가 절차와 위험 관리, 출시 후 모니터링, 문서 기록 등과 관련된 제공자의 절차적 의무 중 일부를 Directive 2013/36/EU에 따른 기존의 의무와 절차에 통합하는 것이 적절하다. 중복을 방지하기 위해, 제공자의 품질 관리 시스템과 고위험 AI 시스템 사용자에게 부과되는 모니터링 의무가 Directive 2013/36/EU에 의해 규제되는 신용 기관에 적용되는 경우 제한적인 개정(derogation)이 이루어져야 한다.

(81) 본 규정의 요구사항에 따른 고위험 AI 시스템 이외의 AI 시스템 개발은 유럽 연합에서 신뢰할 수 있는 인공 지능이 더 널리 수용되는 결과로 이어질 수 있다. 비 고위험 AI 시스템의 제공자가 고위험 AI 시스템에 적용되는 필수 요건의 자발적 적용을 촉진하기 위한 행동 지침을 제정하도록 장려해야 한다. 아울러 제공자가 예컨대 환경의 지속가능성, 장애인의 접근성, AI 시스템의 설계와 개발에 대한 이해관계자의 참여, 개발 팀의 다양성 등과 관련된 추가 요구사항을 자발적으로 적용하도록 장려해야 한다. 유럽연합 집행위원회는 유형이 다른 데이터의 의미론적·기술적 상호운용성과 데이터 접근 인프라를

[56] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

(82) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out herein are nevertheless safe when placed on the market or put into service. To contribute to this objective, the Directive 2001/95/EC of the European Parliament and of the Council[57] would apply as a safety net.

(83) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.

(84) Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement. For certain specific infringements, Member States should take into account the margins and criteria set out in this Regulation. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

(85) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the techniques and approaches referred to in Annex I to define AI systems, the Union harmonisation legislation listed in Annex II, the high-risk AI systems listed in Annex III, the provisions regarding technical documentation listed in Annex IV, the content of the EU declaration of conformity in Annex V, the provisions regarding the conformity assessment procedures in Annex VI and VII and the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[58]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(86) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[59].

(87) Since the objective of this Regulation cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved

---

57 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

58 OJ L 123, 12.5.2016, p. 1.

59 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

포함하여, AI 개발을 위한 데이터의 국가간 교환을 방해하는 기술 장벽을 낮추기 위한 이니셔티브(부문별 이니셔티브를 포함)를 개발할 수 있다.

(82) 본 규정에 따라 고위험이 아니며 따라서 여기에 명시된 요구사항을 준수할 필요가 없는 제품과 관련된 AI 시스템이, 그럼에도 불구하고, 출시되거나 서비스 개시될 경우 안전하게 유지되는 것이 중요하다. 이러한 목적에 기여하기 위해 유럽 의회 및 유럽 이사회 Directive 2001/95/EC[57]가 안전망으로 적용된다.

(83) 유럽 연합 및 국가 수준에서 관할 당국들의 신뢰할 수 있고 건설적인 협력을 보장하기 위해 본 규정의 적용에 관여하는 모든 당사자는 각자의 과업을 수행하는 과정에서 획득한 정보 및 데이터의 기밀성을 보장해야 한다.

(84) 회원국은 위반에 대해 효과적이고 비례적이며 억제적인 처벌을 부과하는 등의 방법으로 본 규정의 조항들이 적절히 시행되도록 보장하는 데 필요한 모든 조치를 취해야 한다. 회원국은 특정한 위반에 대해 본 규정에 명시된 한계와 기준을 고려해야 한다. 유럽 데이터 보호 감독관은 본 규정의 범위 내에 속하는 유럽 연합 기관, 기구, 단체에 벌금을 부과할 수 있는 권한을 가져야 한다.

(85) 필요할 경우 규제 프레임워크를 조정할 수 있도록 보장하기 위해, TFEU 제290조에 따라 법규를 채택할 수 있는 권한을 유럽연합 집행위원회에 위임하여 다음 항목을 개정해야 한다: 부속서 I에 언급된 AI 시스템을 정의하는 기법과 접근법, 부속서 II에 열거된 유럽 연합 조화 법령, 부속서 III에 열거된 고위험 AI 시스템, 부속서 IV에 열거된 기술 문서와 관련된 조항, 부속서 V에 열거된 EU 적합성 선언의 내용, 부속서 VI 및 VII에 열거된 적합성 평가 절차와 관련된 조항, 그리고 품질 관리 시스템의 평가 및 기술 문서의 평가에 근거한 적합성 평가 절차가 적용되어야 하는 고위험 AI 시스템을 규정하는 조항 등. 유럽연합 집행위원회가 준비 작업 과정에서 전문가 수준을 포함한 적절한 협의를 수행하고, 2016년 4월 13일에 발효된 선진 입법(Better Law-Making)을 위한 기구간 협정(Interinstitutional Agreement)[58]에 명시된 원칙에 따라 협의를 진행하는 것이 특히 중요하다. 무엇보다 위임 규정의 준비 과정에 동등한 참여를 보장하기 위해 유럽 의회와 유럽 이사회는 회원국의 전문가들과 동시에 모든 문서를 접수하고, 전문가들은 위임 규정의 준비를 다루는 유럽연합 집행위원회 전문가 그룹의 회의에 체계적으로 접근한다.

(86) 본 규정의 시행을 위해 통일된 조건을 보장하기 위해 유럽연합 집행위원회에 시행 권한이 부여되어야 한다. 이러한 권한은 유럽 의회 및 유럽 이사회 Regulation (EU) No 182/2011[59]에 따라 행사되어야 한다.

(87) 본 규정의 목적은 회원국이 충분히 달성할 수 없고, 조치의 규모 또는 효과의 이유로 유럽 연합 수준에서 보다 원활히 성취될 수 있으므로, 유럽 연합은 TEU

---

57 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

58 OJ L 123, 12.5.2016, p. 1.

59 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p.13).

at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(88) This Regulation should apply from … [*OP – please insert the date established in Art. 85*]. However, the infrastructure related to the governance and the conformity assessment system should be operational before that date, therefore the provisions on notified bodies and governance structure should apply from … [*OP – please insert the date – three months following the entry into force of this Regulation*]. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from [*OP – please insert the date – twelve months following the entry into force of this Regulation*].

(89) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 and delivered an opinion on […]".

HAVE ADOPTED THIS REGULATION:

TITLE I

GENERAL PROVISIONS

Article 1
Subject matter

This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

(a) prohibitions of certain artificial intelligence practices;

(b) specific requirements for high-risk AI systems and obligations for operators of such systems;

(c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;

(d) rules on market monitoring and surveillance.

Article 2
Scope

1. This Regulation applies to:

(a)) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;

(b) users of AI systems located within the Union;

제5조에 명시된 보충성의 원칙에 따른 조치들을 채택할 수 있다. 동일한 조문에 명시된 비례성의 원칙에 따라, 본 규정은 그 목적을 달성하는 데 필요한 것 이상을 요구하지 않는다.

(88) 본 규정은 … [*OP – 제85조에 명시된 날짜 삽입*]부터 적용되어야 한다. 단, 거버넌스 및 적합성 평가 시스템과 관련된 인프라는 상기한 날짜 이전에 운영되어야 하며, 따라서 인증 기관과 거버넌스 구조에 관한 조항은 … [*OP – 날짜 삽입 – 본 규정이 발효된 지 3개월 후*]부터 적용되어야 한다. 아울러, 회원국은 과징금을 포함한 처벌에 관한 규칙을 제정하고 유럽연합 집행위원회에 통지해야 하며, 동 규칙이 본 규정의 적용 날짜에 적절하고 효과적으로 시행되도록 보장해야 한다. 따라서, 처벌에 관한 조항은 [*OP – 날짜 삽입 – 본 규정이 발효된 지 12개월 후*]부터 적용되어야 한다.

(89) Regulation (EU) 2018/1725 제42(2)조에 따라 유럽 데이터 보호 감독관 및 유럽 데이터 보호 이사회와 협의하고 […]에 의견을 전달받았다.

제1편

일반 조항

제1조
주제

본 규정(Regulation)은 다음을 명시한다.

(a) 유럽 연합에서 인공 지능 시스템('AI 시스템)의 출시, 서비스 개시 및 사용을 위한 조화 규칙

(a) 특정한 인공 지능 관행의 금지

(b) 고위험 AI 시스템에 대한 요구사항 및 동 시스템의 운영자에게 부과되는 의무

(c) 자연인, 감정 인식 시스템 및 생체 인식 분류 시스템, 그리고 이미지, 오디오 또는 비디오 콘텐츠를 생성하거나 조작하는 데 사용되는 AI 시스템과 상호 작용하는 AI 시스템에 대한 조화 투명성 규칙

(d) 시장 감시 및 모니터링에 관한 규칙

제2조
범위

1. 본 규정은 다음에 적용된다.

(a) 유럽 연합 내에서 설립되었는지 또는 제3국에서 설립되었는지 여부에 관계없이 유럽 연합에서 AI 시스템을 출시하거나 서비스 개시하는 제공자

(b) 유럽 연합 내에 소재한 AI 시스템 사용자

(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union;

2. For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply:

(a) Regulation (EC) 300/2008;

(b) Regulation (EU) No 167/2013;

(c) Regulation (EU) No 168/2013;

(d) Directive 2014/90/EU;

(e) Directive (EU) 2016/797;

(f) Regulation (EU) 2018/858;

(g) Regulation (EU) 2018/1139;

(h) Regulation (EU) 2019/2144.

3. This Regulation shall not apply to AI systems developed or used exclusively for military purposes.

4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

5. This Regulation shall not affect the application of the provisions on the liability of intermediary service providers set out in Chapter II, Section IV of Directive 2000/31/EC of the European Parliament and of the Council[60] [*as to be replaced by the corresponding provisions of the Digital Services Act*].

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(1) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

[60] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(c) AI 시스템의 산출물이 유럽 연합에서 사용되는 경우, 제3국에 소재한 AI 시스템의 제공자 및 사용자

2. 다음 법규의 범위 내에 속하는, 제품 또는 시스템의 안전 구성요소이거나 그 자체가 제품 또는 시스템인 고위험 AI 시스템에 대해서는 오로지 본 규정의 제84조만 적용된다.

(a) Regulation (EC) 300/2008;

(b) Regulation (EU) No 167/2013;

(c) Regulation (EU) No 168/2013;

(d) Directive 2014/90/EU;

(e) Directive (EU) 2016/797;

(f) Regulation (EU) 2018/858;

(g) Regulation (EU) 2018/1139;

(h) Regulation (EU) 2019/2144.

3. 본 규정은 오직 군사 목적으로만 개발되거나 사용되는 AI 시스템에는 적용되지 않는다.

4. 제3국의 공공 기관 또는 제1항에 따라 본 규정의 범위 내에 속하는 국제 기구가 유럽 연합 또는 회권국과의 법 집행 및 사법 협력을 위한 국제 협약의 프레임워크에서 AI 시스템을 사용하는 경우에는 본 규정이 적용되지 않는다.

5. 본 규정은 유럽 의회 및 유럽 이사회 Directive 2000/31/EC[60] 제II장, IV절[*디지털 서비스법(DSA)의 상응하는 조항에 의해 대체*]에 명시된 중개 서비스 제공자의 책임에 관한 조항의 적용에 영향을 미치지 않는다.

제3조

정의

본 규정의 목적을 위해 다음 정의가 적용된다.

(1) '인공 지능 시스템(Artificial Intelligence system)'(AI 시스템)은 부속서 I에 열거된 기법과 접근법을 통해 개발되고 인간이 정의한 목표를 위해 그것이 상호 작용하는 환경에 영향을 미치는 콘텐츠, 예측, 추천, 결정 등의 아웃풋을 생성할 수 있는 소프트웨어를 의미한다.

(2) '제공자(provider)'는 자체 명의 또는 상표 하에 유료 또는 무료로 출시하거나 서비스 개시하기 위해 AI 시스템을 개발하거나 개발을 의뢰하는 자연인 또는 법인, 공공 기관, 기구 또는 단체를 의미한다.

60 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(3) ‘small-scale provider’ means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC[61];

(4) ‘user’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

(5) ‘authorised representative’ means any natural or legal person established in the Union who has received a written mandate from a provider of an AI system to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;

(6) ‘importer’ means any natural or legal person established in the Union that places on the market or puts into service an AI system that bears the name or trademark of a natural or legal person established outside the Union;

(7) ‘distributor’ means any natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market without affecting its properties;

(8) ‘operator’ means the provider, the user, the authorised representative, the importer and the distributor;

(9) ‘placing on the market’ means the first making available of an AI system on the Union market;

(10) ‘making available on the market’ means any supply of an AI system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(11) ‘putting into service’ means the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose;

(12) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(13) ‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(14) ‘safety component of a product or system’ means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

(15) ‘instructions for use’ means the information provided by the provider to inform the user of in particular an AI system’s intended purpose and proper use, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used;

(16) ‘recall of an AI system’ means any measure aimed at achieving the return to the provider of an AI system made available to users;

[61] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(3) ‘소규모 제공자(small-scale provider)’는 Commission Recommendation 2003/361/EC[61]의 의미 내에서 소상공인 또는 중소기업인 제공자를 의미한다.

(4) ‘사용자(user)’는 개인적, 비전문적 활동에 AI 시스템이 사용되는 경우를 제외하고, 자체 권한에 따라 AI 시스템을 사용하는 자연인 또는 법인, 공공 기관, 기구 또는 기타 단체를 의미한다.

(5) ‘공인 대리인(authorised representative)’은 AI 시스템의 제공자로부터 그를 대신하여 본 규정에 명시된 의무와 절차를 수행할 권한을 서면으로 위임받은 유럽 연합에 소재하는 자연인 또는 법인을 의미한다.

(6) ‘수입업자(importer)’는 유럽 연합 외부에 소재하는 자연인 또는 법인의 이름 또는 상표를 부착한 AI 시스템을 출시하거나 서비스 개시하는 유럽 연합에 소재하는 자연인 또는 법인을 의미한다.

(7) ‘유통업자(distributor)’는 그 속성에 영향을 주지 않고 유럽 연합 시장에 AI 시스템을 제공하는, 제공자 또는 수입업자를 제외한 공급망에 속하는 자연인 또는 법인을 의미한다.

(8) ‘운영자(operator)’는 제공자, 사용자, 공인 대리인, 수입업자 및 유통업자를 의미한다.

(9) ‘출시(placing on the market)’는 AI 시스템을 유럽 연합 시장에 처음으로 공급하는 것을 의미한다.

(10) ‘시장에 공급(making available on the market)’은 유료, 무료를 막론하고 상업 활동 과정에서 유럽 연합 시장에서 유통하거나 사용할 AI 시스템을 공급하는 것을 의미한다.

(11) ‘서비스 개시(putting into service)’는 유럽 연합 시장에서 원래 목적으로 처음 사용하기 위해 사용자에게 직접 또는 자체 용도로 AI 시스템을 공급하는 것을 의미한다.

(12) ‘원래 목적(intended purpose)’은 제공자의 사용 지침, 판촉/홍보 자료, 명세서 및 기술 문서에 명시되고 특정한 사용 맥락과 조건을 포함하는, 제공자가 의도한 AI 시스템의 용도를 의미한다

(13) ‘합리적으로 예측 가능한 오용(reasonably foreseeable misuse)’은 원래 목적에 따르지 않고 합리적으로 예측 가능한 인간 행동 또는 다른 시스템과의 상호작용에서 비롯될 수 있는 방식으로 AI 시스템을 사용하는 것을 의미한다.

(14) ‘제품 또는 서비스의 안전 구성요소(safety component of a product or system)’는 제품 또는 서비스를 위한 안전 기능을 수행하거나, 그 고장 또는 오작동이 사람 또는 재산의 건강과 안전을 위협하는 제품 또는 서비스의 구성요소를 의미한다.

(15) ‘사용 지침(instructions for use)’은 고위험 AI 시스템이 사용되는 특정한 지리적, 행동적, 기능적 환경을 포함하여 AI 시스템의 원래 목적과 올바른 사용법을 사용자에게 알려주기 제공자가 제공하는 정보를 의미한다.

(16) ‘AI 시스템의 리콜(recall of an AI system)’은 사용자에게 공급한 AI 시스템을 제공자에게 반품하기 위한 조치를 의미한다.

---

[61] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(17) ‘withdrawal of an AI system’ means any measure aimed at preventing the distribution, display and offer of an AI system;

(18) ‘performance of an AI system’ means the ability of an AI system to achieve its intended purpose;

(19) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(20) ‘conformity assessment’ means the process of verifying whether the requirements set out in Title III, Chapter 2 of this Regulation relating to an AI system have been fulfilled;

(21) ‘conformity assessment body’ means a body that performs third-party conformity assessment activities, including testing, certification and inspection;

(22) ‘notified body’ means a conformity assessment body designated in accordance with this Regulation and other relevant Union harmonisation legislation;

(23) ‘substantial modification’ means a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation or results in a modification to the intended purpose for which the AI system has been assessed;

(24) ‘CE marking of conformity’ (CE marking) means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 of this Regulation and other applicable Union legislation harmonising the conditions for the marketing of products (‘Union harmonisation legislation’) providing for its affixing;

(25) ‘post-market monitoring’ means all activities carried out by providers of AI systems to proactively collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(26) ‘market surveillance authority’ means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020;

(27) ‘harmonised standard’ means a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012;

(28) ‘common specifications’ means a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation;

(29) ‘training data’ means data used for training an AI system through fitting its learnable parameters, including the weights of a neural network;

(30) ‘validation data’ means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split;

(31) ‘testing data’ means data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;

(17) ‘AI 시스템의 회수(withdrawal of an AI system)’는 AI 시스템 유통, 전시, 제공을 방지하기 위한 조치를 의미한다.

(18) ‘AI 시스템의 성능(performance of an AI system)’은 원래 목적을 달성하는 AI 시스템의 능력을 의미한다.

(19) ‘통보 기관(notifying authority)’은 적합성 평가 기관의 평가, 지명, 통지 및 모니터링에 필요한 절차를 수립하고 수행하는 일을 책임지는 국가 기관을 의미한다.

(20) ‘적합성 평가(conformity assessment)’는 본 규정 제3편 제2장에 명시된 AI 시스템과 관련된 요구사항이 충족되었는지 여부를 확인하는 절차를 의미한다.

(21) ‘적합성 평가 기관(conformity assessment body)’은 테스트, 인증, 검사 등을 포함한 제3자 적합성 평가 활동을 수행하는 기관을 의미한다.

(22) ‘인증 기관(notified body)’은 본 규정 및 기타 관련 유럽 연합 조화 법령에 따라 지명된 적합성 평가 기관을 의미한다.

(23) ‘상당한 수정(substantial modification)’은 AI 시스템이 본 규정 제3편 제2장에 명시된 요구사항을 준수하는 데 영향을 주거나 AI 시스템이 평가된 원래 목적의 수정을 초래하는, 출시 또는 서비스 개시 후에 이루어진 AI 시스템의 변경을 의미한다.

(24) ‘CE 적합성 마크(CE marking of conformity)’(CE 마크)는 AI 시스템이 본 규정 제3편 제2장에 명시된 요구사항 및 제품 출시를 위한 조건을 조화하는 기타 관련 유럽 연합 법규(‘유럽 연합 조화 법령’)를 준수한다는 것을 나타내는 마크를 의미한다.

(25) ‘출시 후 모니터링(post-market monitoring)’은 AI 시스템의 제공자가 시정 또는 예방 조치를 즉시 적용할 필요가 있는지 파악하기 위한 목적으로, 출시되거나 서비스 개시된 AI 시스템을 사용하면서 획득한 경험을 수집·검토하기 위해 수행하는 모든 활동을 의미한다.

(26) ‘시장 감시 기관(market surveillance authority)’은 Regulation (EU) 2019/1020에 따른 활동을 수행하고 조치를 취하는 국가 기관을 의미한다.

(27) ‘조화 표준(harmonised standard)’은 Regulation (EU) No 1025/2012 제2(1)(c)조에 정의된 유럽 표준을 의미한다.

(28) ‘공통 규격(common specifications)’은 본 규정에 따른 특정한 요구사항과 의무를 준수할 수단을 제공하는 기술 솔루션을 포함하는 표준 이외의 문서를 의미한다.

(29) ‘학습 데이터(training data)’는 신경망의 가중치를 포함하여 학습 가능한 매개변수의 조절을 통해 AI 시스템을 학습시키는 데 사용되는 데이터를 의미한다.

(30) ‘검증 데이터(validation data)’는 학습된 AI 시스템의 평가를 제공하고 학습 불가능한 매개변수와 그 학습 프로세스를 튜닝하는 데 사용되는 데이터를 의미한다. 검증 데이터세트는 별도의 데이터세트일 수도 있고 학습 데이터세트의 일부(고정 또는 가변 분할)일 수도 있다.

(31) ‘테스트 데이터(testing data)’는 AI 시스템을 출시하거나 서비스 개시하기 전에 기대 성능을 확인하기 위해 학습되고 검증된 AI 시스템의 독립 평가를 제공하는 데 사용되는 데이터를 의미한다.

(32) ‘input data’ means data provided to or directly acquired by an AI system on the basis of which the system produces an output;

(33) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(34) ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(35) ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

(36) ‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

(37) ‘‘real-time’ remote biometric identification system’ means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.

(38) ‘‘post’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;

(39) ‘publicly accessible space’ means any physical place accessible to the public, regardless of whether certain conditions for access may apply;

(40) ‘law enforcement authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(41) ‘law enforcement’ means activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(42) ‘national supervisory authority’ means the authority to which a Member State assigns the responsibility for the implementation and application of this Regulation, for coordinating the activities entrusted to that Member State, for acting as the single contact point for the Commission, and for representing the Member State at the European Artificial Intelligence Board;

(32) ‘인풋 데이터(input data)’는 시스템이 아웃풋을 산출하는 토대가 되는, AI 시스템에 제공되거나 AI 시스템이 직접 획득하는 데이터를 의미한다.

(33) ‘생체 인식 데이터(biometric data)’는 자연인의 신체적, 생리적, 행동적 특성과 관련된 기술적 처리를 통해 산출되는 얼굴 이미지나 지문 데이터와 같이 그의 고유 신원을 확인할 수 있게 해주는 개인 데이터를 의미한다.

(34) ‘감정 인식 시스템(emotion recognition system)’은 자연인의 생체 인식 데이터를 토대로 그를 식별하거나 그의 감정 또는 의도를 추측하는 AI 시스템을 의미한다.

(35) ‘생체 인식 분류 시스템(biometric categorisation system)’은 자연인의 생체 인식 데이터를 토대로 성별, 연령, 머리 색, 눈동자 색, 문신, 민족, 성적 또는 정치적 지향 등의 범주를 할당하는 AI 시스템을 의미한다.

(36) ‘원격 생체 인식 시스템(remote biometric identification system)’은 당사자가 입회할 것이며 식별할 수 있는지 여부와 무관하게 AI 시스템의 사용자에 대한 사전 지식 없이, 자연인의 생체 인식 데이터를 참조 데이터베이스에 포함된 생체 인식 데이터와 비교하여 원거리에서 자연인을 식별하는 AI 시스템을 의미한다.

(37) ‘실시간 원격 생체 인식 시스템(real-time remote biometric identification system)’은 생체 인식 데이터의 수집, 비교 및 식별이 모두 큰 지연 없이 이루어지는 원격 생체 인식 시스템을 의미한다. 이는 즉각적인 식별과 회피를 방지하기 위한 제한적인 짧은 지연으로 구성된다.

(38) ‘사후 원격 생체 인식 시스템(post remote biometric identification system)’은 ‘실시간’ 원격 생체 인식 시스템 이외의 원격 생체 인식 시스템을 의미한다.

(39) ‘공개적으로 접근 가능한 공간(publicly accessible space)’은 접근을 위한 조건이 적용되는지 여부에 관계없이 일반인이 접근할 수 있는 물리적 공간을 의미한다.

(40) ‘법 집행 기관(law enforcement authority)’은 다음을 의미한다.

(a) 치안에 대한 위협으로부터의 보호와 예방을 포함한 범죄 행위의 방지, 수사, 탐지, 기소 또는 형사 처벌의 집행을 관할하는 공공 기관.

(b) 회원국 법률에 의해 치안에 대한 위협으로부터의 보호와 예방을 포함한 범죄 행위의 방지, 수사, 탐지, 기소 또는 형사 처벌의 집행 목적으로 공권력을 행사하도록 위임받은 기타 기관 또는 실체.

(41) ‘법 집행(law enforcement)’은 치안에 대한 위협으로부터의 보호와 예방을 포함한 범죄 행위의 방지, 수사, 탐지, 기소 또는 형사 처벌의 집행을 위해 법 집행 기관이 수행하는 활동을 의미한다.

(42) ‘국가 감독 기관(national supervisory authority)’은 회원국이 본 규정을 시행·적용하고, 해당 회원국에 위임된 활동을 조율하고, 유럽연합 집행위원회에 대해 단일 연락 지점 역할을 수행하고, 유럽 인공지능 위원회에서 회원국을 대표하는 책임을 할당하는 기관을 의미한다.

(43) ‘national competent authority’ means the national supervisory authority, the notifying authority and the market surveillance authority;

(44) ‘serious incident’ means any incident that directly or indirectly leads, might have led or might lead to any of the following:

(a) the death of a person or serious damage to a person’s health, to property or the environment,

(b) a serious and irreversible disruption of the management and operation of critical infrastructure.

Article 4
Amendments to Annex I

The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5

1. The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person’s consciousness in order to materially distort a person’s behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

(43) ‘국가 관할 기관(national competent authority)’은 국가 감독 기관, 통보 기관 및 시장 감시 기관을 의미한다.

(44) ‘중대한 사건(serious incident)’은 직접적 또는 간접적으로 다음을 초래하거나, 초래했을 수 있거나, 초래할 수 있는 사건을 의미한다

(a) 사람의 죽음 또는 사람의 건강, 재산 또는 환경에 대한 중대한 피해

(b) 중요한 인프라의 관리 및 운영의 중대하고 회복 불가능한 중단.

제4조

부속서I의 개정

유럽연합 집행위원회는 제73조에 따른 위임 규정을 채택하여, 부속서 I에 열거된 기법 및 접근법의 목록을 수정하고 그러한 기법 및 접근법과 유사한 특성을 토대로 동 목록을 시장 및 기술 발전에 맞추어 업데이트할 권한을 가진다.

제2편

금지되는 인공 지능 관행

제5조

1. 다음과 같은 인공 지능 관행은 금지된다.

(a) 당사자 또는 타인에게 물질적 또는 정신적 피해를 주거나 줄 가능성이 있는 방식으로 사람의 행동을 중대하게 왜곡하기 위해 사람의 의식을 벗어난 식역하 기법을 배포하는 AI 시스템의 출시, 서비스 개시 또는 사용

(b) 당사자 또는 타인에게 물질적 또는 정신적 피해를 주거나 줄 가능성이 있는 방식으로 특정 집단에 속하는 사람의 행동을 중대하게 왜곡하기 위해 해당 집단의 연령, 신체 또는 정신 장애로 인한 취약성을 이용하는 AI 시스템의 출시, 서비스 개시 또는 사용

(c) 자연인의 사회적 행동 또는 알려지거나 인식된 개인적 특성 또는 성격 특성을 토대로 일정 기간에 걸쳐 그의 신뢰성을 평가 또는 분류하기 위한, 공공 기관에 의한 또는 그를 대신한 AI 시스템의 출시, 서비스 개시 또는 사용. 단, 소셜 스코어가 다음 중 하나 또는 두 가지 모두로 이어지는 경우.

(i) 데이터가 처음 생성되거나 수집된 맥락과 무관한 사회적 맥락에서 특정 자연인 또는 전체 집단의 차별 또는 홀대

(ii) 그들의 사회적 행동 또는 그 중대성에 비례하지 않거나 정당하지 않은 특정 자연인 또는 전체 집단의 차별 또는 홀대

(d) 법 집행 목적으로 공개적으로 접근 가능한 공간에서 ‘실시간’ 원격 생체 인식 시스템을 사용하는 것. 단, 다음 목적 중 하나를 위해 그러한 사용이 절대적으로 필요한 경우는 예외로 한다.

(i) the targeted search for specific potential victims of crime, including missing children;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

(iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[62] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the

[62] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

(i) 실종 아동을 포함한 범죄의 잠재적 피해자에 대한 표적 수색

(ii) 자연인의 생명 또는 신체적 안전에 대한 구체적이고 실질적이며 임박한 위협 또는 테러 공격의 방지

(iii) Council Framework Decision 2002/584/JHA[62] 제2(2)조에 언급되고 관련 회원국의 법률에 정해진 바에 따라 3년 이상의 최대 기간 동안 구금형 또는 구금 명령으로 처벌 가능한 범죄 행위의 범인 또는 용의자 탐지, 소재 파악, 식별 또는 기소.

2. 제1항 (d)호에 언급된 목적을 위해 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용할 경우 다음 요소를 고려해야 한다.

(a) 사용을 유발하는 상황의 성격. 특히 시스템을 사용하지 않을 경우 초래되는 피해의 심각성, 개연성 및 규모.

(b) 모든 관계자의 권리와 자유에 대한 시스템 사용의 결과. 특히 그러한 결과의 심각성, 개연성 및 규모.

이와 더불어, 제1항 (d)호에 언급된 목적을 위해 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용할 경우, 특히 시간적, 지리적, 개인적 제한을 고려하여, 사용과 관련된 보호 조치 및 조건을 준수해야 한다.

3. 제1항 (d)호 및 제2항과 관련하여, 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 각각의 경우에 대해, 합리적인 요청 시 제4항에 언급된 국가 법률의 세칙에 따라 발급되고 사용이 이루어지는 회원국의 사법 기관 또는 독립 행정 기관이 수여하는 사전 허가를 받아야 한다. 단, 적절한 절차에 따라 정당화되는 긴급 상황에서는 허가 없이 시스템의 사용을 개시할 수 있으며 사용 도중 또는 이후에만 허가를 요청할 수 있다.

관할 사법 또는 행정 기관은 그에 제시된 객관적 증거 또는 명백한 징후를 토대로 문제의 '실시간' 원격 생체 인식 시스템의 사용이 요청에서 밝힌 제1항 d)호에 명시된 목표 중 하나를 달성하는 데 필요하고 비례적이라는 사실이 입증되는 경우에만 허가를 수여해야 한다. 요청에 대해 결정을 내리는 과정에서 관할 사법 또는 행정 기관은 제2항에 언급된 요소들을 고려해야 한다.

4. 회원국은 제1항 (d)호, 제2항 및 제3항에 열거된 제한과 조건 내에서 법 집행 목적으로 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용하는 것을 전부 또는 일부 허가하는 것을 허용하기로 결정할 수 있다.

---

62 Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

TITLE III

HIGH-RISK AI SYSTEMS

CHAPTER 1

CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

Article 6
Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

   (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

   (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

Article 7
Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

   (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;

   (b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

2. When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems

해당 회원국은 제3항에 언급된 허가의 요청, 발급, 행사 및 감독에 대한 필수 세칙을 국가 법률에 명시해야 한다. 아울러 이러한 세칙은 제1항 (d)호에 열거된 목표 및 (d)(iii)호에 언급된 범죄 행위 중 어느 것과 관련하여 관할 기관이 법 집행 목적으로 동 시스템을 사용하도록 허가받을 수 있는지 명시해야 한다.

제3편

고위험 AI 시스템

제1장

AI 시스템의 고위험 분류

제6조

고위험 AI 시스템에 대한 분류 규칙

1. AI 시스템이 (a)호와 (b)호에 언급된 제품과 독립적으로 출시되거나 서비스 개시되는지 여부에 관계없이, 다음 두 가지 조건이 모두 충족되는 경우 해당 AI 시스템은 고위험으로 간주되어야 한다.

   (a) AI 시스템이 부속서 II에 열거된 유럽 연합 조화 법령이 적용되는 제품의 안전 구성요소로 사용되거나 그 자체가 제품인 경우

   (b) AI 시스템이 안전 구성요소인 제품 또는 제품으로서 AI 시스템 자체를 부속서 II에 열거된 유럽 연합 조화 법령에 따라 출시하거나 서비스 개시하려면 제3자 적합성 평가를 거쳐야 한다.

2. 1항에 언급된 고위험 AI 시스템에 더하여, 부속서 III에 언급된 AI 시스템 역시 고위험으로 간주되어야 한다.

제7조

부속서 III의 개정

1. 유럽연합 집행위원회는 제73조에 따른 위임 규정을 채택하여, 다음 두 가지 조건이 모두 충족되는 경우 고위험 AI 시스템을 추가하여 부속서 III에 열거된 목록을 업데이트할 권한을 가진다.

   (a) AI 시스템이 부속서 III의 1~8항에 열거된 분야에서 사용되는 경우

   (b) AI 시스템이 발생의 심각성과 개연성에 비추어 부속서 III에 이미 언급된 고위험 AI 시스템이 초래하는 피해 또는 악영향의 위험과 동등하거나 더 크게 건강과 안전에 피해를 주거나 기본권에 악영향을 미칠 위험을 초래하는 경우.

2. 제1항의 목적을 위해, AI 시스템이 부속서 III에 이미 언급된 고위험 AI 시스템이 초래하는 피해의 위험과 동등하거나 더 크게 건강과 안전에 피해를 주거나 기본권에 악영향을 미칠 위험을 초래하는지 여부를 평가할 때, 유럽

already referred to in Annex III, the Commission shall take into account the following criteria:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;

(d) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

(e) the extent to which potentially harmed or adversely impacted persons are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(f) the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;

(g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;

(h) the extent to which existing Union legislation provides for:

(i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

(ii) effective measures to prevent or substantially minimise those risks.

CHAPTER 2

REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

Article 8
Compliance with the requirements

1. High-risk AI systems shall comply with the requirements established in this Chapter.

2. The intended purpose of the high-risk AI system and the risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

Article 9
Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

위원회는 다음 기준을 고려해야 한다.

(a) AI 시스템의 원래 목적

(b) AI 시스템이 사용되었거나 사용될 가능성이 있는 정도

(c) 국가 관할 당국에 제출된 보고서 또는 문서화된 주장에 의해 입증된, AI 시스템의 사용이 이미 건강과 안전에 피해를 주거나, 기본권에 악영향을 미치거나, 그러한 피해 또는 악영향의 실현에 대해 상당한 우려를 불러일으킨 정도

(d) 특히 많은 사람에게 영향을 미치는 강도와 능력의 맥락에서 그러한 피해 또는 악영향의 잠재적 정도

(e) 잠재적 피해 또는 악영향을 받는 사람이 특히 실제적 또는 법적 이유로 그 결과물을 옵트아웃(opt-out)하는 것이 합리적으로 가능하지 않기 때문에 AI 시스템으로 산출된 결과물에 의존하는 정도

(f) 잠재적 피해 또는 악영향을 받는 사람이 특히 권력, 지식, 경제적·사회적 상황, 또는 연령 등으로 인해 AI 시스템의 사용자와 관련하여 취약한 위치에 놓이는 정도

(g) AI 시스템으로 산출한 결과물을 손쉽게 번복할 수 있는(reversible) 정도(사람의 건강 또는 안전에 영향을 미치는 결과물은 손쉽게 번복 가능한 것으로 간주되지 않음)

(h) 기존의 유럽 연합 법규가 다음 사항을 규정하는 정도

(i) AI 시스템이 초래하는 위험과 관련한 효과적 구제 수단(손해 배상 청구 제외)

(ii) 그러한 위험을 방지하거나 최소화하기 위한 효과적 수단.

제2장

고위험 AI 시스템에 대한 요구사항

제8조

요구사항의 준수

1. 위험 AI 시스템은 이 장에 명시된 요구사항을 준수해야 한다.

2. 그러한 요구사항의 준수 여부를 확인할 때는 고위험 AI 시스템과 제9조에 언급된 위험 관리 시스템의 원래 목적을 고려해야 한다.

제9조

위험 관리 시스템

1. 고위험 AI 시스템과 관련한 위험 관리 시스템을 구축, 시행, 기록, 유지해야 한다.

2. 위험 관리 시스템은 고위험 AI 시스템의 라이프사이클 전반에 걸쳐 지속적으로 운영되고 정기적·체계적 업데이트를 요하는 반복 과정으로 이루어진다. 이는 다음과 같은 단계들로 구성된다.

(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

(b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;

(c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

(d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

3. The risk management measures referred to in paragraph 2, point (d) shall give due consideration to the effects and possible interactions resulting from the combined application of the requirements set out in this Chapter 2. They shall take into account the generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications.

4. The risk management measures referred to in paragraph 2, point (d) shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user.

In identifying the most appropriate risk management measures, the following shall be ensured:

(a) elimination or reduction of risks as far as possible through adequate design and development;

(b) where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated;

(c)) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

In eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used.

5. High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter.

6. Testing procedures shall be suitable to achieve the intended purpose of the AI system and do not need to go beyond what is necessary to achieve that purpose.

7. The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

(a) 각 고위험 AI 시스템과 관련된 알려지고 예측 가능한 위험의 파악 및 분석

(b) 고위험 AI 시스템을 합리적으로 예측 가능한 오용의 조건 하에서 원래의 목적으로 사용할 때 발생할 수 있는 위험의 추정 및 평가

(c) 제61조에 언급된 출시 후 모니터링 시스템에서 수집한 데이터의 분석에 근거한 발생 가능한 다른 위험의 평가

(d) 아래 항들의 규정에 따른 적합한 위험 관리 수단의 채택.

3. 2항 (d)호에 언급된 위험 관리 수단은 본 제2장에 명시된 요구사항의 적용으로 비롯되는 효과와 가능한 상호작용을 충분히 고려해야 한다. 이는 관련 조화 표준 또는 공통 규격에 반영된 것을 포함하여 일반적으로 인정되는 첨단 기술을 고려해야 한다.

4. 2항 (d)호에 언급된 위험 관리 수단은, 고위험 AI 시스템이 원래 목적에 따라 또는 합리적으로 예측 가능한 오용 조건 하에서 사용되는 경우 각 위험 요소와 관련된 잔여 위험과 고위험 AI 시스템의 모든 잔여 위험이 허용 가능한 것으로 판단되도록 보장해야 한다. 단, 고위험 AI 시스템이 원래 목적에 따라 또는 합리적으로 예측 가능한 오용의 조건 하에서 사용되어야 한다. 이러한 잔여 위험을 사용자에게 통지해야 한다.

가장 적합한 위험 관리 수단을 모색하는 과정에서 다음 사항이 보장되어야 한다.

(a) 적합한 설계와 개발을 통해 최대한 위험 제거 또는 완화

(b) 적절한 경우, 제거할 수 없는 위험에 대해 적합한 완화 및 통제 조치 시행

(c) 특히 본 조의 제2항 (b)호에 언급된 위험과 관련하여 제13조에 따른 충분한 정보 제공, 및 적절한 경우 사용자 교육.

고위험 AI 시스템의 사용에 따른 위험을 제거하거나 완화할 때는 사용자가 기대하는 기술적 지식, 경험, 교육, 훈련과 시스템이 사용되는 환경을 충분히 고려해야 한다.

5. 가장 적합한 위험 관리 수단을 파악하기 위한 목적으로 고위험 AI 시스템을 테스트해야 한다. 테스트를 통해 고위험 AI 시스템이 원래 목적에 일치하도록 사용되고 본 장에 명시된 요구사항을 준수하는지 여부를 확인해야 한다.

6. 테스트 절차는 AI 시스템의 원래 목적을 달성하는 데 적합해야 하며 그러한 목적을 달성하는 데 필요한 범위를 넘어설 필요가 없다.

7. 고위험 AI 시스템의 테스트는 적절한 경우 개발 과정에서 임의의 시점에 수행되어야 하며, 어떠한 경우에도 출시 또는 서비스 개시 전에 수행되어야 한다. 테스트는 고위험 AI 시스템의 원래 목적에 적합한 사전 정의된 척도와 확률적 임계값을 기준으로 이루어져야 한다.

8. When implementing the risk management system described in paragraphs 1 to 7, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

9. For credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.

Article 10
Data and data governance

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

   (a) the relevant design choices;

   (b) data collection;

   (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;

   (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;

   (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;

   (f) examination in view of possible biases;

   (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high- risk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

8. 1~7항에 기술된 위험 관리 시스템을 실행할 때는 아동이 고위험 AI 시스템에 접근하거나 영향을 받을 가능성이 있는지 여부에 각별한 주의를 기울여야 한다.

9. Directive 2013/36/EU의 규제를 받는 신용 기관의 경우, 1~8항에 기술된 측면들은 동 Directive 제74조에 따라 동 기관이 수립한 위험 관리 절차의 일부가 되어야 한다.

제10조
데이터 및 데이터 거버넌스

1. 데이터를 통한 모델의 학습을 수반하는 기법을 사용하는 고위험 AI 시스템은 2~5항에 언급된 품질 기술을 충족하는 학습, 검증, 테스트 데이터세트를 기반으로 개발되어야 한다.

2. 학습, 검증, 테스트 데이터세트에는 적절한 데이터 거버넌스 및 관리 관행이 적용되어야 한다. 이러한 관행은 특히 다음과 관련된다.

   (a) 설계 선택

   (b) 데이터 수집

   (c) 주석, 레이블링, 정리, 보강, 집계 등 데이터 준비 처리 작업

   (d) 특히 데이터가 측정하고 표시해야 하는 정보와 관련한 가정의 공식화

   (e) 필요한 데이터세트의 가용성, 품질, 지속가능성에 대한 사전 평가

   (f) 가능한 편향을 고려한 조사

   (g) 가능한 데이터 갭 또는 부족 및 그러한 갭과 부족을 해소하는 방법의 파악.

3. 학습, 검증, 테스트 데이터세트는 관련성 있고, 오류가 없고, 완전해야 한다. 이는 고위험 AI 시스템의 사용 대상인 개인 또는 집단과 관련된 것을 포함하여 적절한 통계적 특성을 가져야 한다. 데이터세트의 이러한 특성은 개별 데이터세트 또는 데이터세트 조합의 수준에서 충족될 수 있다.

4. 학습, 검증, 테스트 데이터세트는 원래 목적이 요구하는 한에서, 고위험 AI 시스템이 사용되는 지리적, 행동적, 기능적 환경에 특유한 특성 또는 요소를 고려해야 한다.

5. 고위험 AI 시스템과 관련된 편향 모니터링, 탐지, 시정의 목적을 위해 절대적으로 필요한 경우, 동 시스템의 제공자는 Regulation (EU) 2016/679 제9(1)조, Directive (EU) 2016/680 제10조 및 Regulation (EU) 2018/1725 제10(1)조에 언급된 특수한 범주의 개인 데이터를 처리할 수 있다. 단, 가명화, 또는 익명화가 추구하는 목적에 상당한 영향을 줄 수 있는 경우 암호화와 같은 첨단 보안 및 개인정보 보호 수단의 사용 및 재사용에 대한 기술적 제한을 포함하여 자연인의 기본권과 자유를 보호할 적절한 수단이 확보되어야 한다.

6. Appropriate data governance and management practices shall apply for the development of high-risk AI systems other than those which make use of techniques involving the training of models in order to ensure that those high-risk AI systems comply with paragraph 2.

Article 11
Technical documentation

1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

   The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV.

2. Where a high-risk AI system related to a product, to which the legal acts listed in Annex II, section A apply, is placed on the market or put into service one single technical documentation shall be drawn up containing all the information set out in Annex IV as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend Annex IV where necessary to ensure that, in the light of technical progress, the technical documentation provides all the necessary information to assess the compliance of the system with the requirements set out in this Chapter.

Article 12
Record-keeping

1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.

2. The logging capabilities shall ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system.

3. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61.

4. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:

   (a) recording of the period of each use of the system (start date and time and end date and time of each use);

   (b) the reference database against which input data has been checked by the system;

   (c) the input data for which the search has led to a match;

6. 그러한 고위험 AI 시스템이 제2항을 준수하도록 보장하기 위해 모델의 학습을 수반하는 기법을 사용하지 않는 고위험 AI 시스템의 개발에 적절한 데이터 거버넌스 및 관리 관행이 적용되어야 한다.

제11조
기술 문서

1. 고위험 AI 시스템이 출시되거나 서비스 개시되기 전에 해당 시스템의 기술 문서를 작성하고 최신으로 유지해야 한다.

   기술 문서는 본 장에 명시된 고위험 AI 시스템이 요구사항을 준수한다는 것을 입증하는 방식으로 작성되어야 하며, AI 시스템이 동 요구사항을 준수하는지 평가하는 데 필요한 모든 정보를 국가 관할 당국과 인증 기관에 제공해야 한다. 여기에는 최소한 부속서 IV에 명시된 요소들이 포함되어야 한다.

2. 부속서 II의 A절에 열거된 법규가 적용되는 제품과 관련한 고위험 AI 시스템이 출시되거나 서비스 개시되는 경우, 부속서 IV에 명시된 모든 정보와 동 법규에 따라 요구되는 정보를 포함하는 하나의 기술 문서가 작성되어야 한다.

3. 유럽연합 집행위원회는 기술 진보에 비추어 시스템이 본 장에 명시된 요구사항을 준수하는지 평가하는 데 필요한 모든 정보가 기술 문서에 포함되도록 보장하기 위해 필요한 경우 제73조에 따른 위임 규정을 채택하여 부속서 IV를 수정할 권한을 가진다.

제12조
기록 유지

1. 고위험 AI 시스템은 고위험 AI 시스템이 운영되는 동안 사건의 자동 기록('로그')이 가능하도록 설계·개발되어야 한다. 이러한 로깅 기능은 공인 표준 또는 공통 규격을 준수해야 한다.

2. 로깅 기능은 AI 시스템의 라이프사이클 전반에 걸쳐 그 기능에 대해 시스템의 원래 목적에 적합한 수준의 추적 가능성을 보장해야 한다.

3. 특히, 로깅 기능은 AI 시스템이 제65(1)조의 의미 내에서 위험을 초래하거나 상당한 수정으로 이어질 수 있는 상황의 발생과 관련하여 고위험 AI 시스템의 운영에 대한 모니터링을 지원하고 제61조에 언급된 출시 후 모니터링을 촉진해야 한다.

4. 부속서 III의 제1항 (a)호에 언급된 고위험 AI 시스템의 경우, 로깅 기능은 최소한 다음 항목을 제공해야 한다.

   (a) 시스템의 각 사용 기간(각 사용의 시작 날짜 및 시간과 종료 날짜 및 시간)의 기록

   (b) 시스템이 인풋 데이터를 확인하는 근거가 된 참조 데이터베이스

   (c) 검색이 일치로 이어진 인풋 데이터

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5).

Article 13
Transparency and provision of information to users

1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title.

2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.

3. The information referred to in paragraph 2 shall specify:

(a) the identity and the contact details of the provider and, where applicable, of its authorised representative;

(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

(i) its intended purpose;

(ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

(iii) any known or foreseeable circumstance, related to the use of the high- risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights;

(iv) its performance as regards the persons or groups of persons on which the system is intended to be used;

(v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system.

(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;

(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;

(e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.

(d) 제14(5)조에 언급된, 결과의 검증에 관여한 자연인의 신원.

제13조
투명성 및 정보 제공

1. 고위험 AI 시스템은 사용자가 시스템의 아웃풋을 해석하고 적절히 사용할 수 있을 만큼 충분히 투명하게 운영되도록 설계·개발되어야 한다. 사용자와 제공자가 본 편(Title)의 제3장에 명시된 각자의 의무를 준수할 수 있도록 하기 위해 적절한 유형과 수준의 투명성이 보장되어야 한다.

2. 고위험 AI 시스템에는 적절한 디지털 형식으로 작성되거나 사용자가 접근하고 이해할 수 있는 간결하고 완전하고 정확하고 명확한 정보를 포함하는 사용 지침이 수반되어야 한다.

3. 2항에 언급된 정보는 다음 사항을 명시해야 한다.

(a) 제공자 및 적절한 경우 공인 대리인의 신원과 연락처 세부사항

(b) 다음을 포함한 고위험 AI 시스템의 수행 특성, 기능 및 제한

(i) 원래 목적

(ii) 고위험 AI 시스템을 테스트·검증한 기준이 되고 예상될 수 있는 제15조에 언급된 정확성, 견고성 및 사이버 보안의 수준, 및 그와 같이 예상되는 정확성, 견고성 및 사이버 보안의 수준에 영향을 미칠 수 있는 알려지고 예측 가능한 상황

(iii) 원래 목적에 따라 또는 합리적으로 예측 가능한 오용 조건 하에서 고위험 AI 시스템을 사용하는 데 따른, 건강과 안전 또는 기본권에 대한 위험으로 이어질 수 있는 알려지거나 예측 가능한 상황

(iv) 시스템의 사용 대상인 개인 또는 집단과 관련된 수행

(v) AI 시스템의 원래 목적을 고려한 인풋 데이터에 대한 규격 또는 사용되는 학습, 검증, 테스트 데이터세트와 관련된 기타 모든 정보.

(c) 고위험 AI 시스템과 초기 적합성 평가 시에 제공자가 사전 결정한 그 성능의 변경

(d) 사용자가 AI 시스템의 아웃풋을 해석할 수 있도록 해주는 기술적 수단을 포함한 제14조에 언급된 인간의 감독 수단

(e) 고위험 AI 시스템의 예상 수명, 및 소프트웨어 업데이트를 포함하여 동 시스템의 올바른 기능을 보장하는 데 필요한 유지 관리 수단

Article 14
Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.

3. Human oversight shall be ensured through either one or all of the following measures:

   (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;

   (b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances:

   (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;

   (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

   (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;

   (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;

   (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

Article 15
Accuracy, robustness and cybersecurity

1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy,

제14조

인간의 감독

1. 고위험 AI 시스템은 사용되는 기간 동안 자연인이 효과적으로(적절한 인간-기계 상호작용 도구의 사용을 포함하여) 감독할 수 있는 방식으로 설계·개발되어야 한다.

2. 인간의 감독은 원래의 목적에 따라 또는 합리적으로 예측 가능한 오용 조건 하에서 고위험 AI 시스템을 사용할 때, 특히 본 장에 명시된 다른 요구사항을 적용하는데도 불구하고 그러한 위험이 지속될 때 발생할 수 있는 건강, 안정 또는 기본권에 대한 위험을 방지하거나 최소화하는 것을 목표로 한다.

3. 인간의 감독은 다음 수단 중 하나 또는 모두를 통해 보장되어야 한다.

   (a) 기술적으로 실현 가능한 경우, 출시되거나 서비스 개시되기 전에 제공자에 의해 식별되어 고위험 AI 시스템에 내장되는 수단

   (b) AI 시스템이 출시되거나 서비스 개시되기 전에 제공자에 의해 식별되고 사용자에 의해 시행하는 것이 적절한 수단.

4. 3항에 언급된 수단은 감독 책임을 맡은 개인이 상황에 따라 다음과 같은 작업을 수행할 수 있도록 해야 한다.

   (a) 고위험 AI 시스템의 능력과 한계를 충분히 이해하고 그 운영을 적절히 모니터하여 이상의 징후, 기능 장애 및 예기치 않은 작동을 탐지하고 가능한 한 신속히 해결한다.

   (b) 특히 자연인이 내리는 의사결정을 위한 정보 또는 권고를 제공하는 데 사용되는 고위험 AI 시스템의 경우, 시스템이 산출한 아웃풋에 자동적으로 의존하거나 지나치게 의존하는 경향('자동화 편향')을 인지한다.

   (c) 특히 시스템의 특성과 가용한 해석 도구 및 방법을 고려하여 고위험 AI 시스템의 아웃풋을 정확하게 해석한다.

   (d) 특별한 상황에서 고위험 AI 시스템을 사용하지 않거나 고위험 AI 시스템의 아웃풋을 무시 또는 번복하기로 결정한다.

   (e) 고위험 AI 시스템의 운영에 개입하거나 "중지" 버튼 또는 유사한 절차를 통해 시스템을 중단시킨다.

5. 부속서 III의 1(a)항에 언급된 고위험 AI 시스템의 경우, 제3항에 언급된 수단들은 사용자가 시스템에서 산출된 식별에 근거하여 어떠한 조치를 취하거나 결정을 내리지 않도록 보장해야 한다.

제15조

정확성, 견고성 및 사이버 보안

1. 고위험 AI 시스템은 원래 목적에 비추어 적절한 수준의 정확성, 견고성 및 사이버 보안을 성취하고, 라이프사이클 전반에 걸쳐 그러한 점에서 일관성 있게 작동하는 방식으로

robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.

2. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.

4. High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

CHAPTER 3

OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES

Article 16
Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

(b) have a quality management system in place which complies with Article 17;

(c) draw-up the technical documentation of the high-risk AI system;

(d) when under their control, keep the logs automatically generated by their high-risk AI systems;

(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(f) comply with the registration obligations referred to in Article 51;

(g) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;

설계·개발되어야 한다.

2. 고위험 AI 시스템의 정확성 수준 및 정확성 척도는 첨부한 사용 지침에 명시되어야 한다.

3. 고위험 AI 시스템은 특히 자연인 또는 다른 시스템과의 상호작용으로 인해 시스템 내에서 또는 시스템이 운영되는 환경에서 발생할 수 있는 오류, 고장, 불일치에 대해 복원력을 가져야 한다.

   고위험 AI 시스템의 견고성은 백업 또는 페일세이프(fail-safe) 플랜을 포함한 기술적 중복(redundancy) 솔루션을 통해 성취될 수 있다.

   출시되거나 서비스 개시된 후에도 계속 학습하는 고위험 AI 시스템은 향후의 운영을 위한 인풋으로 사용되는 아웃풋('피드백 루프')으로 인해 편향될 수 있는 아웃풋이 적절한 완화 조치를 통해 충분히 처리되도록 보장하는 방식으로 개발되어야 한다.

4. 고위험 AI 시스템은 허가받지 않은 제3자가 시스템 취약성을 이용하여 그 사용 또는 수행을 변경하려는 시도에 대해 복원력을 가져야 한다.

   고위험 AI 시스템의 사이버 보안을 보장하기 위한 기술 솔루션은 관련된 상황과 위험에 적절해야 한다.

   AI 특유의 취약성을 해소하는 기술 솔루션에는 학습 데이터세트를 조작하려고 시도하는 공격('데이터 오염'), 모델이 오작동을 일으키도록 설계된 인풋('적대적 샘플'), 또는 모델 결함 등을 방지하고 통제하기 위한 수단이 포함되어야 한다.

제3장

고위험 AI 시스템 제공자와 사용자 및 기타 당사자의 의무

제16조

고위험 AI 시스템 제공자의 의무

고위험 AI 시스템의 제공자는 다음과 같은 의무를 가진다.

(a) 각자의 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하도록 보장한다.

(b) 제17조를 준수하는 품질 관리 시스템을 배치한다.

(c) 고위험 AI 시스템에 관한 기술 문서를 작성한다.

(d) 각자의 통제 하에 있을 때, 고위험 AI 시스템이 자동으로 생성하는 기록(log)을 유지한다.

(e) 고위험 AI 시스템이 출시되거나 서비스 개시되기 전에 적합성 평가 절차를 거치도록 보장한다.

(f) 제51조에 언급된 등록 의무를 준수한다.

(g) 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하지 않는 경우 필요한 시정 조치를 취한다.

(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;

(i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;

(j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

Article 17
Quality management system

1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a)) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;

(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;

(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;

(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;

(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;

(g) the risk management system referred to in Article 9;

(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61;

(i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62;

(j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

(k) systems and procedures for record keeping of all relevant documentation and information;

(l) resource management, including security of supply related measures;

(h) 그들이 AI 시스템을 제공하거나 서비스 개시한 회원국의 국가 관할 당국과 해당되는 경우 인증 기관에 비준수 사례와 그에 대해 취한 시정 조치를 통지한다.

(i) 제49조에 따른 본 규정의 준수를 나타내는 CE 마크를 각자의 고위험 AI 시스템에 부착한다.

(j) 국가 관할 당국이 요구할 경우 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 것을 입증한다.

제17조
품질 관리 시스템

1. 고위험 AI 시스템의 제공자는 본 규정의 준수를 보장하는 품질 관리 시스템을 배치해야 한다. 이 시스템은 서면 정책, 절차, 지침의 형태로 체계적이고 정연한 방식으로 기록되어야 하며, 적어도 다음 측면을 포함해야 한다.

(a) 적합성 평가 절차와 고위험 AI 시스템에 대한 수정의 관리를 위한 절차의 준수를 포함한 규제 준수를 위한 전략

(b) 고위험 AI 시스템의 설계, 설계 관리 및 설계 검증에 사용되는 기법, 절차 및 체계적 조치

(c) 고위험 AI 시스템의 개발, 품질 관리 및 품질 보증에 사용되는 기법, 절차 및 체계적 조치

(d) 고위험 AI 시스템의 개발 전·중·후에 수행되는 조사, 테스트, 검증 절차와 그 수행 빈도

(e) 적용되는 표준을 포함한 기술 규격 및 조화 표준이 충분히 적용되지 않는 경우 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하도록 보장하는 데 사용되는 수단

(f) 고위험 AI 시스템의 출시 또는 서비스 개시 전에 그러한 목적으로 수행되는 데이터 수집, 데이터 분석, 데이터 레이블링, 데이터 저장, 데이터 필터링, 데이터 마이닝, 데이터 집계, 데이터 보존 및 기타 모든 작업을 포함한 데이터 관리를 위한 시스템 및 절차

(g) 제9조에 언급된 위험 관리 시스템

(h) 제61조에 따른 출시 후 모니터링 시스템의 구축, 시행 및 유지관리

(i) 제62조에 따른 중대한 사건 및 오작동의 보고와 관련된 절차

(j) 국가 관할 당국, 데이터의 접근을 제공하거나 지원하는 부분별 기관을 포함한 관할 기관, 인증 기관, 기타 운영자, 고객 또는 이해 당사자와의 의사소통

(k) 관련된 모든 문서와 정보의 기록 유지를 위한 시스템 및 절차

(l) 공급 수단의 보안을 포함한 자원 관리

(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

2. The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation.

3. For providers that are credit institutions regulated by Directive 2013/36/ EU, the obligation to put a quality management system in place shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive. In that context, any harmonised standards referred to in Article 40 of this Regulation shall be taken into account.

Article 18
Obligation to draw up technical documentation

1. Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Article 19
Conformity assessment

1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.

2. For high-risk AI systems referred to in point 5(b) of Annex III that are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.

Article 20
Automatically generated logs

1. Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law.

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation under Articles 74 of that Directive.

(m) 본 항에 열거된 모든 측면과 관련된 경영진 및 기타 직원의 책임을 명시하는 책무성 프레임워크.

2. 1항에 언급된 측면들의 시행은 제공자의 조직 규모에 비례적이어야 한다.

3. 제공자가 Directive 2013/36/EU에 의해 규제되는 신용 기관인 경우, 품질 관리 시스템을 배치해야 할 의무는 동 Directive 제74조에 따른 내부 거버넌스 체계, 프로세스 및 메커니즘에 관한 규칙을 준수함으로써 이행되는 것으로 간주되어야 한다. 이런 맥락에서 본 규정 제40조에 언급된 조화 표준이 고려되어야 한다.

제18조

기술 문서 작성의 의무

1. 고위험 AI 시스템의 제공자는 부속서 IV에 따라 제11조에 언급된 기술 문서를 작성해야 한다.

2. Directive 2013/36/EU에 의해 규제되는 신용 기관인 제공자는 동 Directive 제74조에 따른 내부 거버넌스 체계, 프로세스 및 메커니즘과 관련된 기록의 일부로 기술 문서를 유지해야 한다.

제19조

적합성 평가

1. 고위험 AI 시스템의 제공자는 각자의 시스템이 출시 또는 서비스 개시되기 전에 제43조에 따른 적합성 평가 절차를 거치도록 보장해야 한다. 이러한 적합성 평가에 따라 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하는 것으로 입증된 경우, 제공자는 제48조에 따른 EU 적합성 선언을 작성하고 제49조에 따른 CE 적합성 마크를 부착해야 한다.

2. Directive 2013/36/EU에 의해 규제되는 신용 기관인 제공자가 출시하거나 서비스 개시하는 부속서 III의 5(b)항에 언급된 고위험 AI 시스템의 경우, 동 Directive 제97조에 언급된 절차의 일부로 적합성 평가를 수행해야 한다.

제20조

자동으로 생성되는 로그

1. 고위험 AI 시스템의 제공자는 각자의 고위험 AI 시스템이 자동으로 생성하는 로그를 유지해야 한다. 단, 그러한 로그가 사용자와의 계약 또는 달리 법률에 의해 그들의 통제 하에 있는 경우에 한한다. 로그는 고위험 AI 시스템의 원래 목적과 유럽 연합법 또는 국가법에 따라 적용되는 법적 의무에 비추어 적절한 기간 동안 보관해야 한다.

2. Directive 2013/36/EU에 의해 규제되는 신용 기관인 제공자는 각자의 고위험 AI 시스템이 자동으로 생성하는 로그를 동Directive 제74조에 따른 기록의 일부로 유지해야 한다.

Article 21
Corrective actions

Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly.

Article 22
Duty of information

Where the high-risk AI system presents a risk within the meaning of Article 65(1) and that risk is known to the provider of the system, that provider shall immediately inform the national competent authorities of the Member States in which it made the system available and, where applicable, the notified body that issued a certificate for the high-risk AI system, in particular of the non-compliance and of any corrective actions taken.

Article 23
Cooperation with competent authorities

Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title, in an official Union language determined by the Member State concerned. Upon a reasoned request from a national competent authority, providers shall also give that authority access to the logs automatically generated by the high-risk AI system, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law.

Article 24
Obligations of product manufacturers

Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider.

Article 25
Authorised representatives

1. Prior to making their systems available on the Union market, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union.

2. The authorised representative shall perform the tasks specified in the mandate received from the provider. The mandate shall empower the authorised representative to carry out the following tasks:

제21조

시정 조치

각자가 출시하거나 서비스 개시한 고위험 AI 시스템이 본 규정을 준수하지 않는다고 간주하거나 간주할 이유를 가진 고위험 AI 시스템의 제공자는 상황에 따라 해당 시스템의 준수를 이행하거나 회수 또는 리콜하는 데 필요한 시정 조치를 즉시 취해야 한다. 동 제공자는 해당 고위험 AI 시스템의 유통업자 및 해당될 경우 공인 대리인과 수입업자에게 통지해야 한다.

제22조

통지 의무

고위험 AI 시스템이 제65(1)조의 의미 내에서 위험을 야기하고 그러한 위험이 시스템의 제공자에게 알려진 경우, 동 제공자는 자신이 시스템을 제공한 회원국의 국가 관할 당국과, 해당되는 경우 고위험 AI 시스템에 대한 인증서를 발급한 인증 기관에게 특히 비준수 사실과 취해진 시정 조치를 즉시 통지한다.

제23조

관할 기관과의 협력

국가 관할 기관이 요구할 경우, 고위험 AI 시스템의 제공자는 해당 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 것을 입증하는 데 필요한 모든 정보와 문서를 관련 회원국이 결정하는 유럽 연합 공식 언어로 해당 기관에 제공해야 한다. 또한 국가 관할 기관이 합리적으로 요구할 경우, 제공자는 고위험 AI 시스템이 자동으로 생성한 로그에 대한 접근을 해당 기관에 제공해야 한다. 단, 그러한 로그가 사용자와의 계약 또는 달리 법률에 의해 그들의 통제 하에 있는 경우에 한한다.

제24조

제품 제조업체의 의무

부속서 II의 A절에 열거된 법규가 적용되는 제품과 관련된 고위험 AI 시스템이 동 법규에 따라 제품 제조업체의 명의로 제조된 제품과 함께 출시되거나 서비스 개시되는 경우, 제품의 제조업체는 동 AI 시스템이 본 규정을 준수하도록 보장할 책임을 지고, 동 AI 시스템이 관련된 한에서 현 규정이 제공자에게 부과하는 것과 동일한 의무를 가진다.

제25조

공인 대리인

1. 유럽 연합 외부에서 설립된 제공자는 수입업자를 확인할 수 없는 유럽 연합 시장에 각자의 시스템을 제공하기 전에 서면 위임을 통해 유럽 연합에서 설립된 공인 대리인을 임명한다.
2. 공인 대리인은 공급자로부터 수신한 위임서에 명시된 과업을 수행한다. 위임서는 공인 대리인이 다음 과업을 수행할 수 있는 권한을 수여한다.

(a) keep a copy of the EU declaration of conformity and the technical documentation at the disposal of the national competent authorities and national authorities referred to in Article 63(7);

(b) provide a national competent authority, upon a reasoned request, with all the information and documentation necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law;

(c) cooperate with competent national authorities, upon a reasoned request, on any action the latter takes in relation to the high-risk AI system.

Article 26
Obligations of importers

1. Before placing a high-risk AI system on the market, importers of such system shall ensure that:

(a) the appropriate conformity assessment procedure has been carried out by the provider of that AI system

(b) the provider has drawn up the technical documentation in accordance with Annex IV;

(c) the system bears the required conformity marking and is accompanied by the required documentation and instructions of use.

2. Where an importer considers or has reason to consider that a high-risk AI system is not in conformity with this Regulation, it shall not place that system on the market until that AI system has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the importer shall inform the provider of the AI system and the market surveillance authorities to that effect.

3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable.

4. Importers shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise its compliance with the requirements set out in Chapter 2 of this Title.

5. Importers shall provide national competent authorities, upon a reasoned request, with all necessary information and documentation to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter 2 of this Title in a language which can be easily understood by that national competent authority, including access to the logs automatically generated by the high-risk AI system to the extent such logs are under the control of the provider by virtue of a contractual arrangement with the user or otherwise by law. They shall also cooperate with those authorities on any action national competent authority takes in relation to that system

(a) 제63(7)조에 언급된 국가 관할 기관과 국가 기관이 임의로 처분할 수 있는 EU 적합성 선언과 기술 문서의 사본을 보관한다.

(b) 국가 관할 기관이 합리적으로 요구할 경우, 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 사실을 입증하는 데 필요한 모든 정보와 문서를 제공한다. 여기에는 고위험 AI 시스템이 자동으로 생성한 로그에 대한 접근이 포함된다(그러한 로그가 사용자와의 계약 또는 달리 법률에 의해 그들의 통제 하에 있는 경우).

(c) 관할 국가 기관이 합리적으로 요구할 경우, 고위험 AI 시스템과 관련하여 그들이 취하는 조치에 대해 그들과 협력한다.

제26조
수입업자의 의무

1. 고위험 AI 시스템의 수입업자는 동 시스템을 출시하기 전에 다음 사항을 확인해야 한다.

(a) 동 AI 시스템의 제공자가 적절한 적합성 평가 절차를 수행했는지 여부

(b) 제공자가 부속서 IV에 따른 기술 문서를 작성했는지 여부

(c) 시스템에 필수적인 적합성 마크가 부착되고 필수적인 문서와 사용 지침이 첨부되는지 여부.

2. 수입업자가 고위험 AI 시스템이 본 규정을 준수하지 않는다고 간주하거나 간주할 이유가 있는 경우에는 준수를 이행하기 전까지 동 시스템을 출시해서는 안 된다. 고위험 AI 시스템이 제65(1)조의 의미 내에서 위험을 야기하는 경우 수입업자는 이를 AI 시스템의 제공자와 시장 감시 기관에 통지해야 한다.

3. 수입업자는 그들의 이름, 등록 상표 및 연락 가능한 주소를 고위험 AI 시스템에, 또는 그것이 불가능한 경우 상황에 따라 포장 또는 첨부 문서에 표시해야 한다.

4. 수입업자는 고위험 AI 시스템이 각자의 책임 하에 있는 동안 보관 또는 운송 상태가 본 편 제2장에 명시된 요구사항의 준수를 저해하지 않도록 보장해야 한다.

5. 국가 관할 기관이 합리적으로 요구할 경우, 수입업자는 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 사실을 입증하는 데 필요한 모든 정보와 문서를 동 국가 관할 기관이 쉽게 이해할 수 있는 언어로 제공해야 한다. 여기에는 고위험 AI 시스템이 자동으로 생성한 로그에 대한 접근이 포함된다(그러한 로그가 사용자와의 계약 또는 달리 법률에 의해 제공자의 통제 하에 있는 경우). 아울러 수입업자는 동 시스템과 관련하여 국가 관할 기관이 취하는 모든 조치에 대해 동 기관과 협력해야 한다.

Article 27
Obligations of distributors

1. Before making a high-risk AI system available on the market, distributors shall verify that the high-risk AI system bears the required CE conformity marking, that it is accompanied by the required documentation and instruction of use, and that the provider and the importer of the system, as applicable, have complied with the obligations set out in this Regulation.

2. Where a distributor considers or has reason to consider that a high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title, it shall not make the high-risk AI system available on the market until that system has been brought into conformity with those requirements. Furthermore, where the system presents a risk within the meaning of Article 65(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.

3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, where applicable, storage or transport conditions do not jeopardise the compliance of the system with the requirements set out in Chapter 2 of this Title.

4. A distributor that considers or has reason to consider that a high-risk AI system which it has made available on the market is not in conformity with the requirements set out in Chapter 2 of this Title shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 65(1), the distributor shall immediately inform the national competent authorities of the Member States in which it has made the product available to that effect, giving details, in particular, of the non-compliance and of any corrective actions taken.

5. Upon a reasoned request from a national competent authority, distributors of high- risk AI systems shall provide that authority with all the information and documentation necessary to demonstrate the conformity of a high-risk system with the requirements set out in Chapter 2 of this Title. Distributors shall also cooperate with that national competent authority on any action taken by that authority.

Article 28
Obligations of distributors, importers, users or any other third-party

1. Any distributor, importer, user or other third-party shall be considered a provider for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

   (a) they place on the market or put into service a high-risk AI system under their name or trademark;

   (b) they modify the intended purpose of a high-risk AI system already placed on the market or put into service;

   (c) they make a substantial modification to the high-risk AI system.

2. Where the circumstances referred to in paragraph 1, point (b) or (c), occur, the provider that initially placed the high-risk AI system on the market or put it into service shall no longer be considered a provider for the purposes of this Regulation.

제27조

유통업자의 의무

1. 유통업자는 고위험 AI 시스템을 출시하기 전에 고위험 AI 시스템에 필수 CE 적합성 마크가 부착되었는지, 필수 문서 및 사용 지침이 첨부되었는지, 시스템의 제공자와 수입업자가 본 규정에 명시된 의무를 준수했는지 등을 확인해야 한다.

2. 유통업자가 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하지 않는다고 간주하거나 간주할 이유가 있는 경우에는 그러한 요구사항을 준수하기 전까지 동 시스템을 출시해서는 안 된다. 시스템이 제65(1)조의 의미 내에서 위험을 야기하는 경우 유통업자는 상황에 따라 시스템의 제공자 또는 수입업자에게 이를 통지해야 한다.

3. 유통업자는 고위험 AI 시스템이 각자의 책임 하에 있는 동안 보관 또는 운송 상태가 본 편 제2장에 명시된 요구사항의 준수를 저해하지 않도록 보장해야 한다.

4. 자신이 출시한 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하지 않는다고 간주하거나 간주할 이유가 있는 유통업자는 해당 시스템이 동 요구사항을 준수하도록 하는 데 필요한 시정 조치를 취하거나, 동 시스템을 회수 또는 리콜하거나, 상황에 따라 제공자, 수입업자 또는 관련 운영자가 그러한 시정 조치를 취하도록 보장해야 한다. 고위험 AI 시스템이 제65(1)조의 의미 내에서 위험을 야기하는 경우 유통업자는 자신이 제품을 제공한 회원국의 국가 관할 기관에 이를 즉시 통지하고, 특히 비준수 및 취해진 시정 조치의 세부사항을 제공해야 한다.

5. 국가 관할 기관이 합리적으로 요구할 경우, 고위험 AI 시스템의 유통업자는 해당 고위험 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 것을 입증하는 데 필요한 모든 정보와 문서를 해당 기관에 제공해야 한다. 아울러 유통업자는 해당 국가 관할 기관이 취하는 모든 조치에 대해 동 기관과 협력해야 한다.

제28조

유통업자, 수입업자, 사용자 또는 기타 제3자의 의무

1. 유통업자, 수입업자, 사용자 또는 기타 제3자는 본 규정의 목적을 위해 제공자로 간주되며, 다음과 같은 상황에서 제16조에 따른 제공자의 의무를 져야 한다.

   (a) 자신의 명의 또는 상표로 고위험 AI 시스템을 출시하거나 서비스 개시하는 경우

   (b) 이미 출시되거나 서비스 개시된 고위험 AI 시스템의 원래 목적을 변경하는 경우

   (c) 고위험 AI 시스템을 상당히 개조하는 경우.

2. 제1항 (b)호 또는 (c)호에 언급된 상황이 발생하는 경우, 고위험 AI 시스템을 처음 출시하거나 서비스 개시한 제공자는 더 이상 본 규정의 목적을 위한 제공자로 간주되지 않는다.

Article 29
Obligations of users of high-risk AI systems

1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5.

2. The obligations in paragraph 1 are without prejudice to other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

3. Without prejudice to paragraph 1, to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.

4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.

   For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

5. Users of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high- risk AI system and applicable legal obligations under Union or national law.

   Users that are credit institutions regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.

CHAPTER 4

NOTIFIYING AUTHORITIES AND NOTIFIED BODIES

Article 30
Notifying authorities

1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

2. Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.

제29조

고위험 AI 시스템 사용자의 의무

1. 고위험 AI 시스템의 사용자는 제2항 및 5항에 따라 시스템에 첨부된 사용 지침에 따라 동 시스템을 사용해야 한다.

2. 제1항의 의무는 유럽 연합법 또는 국가법에 따른 사용자의 다른 의무를 침해하지 않으며, 제공자가 명시하는 인간의 감독 조치를 시행하기 위한 목적으로 자체 자원 및 활동을 조직하는 사용자의 재량권을 침해하지 않는다.

3. 제1항을 침해함이 없이, 사용자가 인풋 데이터에 대해 통제력을 행사하는 경우 동 사용자는 인풋 데이터가 고위험 AI 시스템의 원래 목적에 비추어 관련성을 가지도록 보장해야 한다.

4. 사용자는 사용 지침을 토대로 고위험 AI 시스템의 운영을 모니터해야 한다. 사용자가 사용 지침에 따른 사용으로 AI 시스템이 제65(1)조의 의미 내에서 위험을 야기할 수 있다고 간주할 만한 이유가 있는 경우, 동 사용자는 제공자 또는 유통업자에게 통지하고 시스템의 사용을 중단해야 한다. 또한 사용자가 제62조의 의미 내에서 중대한 사건 또는 오작동을 파악한 경우 이를 제공자 또는 유통업자에게 통지하고 AI 시스템의 사용을 중단해야 한다. 사용자가 제공자에게 연락할 수 없는 경우에는 제62조를 준용하여(mutatis mutandis) 적용한다.

   사용자가 Directive 2013/36/EU에 의해 규제되는 신용 기관인 경우, 제1항에 명시된 모니터링 의무는 동 Directive 제74조에 따른 내부 거버넌스 체계, 프로세스 및 메커니즘에 관한 규칙을 준수함으로써 이행되는 것으로 간주되어야 한다.

5. 고위험 AI 시스템의 사용자는 각자의 고위험 AI 시스템이 자동으로 생성하는 로그를 유지해야 한다. 단, 그러한 로그가 그들의 통제 하에 있는 경우에 한한다. 로그는 고위험 AI 시스템의 원래 목적과 유럽 연합법 또는 국가법에 따라 적용되는 법적 의무에 비추어 적절한 기간 동안 보관해야 한다.

   Directive 2013/36/EU에 의해 규제되는 신용 기관인 사용자는 동 Directive 제74조에 따른 내부 거버넌스 체계, 프로세스 및 메커니즘과 관련된 기록의 일부로 로그를 유지해야 한다.

6. 고위험 AI 시스템의 사용자는 제13조에 따라 제공되는 정보를 사용하여 상황에 따라 Regulation (EU) 2016/679 제35조 또는 Directive (EU) 2016/680 제27조에 따른 개인정보 영향 평가를 수행해야 할 의무를 준수해야 한다.

제4장

통보 기관 및 인증 기관

제30조

통보 기관

1. 각 회원국은 적합성 평가 기관의 평가, 지명, 통보 및 모니터링을 위해 필요한 절차를 수립·수행하는 일을 책임지는 통보 기관을 지명하거나 설립한다.

2. 회원국은 Regulation (EC) No 765/2008에 언급된 국가 인가 기관(accreditation body)을 통보 기관으로 지명할 수 있다.

3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies and the objectivity and impartiality of their activities are safeguarded.

4. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.

5. Notifying authorities shall not offer or provide any activities that conformity assessment bodies perform or any consultancy services on a commercial or competitive basis.

6. Notifying authorities shall safeguard the confidentiality of the information they obtain.

7. Notifying authorities shall have a sufficient number of competent personnel at their disposal for the proper performance of their tasks.

8. Notifying authorities shall make sure that conformity assessments are carried out in a proportionate manner, avoiding unnecessary burdens for providers and that notified bodies perform their activities taking due account of the size of an undertaking, the sector in which it operates, its structure and the degree of complexity of the AI system in question.

Article 31
Application of a conformity assessment body for notification

1. Conformity assessment bodies shall submit an application for notification to the notifying authority of the Member State in which they are established.

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 33. Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 33. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations may be used to support their designation procedure under this Regulation, as appropriate.

Article 32
Notification procedure

1. Notifying authorities may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 33.

2. Notifying authorities shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

3. 통보 기관은 적합성 평가 기관과의 이해 충돌이 발생하지 않고 활동의 객관성과 공평성이 보호되는 방식으로 설립, 조직, 운영되어야 한다.

4. 통보 기관은 적합성 평가 기관의 통지와 관련된 사안이 동 기관의 평가를 수행하는 사람과 다른 담당자에 의해 결정되는 방식으로 조직되어야 한다.

5. 통보 기관은 적합성 평가 기관이 수행하는 활동 또는 상업적·경쟁적 성격의 컨설팅 서비스를 제의하거나 제공해서는 안 된다.

6. 통보 기관은 그들이 획득하는 정보의 기밀을 보호해야 한다.

7. 통보 기관은 적절한 과업 수행을 위해 재량껏 이용할 수 있는 충분한 수의 담당 직원을 보유해야 한다.

8. 통보 기관은 제공자에게 불필요한 부담을 주지 않으면서 균형 잡힌 방식으로 적합성 평가가 수행되고 인증 기관(notified body)이 사업의 규모, 그것이 운영되는 분야, 그 구조, 해당 AI 시스템의 복잡성 수준 등을 충분히 고려하여 활동을 수행하도록 보장해야 한다.

제31조

적합성 평가 기관의 인증 신청

1. 적합성 평가 기관은 인증(notification) 신청서를 그들이 설립된 회원국의 통보 기관에 제출해야 한다.

2. 인증 신청서에는 적합성 평가 활동, 적합성 평가 모듈, 적합성 평가 기관이 능숙하다고 주장하는 인공 지능 기술 등에 대한 설명과 적합성 평가 기관이 제33조에 명시된 요구사항을 충족한다는 사실을 입증하는 국가 인가 기관이 발급한 인가 증명서(존재할 경우) 등이 첨부되어야 한다. 아울러, 기타 유럽 연합 조화 법령에 따른 신청 인증 기관의 지명과 관련된 유효한 문서가 추가되어야 한다.

3. 적합성 평가 기관이 인가 증명서를 제출할 수 없는 경우 동 기관이 제33조에 명시된 요구사항을 준수하는지 여부의 검증, 인정 및 정기 모니터링에 필요한 증거 서류를 통보 기관에 제공해야 한다. 기타 유럽 연합 조화 법령에 따라 지명된 인증 기관의 경우, 그러한 지명과 관련된 모든 문서와 증명서를 사용하여 본 규정에 따른 지명 절차를 뒷받침할 수 있다.

제32조

통보 절차

1. 통보 기관은 오로지 제33조에 명시된 요구사항을 충족한 적합성 평가 기관만을 인증(notify)할 수 있다.

2. 통보 기관은 유럽연합 집행위원회가 개발·관리하는 전자 통지 도구를 사용하여 유럽연합 집행위원회 및 기타 회원국에 통보해야 한다.

3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies concerned.

4. The conformity assessment body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within one month of a notification.

5. Notifying authorities shall notify the Commission and the other Member States of any subsequent relevant changes to the notification.

Article 33
Notified bodies

1. Notified bodies shall verify the conformity of high-risk AI system in accordance with the conformity assessment procedures referred to in Article 43.

2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks.

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall be such as to ensure that there is confidence in the performance by and in the results of the conformity assessment activities that the notified bodies conduct.

4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which it performs conformity assessment activities. Notified bodies shall also be independent of any other operator having an economic interest in the high- risk AI system that is assessed, as well as of any competitors of the provider.

5. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

6. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies respect the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out.

7. Notified bodies shall have procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the AI system in question.

8. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State concerned in accordance with national law or that Member State is directly responsible for the conformity assessment.

9. Notified bodies shall be capable of carrying out all the tasks falling to them under this Regulation with the highest degree of professional integrity and the requisite

3. 통보에는 적합성 평가 활동, 적합성 평가 모듈, 관련 인공 지능 기술 등의 완전한 세부사항이 포함되어야 한다.

4. 관련 적합성 평가 기관은 오로지 통보 후 1개월 이내에 유럽연합 집행위원회 또는 기타 회원국이 이의를 제기하지 않는 경우에만 인증 기관의 활동을 수행할 수 있다.

5. 통보 기관은 통보와 관련된 차후의 변경을 유럽연합 집행위원회와 기타 회원국에 통지해야 한다.

제33조
인증 기관

1. 인증 기관(notified body)은 제43조에 언급된 적합성 평가 절차에 따라 고위험 AI 시스템의 적합성을 확인한다.

2. 인증 기관은 각자의 과업을 이행하는 데 필요한 조직, 품질 관리, 자원 및 프로세스 요구사항을 충족해야 한다.

3. 인증 기관의 조직 구조, 책임 할당, 보고 체계 및 운영은 인증 기관이 수행하는 적합성 평가 활동과 그 결과에 대해 신뢰를 주는 방식으로 이루어져야 한다.

4. 인증 기관은 적합성 평가 활동의 대상인 고위험 AI 시스템의 제공자와 독립되어 있어야 한다. 아울러 인증 기관은 평가 대상인 고위험 AI 시스템에 경제적 이해를 가지는 기타 운영자 및 제공자의 경쟁업체와 독립되어 있어야 한다.

5. 인증 기관은 그 활동의 독립성, 객관성, 공평성을 보호하도록 조직·운영되어야 한다. 인증 기관은 그 조직, 인사 및 평가 활동 전반에 걸쳐 공평성을 보호하고 공평성의 원칙을 촉진·적용하기 위한 구조와 절차를 문서화하고 시행해야 한다.

6. 인증 기관은 그 직원, 위원회, 자회사, 하청인 및 관련 기관 또는 외부 기관의 직원들이 적합성 평가 활동을 수행하는 과정에서 소유하게 되는 정보의 기밀을 유지하도록(단, 법률에 의해 공개가 요구되는 경우는 예외) 보장하는 문서화된 절차를 확립해야 한다. 인증 기관의 직원은 본 규정에 따른 과업을 수행하는 과정에서 획득한 모든 정보와 관련된 직무상 비밀을 엄수해야 한다. 단, 그들이 활동을 수행하는 회원국의 통보 기관과 관련된 것은 예외로 한다.

7. 인증 기관은 사업의 규모, 그것이 운영되는 분야, 그 구조, 해당 AI 시스템의 복잡성 수준 등을 충분히 고려한 활동 수행을 위한 절차를 수립해야 한다.

8. 인증 기관은 그들의 적합성 평가 활동에 대해 적절한 책임 보험을 확보해야 한다. 단, 국가 법률에 따라 관련 회원국이 책임을 지거나 동 회원국이 적합성 평가를 직접 책임지는 경우는 예외로 한다.

9. 인증 기관은 본 규정에 따라 그들에게 귀속되는 모든 과업을, 인증 기관이 직접 수행하는지 또는 그들을 대신하여 그들의 책임 하에 수행되는지 여부와 관계없이, 최고

competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their responsibility.

10. Notified bodies shall have sufficient internal competences to be able to effectively evaluate the tasks conducted by external parties on their behalf. To that end, at all times and for each conformity assessment procedure and each type of high-risk AI system in relation to which they have been designated, the notified body shall have permanent availability of sufficient administrative, technical and scientific personnel who possess experience and knowledge relating to the relevant artificial intelligence technologies, data and data computing and to the requirements set out in Chapter 2 of this Title.

11. Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly or be represented in European standardisation organisations, or ensure that they are aware and up to date in respect of relevant standards.

12. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 30 to allow it to conduct its assessment, designation, notification, monitoring and surveillance activities and to facilitate the assessment outlined in this Chapter.

Article 34
Subsidiaries of and subcontracting by notified bodies

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 33 and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever these are established.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider.

4. Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.

Article 35
Identification numbers and lists of notified bodies designated under this Regulation

1. The Commission shall assign an identification number to notified bodies. It shall assign a single number, even where a body is notified under several Union acts.

2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been assigned to them and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.

수준의 직업적 성실성과 특정 분야에 필수적인 역량을 가지고 수행할 수 있어야 한다.

10. 인증 기관은 외부 당사자가 그들을 대신하여 수행하는 과업을 효과적으로 평가할 수 있는 충분한 내부 역량을 갖추어야 한다. 이를 위해 언제나 그리고 그들이 담당하는 각 유형의 고위험 AI 시스템과 적합성 평가에 대해, 인증 기관은 관련 인공 지능 기술, 데이터 및 데이터 컴퓨팅, 그리고 본 편 제2장에 명시된 요구사항과 관련한 경험과 지식을 보유한 충분한 행정, 기술, 과학 인력을 상시 동원할 수 있어야 한다.

11. 인증 기관은 제38조에 언급된 협조 활동에 참여해야 한다. 아울러 유럽 표준화 기구에 직접 참여하거나, 대표를 파견하거나, 또는 관련된 최신의 표준을 인지해야 한다.

12. 인증 기관은 제30조에 언급된 통보 기관이 평가, 지명, 통보, 모니터링, 감시 활동을 수행하고 본 장에 약술된 평가를 촉진할 수 있도록 지원하기 위해, 해당 통보 기관이 요구할 경우 제공자의 문서 기록을 포함한 모든 관련 문서 기록을 제출해야 한다.

제34조

인증 기관의 자회사 및 하청인

1. 인증 기관이 적합성 평가와 관련된 특정 과업을 하청하거나 자회사에 의뢰하는 경우, 동 기관은 하청인 또는 자회사가 제33조에 명시된 요구사항을 충족하도록 보장하고 이를 통보 기관에 통지한다.

2. 인증 기관은 하청인 또는 자회사가 설립된 경우 이들이 수행하는 과업에 대해 전적인 책임을 진다.

3. 제공자의 동의가 있어야만 활동을 하청하거나 자회사에 의뢰할 수 있다.

4. 인증 기관은 하청인 또는 자회사의 자격 평가 및 본 규정에 따라 그들이 수행하는 작업과 관련된 문서를 통보 기관이 처분할 수 있도록 보관해야 한다.

제35조

본 규정에 따라 지명된 인증 기관의 식별 번호 및 목록

1. 유럽연합 집행위원회는 인증 기관에 식별 번호를 할당한다. 하나의 기관이 여러 개의 유럽 연합법에 따라 인증된 경우에도 하나의 번호가 할당된다.

2. 유럽연합 집행위원회는 본 규정에 따라 인증된 기관들의 목록과 그들에게 할당된 식별 번호 및 인증의 대상이 된 활동을 공개해야 한다. 유럽연합 집행위원회는 목록을 최신으로 유지해야 한다.

Article 36
Changes to notifications

1. Where a notifying authority has suspicions or has been informed that a notified body no longer meets the requirements laid down in Article 33, or that it is failing to fulfil its obligations, that authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body investigation no longer meets the requirements laid down in Article 33 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the notification as appropriate, depending on the seriousness of the failure. It shall also immediately inform the Commission and the other Member States accordingly.

2. In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying authority shall take appropriate steps to ensure that the files of that notified body are either taken over by another notified body or kept available for the responsible notifying authorities at their request.

Article 37
Challenge to the competence of notified bodies

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt whether a notified body complies with the requirements laid down in Article 33.

2. The Notifying authority shall provide the Commission, on request, with all relevant information relating to the notification of the notified body concerned.

3. The Commission shall ensure that all confidential information obtained in the course of its investigations pursuant to this Article is treated confidentially.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements laid down in Article 33, it shall adopt a reasoned decision requesting the notifying Member State to take the necessary corrective measures, including withdrawal of notification if necessary. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 38
Coordination of notified bodies

1. The Commission shall ensure that, with regard to the areas covered by this Regulation, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures of AI systems pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies**.**

2. Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

제36조

인증의 변경

1. 인증 기관이 제33조에 명시된 요구사항을 더 이상 충족하지 않거나 의무를 이행하지 않는 것으로 의심되거나 통지를 받는 경우 통보 기관은 지체 없이 최대한 성실하게 문제를 조사한다. 이러한 맥락에서 통보 기관은 제기된 이의에 대해 관련 인증 기관에 통지하고 동 인증 기관이 자신의 견해를 밝힐 수 있는 기회를 제공해야 한다. 인증 기관이 제33조에 명시된 요구사항을 더 이상 충족하지 않거나 의무를 이행하지 않는다는 결론에 이를 경우, 통보 기관은 불이행의 중대성에 따라 적절히 인증을 제한, 정지 또는 취소해야 한다. 아울러, 이를 즉시 유럽연합 집행위원회 및 기타 회원국에 통지해야 한다.

2. 인증을 제한, 정지 또는 취소하거나 인증 기관이 활동을 중지하는 경우, 통보 기관은 해당 인증 기관의 파일이 다른 인증 기관에 의해 인수되거나 담당 통보 기관이 요구 시 이용할 수 있도록 보장하기 위해 적절한 조치를 취한다.

제37조

인증 기관의 권한에 대한 이의 제기

1. 유럽연합 집행위원회는 필요한 경우 인증 기관이 제33조에 명시된 요구사항을 준수하는지 여부를 의심할 이유가 있는 모든 사례를 조사한다.

2. 통보 기관은 유럽연합 집행위원회가 요구할 경우 관련 인증 기관의 인증과 관련된 모든 정보를 제공한다.

3. 유럽연합 집행위원회는 본 조항에 따른 수사 과정에서 획득한 모든 기밀 정보가 기밀로 취급되도록 보장해야 한다.

4. 인증 기관이 제33조에 명시된 요구조항을 충족하지 않거나 더 이상 충족하지 않는다는 것을 확인하는 경우, 유럽연합 집행위원회는 통보(notifying) 회원국에 대해 필요한 경우 인증의 취소를 포함하여 필요한 시정 조치를 취할 것을 요구하는 합리적 결정을 채택해야 한다. 그러한 실행 규정(implementing act)은 제74(2)조에 언급된 심사 절차에 따라 채택되어야 한다.

제38조

인증 기관의 협력

1. 유럽연합 집행위원회는 본 규정이 적용되는 영역에서, 본 규정에 따른 AI 시스템의 적합성 평가 절차에 참여하는 인증 기관들 간에 적절한 조율과 협력이 이루어지고 부문별 인증 기관 그룹의 형태로 적절히 운영되도록 보장해야 한다.

2. 회원국은 그들이 인증한 기관이 해당 그룹의 작업에 직접 또는 지명된 대리인을 통해 참여하도록 보장한다.

Article 39
Conformity assessment bodies of third countries

Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified Bodies under this Regulation.

CHAPTER 5

STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION

Article 40
Harmonised standards

High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements.

Article 41
Common specifications

1. Where harmonised standards referred to in Article 40 do not exist or where the Commission considers that the relevant harmonised standards are insufficient or that there is a need to address specific safety or fundamental right concerns, the Commission may, by means of implementing acts, adopt common specifications in respect of the requirements set out in Chapter 2 of this Title. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

2. The Commission, when preparing the common specifications referred to in paragraph 1, shall gather the views of relevant bodies or expert groups established under relevant sectorial Union law.

3. High-risk AI systems which are in conformity with the common specifications referred to in paragraph 1 shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those common specifications cover those requirements.

4. Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that are at least equivalent thereto.

Article 42
Presumption of conformity with certain requirements

1. Taking into account their intended purpose, high-risk AI systems that have been trained and tested on data concerning the specific geographical, behavioural and functional setting within which they are intended to be used shall be presumed to be in compliance with the requirement set out in Article 10(4).

제39조

제3국의 적합성 평가 기관

유럽 연합이 계약을 체결한, 제3국의 법률에 따라 설립된 적합성 평가 기관은 본 규정에 따른 인증 기관의 활동을 수행할 권한을 부여받을 수 있다.

제5장

표준, 적합성 평가, 인증서, 등록

제40조

조화 표준

유럽 연합 관보에 그 참조가 게재된 조화 표준 또는 그 일부를 준수하는 고위험 AI 시스템은 본 편 제2장에 명시된 요구사항을 준수하는 것으로 추정된다(단, 그러한 표준에 동 요구사항이 포함되는 경우).

제41조

공통 규격

1. 제40조에 언급된 조화 표준이 존재하지 않거나 유럽연합 집행위원회가 관련 조화 표준이 불충분하거나 특정한 안전 또는 기본권 문제를 해결할 필요가 있다고 간주하는 경우, 유럽연합 집행위원회는 실행 규정을 통해 본 편 제2장에 명시된 요구사항과 관련한 공통 규격을 채택할 수 있다. 이러한 실행 규정은 제74(2)조에 언급된 심사 절차에 따라 채택될 수 있다.

2. 유럽연합 집행위원회는 제1항에 언급된 공통 규격을 작성할 때 관련 부문별 유럽 연합법에 따라 설립된 관련 기관 또는 전문가 그룹의 견해를 수렴해야 한다.

3. 1항에 언급된 공통 규격을 준수하는 고위험 AI 시스템은 본 편 제2장에 명시된 요구사항을 준수하는 것으로 추정된다(단, 그러한 공통 규격에 동 요구사항이 포함하는 경우).

4. 제공자가 제1항에 언급된 공통 규격을 준수하지 않는 경우에는 그와 적어도 동등한 기술 솔루션을 채택했음을 적절한 절차에 따라 정당화해야 한다.

제42조

특정 요구사항의 준수 추정

1. 특정한 지리적, 행동적, 기능적 환경과 관련한 데이터를 통해 학습과 테스트를 거친 고위험 AI 시스템은 그 원래 목적을 고려하여 제10(4)조에 명시된 요구사항을 준수하는 것으로 추정된다.

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[63] and the references of which have been published in the Official Journal of the European Union shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

Article 43
Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

   (a) the conformity assessment procedure based on internal control referred to in Annex VI;

   (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

   Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

   For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

2. For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body. For high-risk AI systems referred to in point 5(b) of Annex III, placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU, the conformity assessment shall be carried out as part of the procedure referred to in Articles 97 to101 of that Directive.

3. For high-risk AI systems, to which legal acts listed in Annex II, section A, apply, the provider shall follow the relevant conformity assessment as required under those legal acts. The requirements set out in Chapter 2 of this Title shall apply to those

[63] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 1).

2. 유럽 의회 및 유럽 이사회 Regulation (EU) 2019/881[63]에 의거한 사이버 보안 제도에 따라 인증서 또는 적합성 확인서가 발급되고 유럽 연합 관보에 그 참조가 게재된 고위험 AI 시스템은 본 규정 제15조에 명시된 사이버 보안 요구사항을 준수하는 것으로 추정된다(단, 사이버 보안 인증서 또는 적합성 확인서에 그러한 요구사항이 포함되는 경우).

제43조

적합성 평가

1. 부속서 III의 제1항에 열거된 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 사실을 입증하기 위해 제공자가 제40조에 언급된 조화 표준 또는 해당되는 경우 제41조에 언급된 공통 규격을 적용한 경우에는 다음 절차 중 하나를 따라야 한다.

   (a) 부속서 VI에 언급된 내부 관리에 기초한 적합성 평가 절차

   (b) 부속서 VII에 언급된, 인증 기관이 참여하는 품질 관리 시스템의 평가와 기술 문서의 평가에 기초한 적합성 평가 절차.

   고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 사실을 입증하기 위해 제공자가 제40조에 언급된 조화 표준을 적용하지 않거나 일부만 적용한 경우, 또는 그러한 조화 표준이 존재하지 않고 제41조에 언급된 공통 규격을 적용할 수 없는 경우, 제공자는 부속서 VII에 명시된 적합성 평가 절차를 따른다.

   부속서 VII에 언급된 적합성 평가 절차의 목적을 위해 제공자는 인증 기관을 임의로 선택할 수 있다. 단, 법 집행을 통해 시스템이 서비스 개시되는 경우, 이주·망명 당국 및 EU 기관, 기구, 단체, 또는 제63(5)조 또는 (6)조에 언급된 시장 감시 기관이 인증 기관 역할을 수행한다.

2. 부속서 III의 2~8항에 언급된 고위험 AI 시스템의 경우, 제공자는 인증 기관의 참여를 규정하지 않는, 부속서 VI에 언급된 내부 관리에 기초한 적합성 평가 절차를 따른다. Directive 2013/36/EU에 의해 규제되는 신용 기관이 출시하거나 서비스 개시하는 부속서 III의 5(b)항에 언급된 고위험 AI 시스템의 경우 적합성 평가 절차는 동 Directive 제97~101조에 언급된 절차의 일부로 수행된다.

3. 부속서 II의 A절에 열거된 법규가 적용되는 고위험 AI 시스템의 경우, 제공자는 동 법규에 따라 요구되는 관련 적합성 평가를 따른다. 이러한 고위험 AI 시스템에는 본 편 제2장에 명시된 요구사항이 적용되며 상기한 평가의

[63] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 1).

high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.

For the purpose of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Chapter 2 of this Title, provided that the compliance of those notified bodies with requirements laid down in Article 33(4), (9) and (10) has been assessed in the context of the notification procedure under those legal acts.

Where the legal acts listed in Annex II, section A, enable the manufacturer of the product to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may make use of that option only if he has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering the requirements set out in Chapter 2 of this Title.

4. High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user.

For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

5. The Commission is empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating Annexes VI and Annex VII in order to introduce elements of the conformity assessment procedures that become necessary in light of technical progress.

6. The Commission is empowered to adopt delegated acts to amend paragraphs 1 and 2 in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimizing the risks to health and safety and protection of fundamental rights posed by such systems as well as the availability of adequate capacities and resources among notified bodies.

Article 44
Certificates

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in an official Union language determined by the Member State in which the notified body is established or in an official Union language otherwise acceptable to the notified body.

2. Certificates shall be valid for the period they indicate, which shall not exceed five years. On application by the provider, the validity of a certificate may be extended for further periods, each not exceeding five years, based on a re-assessment in accordance with the applicable conformity assessment procedures.

3. Where a notified body finds that an AI system no longer meets the requirements set out in Chapter 2 of this Title, it shall, taking account of the principle of

일부가 된다. 이와 함께 부속서 II의 제4.3항, 4.4항, 4.5항과 제4.6항 5호가 적용된다.

이러한 평가의 목적을 위해, 상기한 법규에 따라 인증된 인증 기관은 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수하도록 관리할 권한을 가진다. 단, 동 인증 기관이 제33(4), (9), (10)조에 명시된 요구사항을 준수하는지 여부는 동 법규에 따른 인증 절차의 맥락에서 평가되어야 한다.

부속서 II의 A절에 열거된 법규에 제품의 제조업체가 모든 관련 요구사항을 포함하는 모든 조화 표준을 적용한 경우에 한하여 동 제조업체가 제3자 적합성 평가를 옵트아웃할 수 있도록 규정된 경우, 동 제조업체는 본 편 제2장에 명시된 요구사항을 포함하는 조화 표준 또는 해당되는 경우 제41조에 언급된 공통 규격을 적용한 경우에만 해당 옵션을 사용할 수 있다.

4. 고위험 AI 시스템이 상당히 수정될 때마다, 수정된 시스템이 추가로 유통될 것인지 또는 현재 사용자에 의해 계속 사용될 것인지 여부에 관계없이, 새로운 적합성 평가 절차를 거쳐야 한다.

출시되거나 서비스 개시된 후에도 계속 학습하는 고위험 AI 시스템의 경우, 초기 적합성 평가 시에 제공자가 사전 결정하고 부속서 IV의 2(f)항에 언급된 기술 문서에 포함된 정보의 일부인 고위험 AI 시스템 및 그 성능의 변경은 상당한 수정에 해당되지 않는다.

5. 유럽연합 집행위원회는 기술 진보에 따라 필요하게 되는 적합성 평가 절차의 요소들을 도입하기 위해 부속서 VI 및 VII를 업데이트하기 위한 목적으로 제73조에 따른 위임 규정을 채택할 권한을 가진다.

6. 유럽연합 집행위원회는 부속서 III의 제2~8항에 언급된 고위험 AI 시스템에 부속서 II에 언급된 적합성 평가 절차 또는 그 일부를 적용하기 위해 제1항 및 2항을 수정하는 위임 규정을 채택할 권한을 가진다. 유럽연합 집행위원회는 부속서 VI에 언급된 내부 관리에 기초한 적합성 평가 절차가 상기한 시스템이 야기하는 건강과 안전 및 기본권 보호에 대한 위험을 방지하거나 최소화하는 효과와 인증 단체들이 충분한 역량과 자원을 확보할 수 있는지 여부를 고려하여 상기한 위임 규정을 채택해야 한다.

제44조

인증서

1. 부속서 VII에 따라 인증 기관이 발급하는 인증서는 인증 기관이 설립된 회원국이 결정하거나 달리 인증 기관이 받아들일 수 있는 유럽 연합 공식 언어로 작성되어야 한다.

2. 인증서는 인증 기관이 명시하는 5년을 초과하지 않는 기간 동안 유효해야 한다. 제공자가 신청할 경우, 해당 적합성 평가 절차에 따른 재평가를 토대로 인증서의 유효 기간을 각각 5년을 초과하지 않는 추가 기간 동안 연장할 수 있다.

3. 특정한 AI 시스템이 본 편 제2장에 명시된 요구사항을 더 이상 충족하지 않는다고 판단되는 경우 인증 기관은 비례성의 원칙을 고려하여 발급된 인증서를 일시 중지 또는

proportionality, suspend or withdraw the certificate issued or impose any restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.

Article 45
Appeal against decisions of notified bodies

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available to parties having a legitimate interest in that decision.

Article 46
Information obligations of notified bodies

1. Notified bodies shall inform the notifying authority of the following:
   (a) any Union technical documentation assessment certificates, any supplements to those certificates, quality management system approvals issued in accordance with the requirements of Annex VII;
   (b) any refusal, restriction, suspension or withdrawal of a Union technical documentation assessment certificate or a quality management system approval issued in accordance with the requirements of Annex VII;
   (c) any circumstances affecting the scope of or conditions for notification;
   (d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;
   (e)) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.
2. Each notified body shall inform the other notified bodies of:
   (a)) quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued;
   (b) EU technical documentation assessment certificates or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.
3. Each notified body shall provide the other notified bodies carrying out similar conformity assessment activities covering the same artificial intelligence technologies with relevant information on issues relating to negative and, on request, positive conformity assessment results.

Article 47
Derogation from conformity assessment procedure

1. By way of derogation from Article 43, any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period of time, while the necessary conformity

취소하거나 그에 대해 제한을 부과해야 한다. 단, 시스템의 제공자가 인증 기관이 정한 적절한 기한 내에 적절한 시정 조치를 취하여 그러한 요구사항의 준수를 보장하는 경우는 예외로 한다. 인증 기관은 그러한 결정의 이유를 밝혀야 한다.

제45조

인증 기관의 결정에 대한 항의

회원국은 인증 기관의 결정에 적법한 이해를 가지는 당사자가 동 결정에 대한 항의 절차를 이용할 수 있도록 보장한다.

제46조

인증 기관의 정보 제공 의무

1. 인증 기관은 통보 기관에게 다음 정보를 제공해야 한다.

   (a) 부속서 VII의 요구사항에 따라 발급된 유럽 연합 기술 문서 평가 인증서, 동 인증서의 추록, 품질 관리 시스템 승인

   (b) 부속서 VII의 요구사항에 따라 발급된 유럽 연합 기술 문서 평가 인증서 또는 품질 관리 시스템 승인의 거부, 제한, 일시 중지 또는 취소

   (c) 인증(notification)의 범위 또는 조건에 영향을 미치는 상황

   (d) 적합성 평가 활동과 관련하여 시장 감시 기관으로부터 수신한 정보 요청

   (e) 요청 시, 인증의 범위 내에서 수행한 적합성 평가 활동 또는 국가간 활동 및 하청 계약을 포함한 기타 활동

2. 각 인증 기관은 다른 인증 기관에게 다음 정보를 제공해야 한다.

   (a) 자신이 거부, 일시 중지 또는 취소한 품질 관리 시스템 승인, 그리고 요청 시 자신이 발급한 품질 시스템 승인

   (b) 자신이 거부, 취소, 일시 중지 또는 달리 제한한 EU 기술 문서 평가 인증서 또는 그 추록, 그리고 요청 시 자신이 발급한 인증서 및/또는 그 추록

3. 각 인증 기관은 동일한 인공 지능 기술을 포함하는 유사한 적합성 평가 활동을 수행하는 다른 인증 기관에게 부정적 및 (요청 시) 긍정적인 적합성 평가 결과와 관련된 문제에 관한 정보를 제공해야 한다.

제47조

적합성 평가 절차의 예외적용

1. 시장 감시 기관은 제43조에 대한 법적예외허용을 통해, 공공 안전 또는 개인의 생명과 건강의 보호, 환경의 보호, 주요 산업 및 인프라 자산의 보호 등 예외적인 이유로 관련 회원국의 영토 내에서 특정 고위험 AI 시스템을 출시하거나 서비스 개시하는 것을 허가할 수 있다. 이러한 허가는 필요한 적합성 평가 절차가 수행되는

assessment procedures are being carried out, and shall terminate once those procedures have been completed. The completion of those procedures shall be undertaken without undue delay.

2. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.

3. Where, within 15 calendar days of receipt of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.

4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 2 to be unfounded, the Commission shall without delay enter into consultation with the relevant Member State; the operator(s) concerned shall be consulted and have the possibility to present their views. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant operator or operators.

5. If the authorisation is considered unjustified, this shall be withdrawn by the market surveillance authority of the Member State concerned.

6. By way of derogation from paragraphs 1 to 5, for high-risk AI systems intended to be used as safety components of devices, or which are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.

Article 48
EU declaration of conformity

1. The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union legislations applicable to the

제한된 기간 동안 지속되고 그러한 절차가 완료되는 즉시 종료된다. 그러한 절차는 불합리한 지체 없이 완료되어야 한다.

2. 시장 감시 기관은 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다고 판단하는 경우에만 제1항에 언급된 허가를 발급해야 한다. 시장 감시 기관은 제1항에 따라 발급한 허가에 대해 유럽연합 집행위원회와 다른 회원국에 통지한다.

3. 회원국 또는 유럽연합 집행위원회가 제2항에 언급된 통지를 수신한 후 15역일 이내에 제1항에 따라 회원국의 시장 감시 기관이 발급한 허가와 관련하여 아무런 이의를 제기하지 않는 경우 동 허가는 정당화된 것으로 간주된다.

4. 2항에 언급된 통지를 수신한 후 15역일 이내에 회원국이 다른 회원국의 시장 감시 기관이 발급한 허가에 대해 이의를 제기하거나, 또는 유럽연합 집행위원회가 동 허가가 유럽 연합법에 위배되거나 제2항에 언급된 시스템의 준수와 관련한 회원국의 결론이 근거 없다고 간주하는 경우, 유럽연합 집행위원회는 지체 없이 관련 회원국과 협의를 벌여야 한다. 관련 운영자는 협의에 응하고 각자의 의견을 제시할 수 있다. 유럽연합 집행위원회는 이를 고려하여 허가가 정당한지 여부를 결정한다. 유럽연합 집행위원회는 이러한 결정을 관련 회원국과 관련 운영자에게 통지한다.

5. 허가가 정당하지 않다고 간주되는 경우 관련 회원국의 시장 감시 기관은 이를 취소해야 한다.

6. 제1~5항의 개정을 통해, Regulation (EU) 2017/745 및 Regulation (EU) 2017/746이 적용되는 장치의 안전 구성요소로 사용되거나 그 자체가 장치인 고위험 AI 시스템의 경우, 본 편 제2장에 명시된 요구사항의 준수에 대한 적합성 평가의 개정과 관련하여 Regulation (EU) 2017/745 제59조 및 Regulation (EU) 2017/746 제54조가 적용된다.

제48조

EU 자기적합성 선언

1. 제공자는 각 AI 시스템에 대해 EU 적합성 선언서를 작성하고 AI 시스템이 출시되거나 서비스 개시된 후 10년간 국가 관할 당국이 처분할 수 있도록 보관해야 한다. EU 적합성 선언은 작성 대상이 된 AI 시스템을 밝혀야 한다. 관련 국가 관할 기관이 요청할 경우 EU 적합성 선언서 사본을 제공해야 한다.

2. EU 적합성 선언은 문제의 고위험 AI 시스템이 본 편 제2장에 명시된 요구사항을 준수한다는 것을 언명해야 한다. EU 적합성 선언에는 부속서 V에 명시된 정보가 포함되어야 하며 유럽 연합 공식 언어 또는 고위험 AI 시스템이 제공된 회원국이 요구하는 언어로 번역되어야 한다.

3. 고위험 AI 시스템에 역시 EU 적합성 선언을 요구하는 다른 유럽 연합 조화 법령이 적용되는 경우, 해당 고위험 AI 시스템에 적용되는 모든 유럽 연합

high-risk AI system. The declaration shall contain all the information required for identification of the Union harmonisation legislation to which the declaration relates.

4. By drawing up the EU declaration of conformity, the provider shall assume responsibility for compliance with the requirements set out in Chapter 2 of this Title. The provider shall keep the EU declaration of conformity up-to-date as appropriate.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 73 for the purpose of updating the content of the EU declaration of conformity set out in Annex V in order to introduce elements that become necessary in light of technical progress.

Article 49
CE marking of conformity

1. The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.

2. The CE marking referred to in paragraph 1 of this Article shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

3. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

Article 50
Document retention

The provider shall, for a period ending 10 years after the AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

(a) the technical documentation referred to in Article 11;

(b) the documentation concerning the quality management system referred to Article 17;

(c) the documentation concerning the changes approved by notified bodies where applicable;

(d) the decisions and other documents issued by the notified bodies where applicable;

(e) the EU declaration of conformity referred to in Article 48.

Article 51
Registration

Before placing on the market or putting into service a high-risk AI system referred to in Article 6(2), the provider or, where applicable, the authorised representative shall register that system in the EU database referred to in Article 60.

법규에 대해 하나의 EU 적합성 선언을 작성해야 한다. 선언에는 그와 관련된 모든 유럽 연합 조화 법령의 식별에 필요한 모든 정보가 포함되어야 한다.

4. 제공자는 EU 적합성 선언을 작성함으로써 본 편 제2장에 명시된 요구사항을 준수할 책임을 진다. 제공자는 적절한 경우 EU 적합성 선언을 최신으로 유지해야 한다.

5. 유럽연합 집행위원회는 기술 발전에 따라 필요하게 되는 요소들을 도입하기 위해 부속서 V에 명시된 EU 적합성 선언의 내용을 업데이트하기 위한 목적으로 제73조에 따른 위임 규정을 채택할 권한을 가진다.

제49조

CE 적합성 마크

1. CE 마크는 고위험 AI 시스템에 눈에 띄게, 읽기 쉽게, 지워지지 않게 부착해야 한다. 이것이 가능하지 않거나 고위험 AI 시스템의 성격 때문에 곤란한 경우에는 상황에 따라 포장이나 첨부 문서에 부착한다.

2. 본 조 제1항에 언급된 CE 마크에는 Regulation (EC) No 765/2008 제30조에 명시된 일반 원칙이 적용된다.

3. 적절한 경우, CE 마크 옆에 43조에 명시된 적합성 평가 절차를 책임지는 인증 기관의 식별 번호를 표시한다. 식별 번호는 고위험 AI 시스템이 CE 마크의 요구사항을 충족한다고 언급하는 판촉 자료에도 표시되어야 한다.

제50조

문서 보존

제공자는 AI 시스템이 출시되거나 서비스 개시된 지 10년 후에 종료되는 기간 동안 국가 관할 기관이 처분할 수 있도록 다음 문서를 보관해야 한다.

(a) 제11조에 언급된 기술 문서

(b) 제17조에 언급된 품질 관리 시스템과 관련된 문서

(c) 해당되는 경우 인증 기관이 승인한 변경과 관련된 문서

(d) 해당되는 경우 인증 기관이 발급한 결정 및 기타 문서

(e) 제48조에 언급된 EU 적합성 선언

제51조

등록

제6(2)에 언급된 고위험 AI 시스템을 출시하거나 서비스 개시하기 전에, 제공자 또는 해당되는 경우 공인 대리인은 동 시스템을 제60조에 언급된 EU 데이터베이스에 등록한다.

TITLE IV

TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS

Article 52
Transparency obligations for certain AI systems

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences.

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.

   However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties.

4. Paragraphs 1, 2 and 3 shall not affect the requirements and obligations set out in Title III of this Regulation.

TITLE V

MEASURES IN SUPPORT OF INNOVATION

Article 53
AI regulatory sandboxes

1. AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan. This shall take place under the direct supervision and guidance by the competent authorities with a view to ensuring compliance with the requirements of this Regulation and, where relevant, other Union and Member States legislation supervised within the sandbox.

2. Member States shall ensure that to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data,

제4편

특정 AI 시스템에 대한 투명성 의무

제52조

특정 AI 시스템에 대한 투명성 의무

1. 제공자는 자연인과 상호 작용하는 AI 시스템이 해당 자연인이 AI 시스템과 상호 작용하고 있다는 것을 고지하는 방식으로 설계·개발되도록 보장한다. 단, 사용 상황과 맥락에서 이것이 명백한 경우는 예외로 한다. 이 의무는 범죄 행위의 탐지, 방지, 수사, 기소를 위해 법률이 허가한 AI 시스템에는 적용되지 않는다. 단, 일반인이 이러한 시스템을 범죄 행위의 신고에 이용할 수 있는 경우는 예외로 한다.

2. 감정 인식 시스템 또는 생체 인식 분류 시스템의 사용자는 그에 노출되는 자연인에게 시스템의 작동에 대해 고지해야 한다. 이 의무는 범죄 행위의 탐지, 방지, 수사를 위해 법률이 허용하는 생체 인식 분류에 사용되는 AI 시스템에는 적용되지 않는다.

3. 기존의 사람, 물체, 장소, 기타 실체 또는 사건과 현저히 유사하고 마치 진본처럼 보이는 이미지, 오디오 또는 비디오 콘텐츠를 생성하거나 조작하는('딥 페이크') AI 시스템의 사용자는 해당 콘텐츠가 인공적으로 생성 또는 조작되었음을 공개해야 한다.

   단, 범죄 행위의 탐지, 방지, 수사를 위해 법률이 사용을 허가하거나 EU 기본권 헌장에 보장된 표현의 자유 또는 학문과 예술의 자유에 대한 권리를 행사하기 위해 필요하고 제3자의 권리와 자유에 대한 적절한 보호 조치가 적용되는 경우에는 제1항이 적용되지 않는다.

4. 제1, 2, 3항은 본 규정의 제3편에 명시된 요구사항 및 의무에 영향을 미치지 않는다.

제5편

혁신을 지원하는 조치

제53조

AI 규제 샌드박스

1. 하나 이상의 회원국 관할 기관 또는 유럽 데이터 보호 감독관에 의해 설립된 AI 규제 샌드박스는 특정한 계획에 따라 혁신적인 AI 시스템이 출시되거나 서비스 개시되기 전에 제한된 시간 동안 개발, 테스트, 검증할 수 있는 통제 환경을 제공한다. 이는 본 규정과 해당되는 경우 샌드박스 내에서 감독을 받는 기타 유럽 연합 및 회원국 법규의 요구사항 준수를 보장하기 위해 관할 기관의 직접 감독 및 지도 하에 이루어진다.

2. 회원국은 혁신적인 AI 시스템이 개인 데이터의 처리를 수반하거나 데이터의 접근을 제공 또는 지원하는 다른 국가 기관 또는 관할 기관의 감독을 받는 경우 국가 데이터 보호

the national data protection authorities and those other national authorities are associated to the operation of the AI regulatory sandbox.

3. The AI regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Any significant risks to health and safety and fundamental rights identified during the development and testing of such systems shall result in immediate mitigation and, failing that, in the suspension of the development and testing process until such mitigation takes place.

4. Participants in the AI regulatory sandbox shall remain liable under applicable Union and Member States liability legislation for any harm inflicted on third parties as a result from the experimentation taking place in the sandbox.

5. Member States' competent authorities that have established AI regulatory sandboxes shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board. They shall submit annual reports to the Board and the Commission on the results from the implementation of those scheme, including good practices, lessons learnt and recommendations on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox.

6. The modalities and the conditions of the operation of the AI regulatory sandboxes, including the eligibility criteria and the procedure for the application, selection, participation and exiting from the sandbox, and the rights and obligations of the participants shall be set out in implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74(2).

Article 54

Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

1. In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions:

   (a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

      (i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

      (ii) public safety and public health, including disease prevention, control and treatment;

      (iii) a high level of protection and improvement of the quality of the environment;

   (b) the data processed are necessary for complying with one or more of the requirements referred to in Title III, Chapter 2 where those requirements cannot be effectively fulfilled by processing anonymised, synthetic or other non-personal data;

기관과 상기한 다른 국가 기관이 AI 규제 샌드박스의 운영에 참여하도록 보장한다.

3. AI 규제 샌드박스는 관할 기관의 감독 및 시정 권한에 영향을 주어서는 안 된다. 시스템의 개발 및 테스트 과정에서 건강과 안전 및 기본권에 대한 중대한 위험이 확인되는 경우 이를 즉시 완화해야 하며 그에 실패할 경우 완화가 이루어질 때까지 개발 및 테스트 프로세스가 일시 중지된다.

4. AI 규제 샌드박스의 참가자는 샌드박스에서 이루어지는 실험의 결과로 제3자에게 가해지는 피해에 대해 해당 유럽 연합 및 회원국 책임 법규에 따른 책임을 진다.

5. AI 규제 샌드박스를 설립한 회원국의 관할 기관은 유럽 인공지능 위원회의 프레임워크 내에서 활동을 조율하고 협력한다. 이들은 동 제도의 시행에 따른 결과를 연례 보고서를 위원회와 유럽연합 집행위원회에 제출해야 한다. 여기에는 우수 사례, 획득한 교훈, 그리고 그 설립과 해당될 경우 본 규정 및 샌드박스 내에서 감독을 받는 기타 유럽 연합 법규의 적용에 대한 권고사항이 포함된다.

6. 샌드박스 신청, 선정, 참여, 탈퇴를 위한 자격 기준과 절차를 포함한 AI 규제 샌드박스의 운영 방식과 조건 및 참가자의 권리와 의무는 실행 규정에 명시된다. 이러한 실행 규정은 제74(2)조에 언급된 심사 절차에 따라 채택된다.

제54조

AI 규제 샌드박스에서 공익을 위해 특정 AI 시스템을 개발하기 위한 개인 데이터의 추가 처리

1. AI 규제 샌드박스에서는 다음과 같은 조건 하에, 다른 목적으로 적법하게 수집한 개인 데이터를 특정한 혁신적 AI 시스템을 개발·테스트하기 위한 목적으로 처리한다.

   (a) 다음 영역 중 하나 이상에서 상당한 공익을 보호하기 위해 혁신적 AI 시스템을 개발한다.

      (i) 관할 기관의 통제와 책임 하에 공공 안전에 대한 위협으로부터의 보호와 방지를 포함한 범죄 행위의 방지, 수사, 탐지 기소, 또는 형사 처벌의 집행. 처리는 회원국 또는 유럽 연합 법규에 근거해야 한다.

      (ii) 질병 예방, 통제, 치료를 포함한 공공 보건 및 공공 안전

      (iii) 높은 수준의 환경의 질 보호 및 개선

   (b) 익명화 정보, 합성 정보 또는 기타 비 개인 데이터를 처리하는 것만으로 제3편 제2장에 명시된 요구사항을 효과적으로 충족할 수 없는 경우 동 요구사항을 준수하는 데 해당 데이터가 필요하다.

(c) there are effective monitoring mechanisms to identify if any high risks to the fundamental rights of the data subjects may arise during the sandbox experimentation as well as response mechanism to promptly mitigate those risks and, where necessary, stop the processing;

(d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the participants and only authorised persons have access to that data;

(e) any personal data processed are not be transmitted, transferred or otherwise accessed by other parties;

(f) any processing of personal data in the context of the sandbox do not lead to measures or decisions affecting the data subjects;

(g) any personal data processed in the context of the sandbox are deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox and 1 year after its termination, solely for the purpose of and only as long as necessary for fulfilling accountability and documentation obligations under this Article or other application Union or Member States legislation;

(i) complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation in Annex IV;

(j) a short summary of the AI project developed in the sandbox, its objectives and expected results published on the website of the competent authorities.

2. Paragraph 1 is without prejudice to Union or Member States legislation excluding processing for other purposes than those explicitly mentioned in that legislation.

Article 55
Measures for small-scale providers and users

1. Member States shall undertake the following actions:

(a)) provide small-scale providers and start-ups with priority access to the AI regulatory sandboxes to the extent that they fulfil the eligibility conditions;

(b) organise specific awareness raising activities about the application of this Regulation tailored to the needs of the small-scale providers and users;

(c) where appropriate, establish a dedicated channel for communication with small-scale providers and user and other innovators to provide guidance and respond to queries about the implementation of this Regulation.

2. The specific interests and needs of the small-scale providers shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size and market size.

(c) 샌드박스 실험 과정에서 정보 주체의 기본권에 대해 높은 위험이 발생할 수 있는지 파악하는 효과적 모니터링 메커니즘과 그러한 위험을 즉시 완화하고 필요할 경우 처리를 중단하는 대응 메커니즘이 갖춰져 있다.

(d) 샌드박스의 맥락에서 처리되는 개인 데이터가 기능적으로 분리·보호되는 데이터 처리 환경에 있고, 참가자의 통제 하에 오로지 허가된 사람만 해당 데이터에 접근할 수 있다.

(e) 처리되는 개인 데이터를 다른 당사자가 전송, 이전 또는 접근하지 않는다.

(f) 샌드박스의 맥락에서 개인 데이터의 처리가 정보 주체에게 영향을 미치는 조치 또는 결정으로 이어지지 않는다.

(g) 샌드박스에 대한 참여가 종료되거나 개인 데이터의 보존 기간이 만료되면 샌드박스의 맥락에서 처리되는 모든 개인 데이터가 삭제된다

(h) 샌드박스의 맥락에서 개인 데이터의 처리에 대한 기록은 오로지 본 조항 또는 관련 유럽 연합 또는 회원국 법규에 따른 책무성 및 기록 의무의 목적으로, 그리고 그에 필요한 경우에 한하여, 샌드박스에 대한 참여 기간 및 종료 후 1년간 보관된다.

(i) 처리에 대한 완전하고 상세한 설명과 AI 시스템의 학습, 테스트, 검증을 뒷받침하는 근거를 테스트 결과와 함께 부속서 IV에 명시된 기술 문서의 일부로 보관한다.

(j) 샌드박스에서 개발된 AI 프로젝트와 그 목표 및 기대하는 결과의 간단한 요약을 관할 기관의 웹사이트에 게시한다.

2. 제1항은 명시된 것 이외의 목적으로 처리하는 것을 금지하는 유럽 연합 또는 회원국 법규를 침해하지 않는다.

제55조

소규모 제공자 및 사용자를 위한 조치

1. 회원국은 다음 조치를 수행한다.

(a) 소규모 제공자와 스타트업이 자격 조건을 충족하는 경우 AI 규제 샌드박스에 우선적으로 접근할 수 있도록 한다.

(b) 소규모 제공자 및 사용자의 요구에 맞춤화된, 본 규정의 적용에 대한 인식 제고 활동을 조직한다.

(c) 적절한 경우 소규모 제공자 및 사용자와 기타 혁신자들과의 의사소통을 위한 전담 채널을 구축하여 본 규정의 시행에 대한 지침을 제공하고 질문에 응답한다.

2. 제43조에 따른 적합성 평가의 수수료를 책정할 때 소규모 제공자의 특정한 이해와 요구를 고려하여 그들의 규모와 시장 규모에 비례하도록 수수료를 경감한다.

TITLE VI

GOVERNANCE

CHAPTER 1

EUROPEAN ARTIFICIAL INTELLIGENCE BOARD

Article 56
Establishment of the European Artificial Intelligence Board

1. A 'European Artificial Intelligence Board' (the 'Board') is established.

2. The Board shall provide advice and assistance to the Commission in order to:

   (a) contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by this Regulation;

   (b) coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation;

   (c) assist the national supervisory authorities and the Commission in ensuring the consistent application of this Regulation.

Article 57
Structure of the Board

1. The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.

2. The Board shall adopt its rules of procedure by a simple majority of its members, following the consent of the Commission. The rules of procedure shall also contain the operational aspects related to the execution of the Board's tasks as listed in Article 58. The Board may establish sub-groups as appropriate for the purpose of examining specific questions.

3. The Board shall be chaired by the Commission. The Commission shall convene the meetings and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and with its rules of procedure. The Commission shall provide administrative and analytical support for the activities of the Board pursuant to this Regulation.

4. The Board may invite external experts and observers to attend its meetings and may hold exchanges with interested third parties to inform its activities to an appropriate extent. To that end the Commission may facilitate exchanges between the Board and other Union bodies, offices, agencies and advisory groups.

제6편

거버넌스

제1장

유럽 인공지능 위원회

제56조

유럽 인공지능 위원회의 설립

1. '유럽 인공지능 위원회(European Artificial Intelligence Board)'('위원회)를 설립한다.

2. 위원회는 다음을 위해 유럽연합 집행위원회에 조언과 조력을 제공한다.

   (a) 본 규정이 적용되는 문제와 관련한 국가 감독 기관과 유럽연합 집행위원회의 효과적 협력에 기여한다.

   (b) 본 규정이 적용되는 문제와 관련한 역내 시장 전반에 걸쳐 새롭게 부각되는 문제에 대한 유럽연합 집행위원회와 국가 감독 기관 및 기타 관할 기관의 지침과 분석을 조율하고 기여한다.

   (c) 국가 감독 기관과 유럽연합 집행위원회가 본 규정을 일관성 있게 적용할 수 있도록 조력한다.

제57조

위원회의 구조

1. 위원회는 고위급 임원들로 대표되는 국가 감독 기관과 유럽 데이터 보호 감독관으로 구성된다. 회의에서 토론되는 문제와 관련이 있는 다른 국가 기관을 회의에 초청할 수 있다.

2. 위원회는 회원 과반수의 찬성과 유럽연합 집행위원회의 동의를 얻어 절차 규칙을 채택한다. 절차 규칙에는 또한 제58조에 열거된 위원회의 과업 수행과 관련된 운영 측면이 포함된다. 위원회는 필요할 경우 특정 문제를 조사하는 목적을 위해 소분과를 둘 수 있다.

3. 위원회의 의장은 유럽연합 집행위원회가 맡는다. 유럽연합 집행위원회는 본 규정에 따른 위원회의 과업과 절차 규칙에 따라 회의를 개최하고 의제를 준비한다. 유럽연합 집행위원회는 본 규정에 따른 위원회의 활동에 대해 행정 및 분석 지원을 제공한다.

4. 위원회는 외부 전문가와 옵서버를 회의에 초청할 수 있으며, 적절한 수준으로 그들의 활동을 지원하기 위해 이해관계가 있는 제3자와 교류를 가질 수 있다. 이를 위해 유럽연합 집행위원회는 (인공지능) 위원회와 다른 유럽 연합 기관, 국/청, 기구 및 자문 그룹 간의 교류를 촉진할 수 있다.

Article 58
Tasks of the Board

When providing advice and assistance to the Commission in the context of Article 56(2), the Board shall in particular:

(a) collect and share expertise and best practices among Member States;

(b) contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53;

(c) issue opinions, recommendations or written contributions on matters related to the implementation of this Regulation, in particular

  (i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,

  (ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,

  (iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.

CHAPTER 2

NATIONAL COMPETENT AUTHORITIES

Article 59
Designation of national competent authorities

1. National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.

2. Each Member State shall designate a national supervisory authority among the national competent authorities. The national supervisory authority shall act as notifying authority and market surveillance authority unless a Member State has organisational and administrative reasons to designate more than one authority.

3. Member States shall inform the Commission of their designation or designations and, where applicable, the reasons for designating more than one authority.

4. Member States shall ensure that national competent authorities are provided with adequate financial and human resources to fulfil their tasks under this Regulation. In particular, national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of artificial intelligence technologies, data and data computing, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.

5. Member States shall report to the Commission on an annual basis on the status of the financial and human resources of the national competent authorities with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

6. The Commission shall facilitate the exchange of experience between national competent authorities.

제58조

위원회의 과업

위원회는 제56(2)조의 맥락에서 유럽연합 집행위원회에 조언과 조력을 제공할 때 특히 다음을 수행한다.

(a) 회원국들 사이에서 전문 지식과 모범 사례를 수집하고 공유한다.

(b) 제53조에 언급된 규제 샌드박스의 기능을 포함하여, 회원국들의 일관성 있는 행정 실무에 기여한다.

(c) 본 규정의 시행, 특히 다음과 관련된 문제에 대해 의견, 권고 또는 기고문을 제공한다

(i) 제3편 제2장에 명시된 요구사항과 관련된 기술 규격 또는 기존 표준

(ii) 제40조 및 41조에 언급된 조화 표준 또는 공통 규격의 사용

(iii) 제71조에 언급된 과징금의 책정과 관련된 가이드라인을 포함한 지침서의 작성.

제2장

국가 관할 기관

제59조

국가 관할 기관의 지명

1. 국가 관할 기관은 각 회원국이 본 규정의 적용과 시행을 보장하기 위한 목적으로 설립하거나 지명한다. 국가 관할 기관은 그 활동과 과업의 객관성과 공평성을 보호하도록 조직되어야 한다.

2. 각 회원국은 국가 관할 기관들 중에서 국가 감독 기관을 지명한다. 국가 감독 기관은 통보 기관 및 시장 감시 기관의 역할을 수행한다. 회원국이 둘 이상의 기관을 지명할 조직적·행정적 이유가 있는 경우는 예외로 한다.

3. 회원국은 지명 사실과 해당될 경우 둘 이상의 기관을 지명하는 이유를 유럽연합 집행위원회에 통지한다.

4. 회원국은 국가 관할 기관이 본 규정에 따른 과업을 이행하기에 충분한 재정 및 인적 자원을 제공받도록 보장한다. 특히, 국가 관할 기관은 인공 지능 기술, 데이터 및 데이터 컴퓨팅, 기본권, 건강 및 안전 위험, 기존 표준 및 법적 요건 등에 대한 심층적 이해를 포함한 전문 지식과 역량을 갖춘 상시 가용한 충분한 수의 인력을 보유해야 한다.

5. 회원국은 타당성 평가를 통해 국가 관할 기관의 재정 및 인적 자원 상태를 파악하고 이를 매년 유럽연합 집행위원회에 보고해야 한다. 유럽연합 집행위원회는 이러한 정보를 위원회에 전송하여 토론하고 가능한 경우 권고를 제공할 수 있도록 해야 한다.

6. 유럽연합 집행위원회는 국가 관할 기관들 간에 경험의 교환을 촉진한다.

7. National competent authorities may provide guidance and advice on the implementation of this Regulation, including to small-scale providers. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union legislation, the competent national authorities under that Union legislation shall be consulted, as appropriate. Member States may also establish one central contact point for communication with operators.

8. When Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as the competent authority for their supervision.

TITLE VII

EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS

Article 60
EU database for stand-alone high-risk AI systems

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Article 51.

2. The data listed in Annex VIII shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.

3. Information contained in the EU database shall be accessible to the public.

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

5. The Commission shall be the controller of the EU database. It shall also ensure to providers adequate technical and administrative support.

TITLE VIII

POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE

CHAPTER 1

POST-MARKET MONITORING

Article 61
Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

7. 국가 관할 기관은 본 규정의 시행에 대한 지침과 조언을 소규모 제공자를 포함한 대상에게 제공할 수 있다. 국가 관할 기관이 다른 유럽 연합 법규가 적용되는 영역에서 AI 시스템과 관련된 지침과 조언을 제공하고자 하는 경우, 동 유럽 연합 법규에 따른 관할 국가 기관과 협의해야 한다. 아울러 회원국은 운영자들과 의사소통하기 위한 하나의 중앙 연락 지점을 설정할 수 있다.

8. 유럽 연합 기관, 기구, 단체가 본 규정의 범위 내에 속하는 경우 유럽 연합 데이터 보호 감독 기구는 그들의 감독을 위한 관할 기관의 역할을 수행해야 한다.

제7편

독립형 고위험 AI 시스템을 위한 EU 데이터베이스

제60조

독립형 고위험 AI 시스템을 위한 EU 데이터베이스

1. 유럽연합 집행위원회는 회원국들과 협력하여 제51조에 따라 등록되고 제6(2)조에 언급된 고위험 AI 시스템에 관한, 제2항에 언급된 정보를 포함하는 EU 데이터베이스를 구축하고 유지한다.

2. 제공자는 부속서 VIII에 열거된 데이터를 EU 데이터베이스에 입력해야 한다. 유럽연합 집행위원회는 이들에게 기술적·행정적 지원을 제공한다.

3. EU 데이터베이스에 포함된 정보는 일반인이 접근할 수 있어야 한다.

4. EU 데이터베이스에는 오로지 본 규정에 따라 정보를 수집·처리하는 데 필요한 경우에만 개인 데이터가 포함되어야 한다. 이 정보에는 시스템을 등록하는 일을 책임지고 제공자를 대표할 법적 권한을 가지는 자연인의 이름과 연락처 세부사항이 포함된다.

5. 유럽연합 집행위원회는 EU 데이터베이스의 관리자(controller)가 된다. 유럽연합 집행위원회는 또한 제공자에게 충분한 기술적·행정적 지원을 보장해야 한다.

제8편

출시 후 모니터링, 정보 공유, 시장 감시

제1장

출시 후 모니터링

제61조

제공자에 의한 출시 후 모니터링 및 고위험 AI 시스템에 대한 출시 후 모니터링 계획

1. 제공자는 인공 지능 기술의 성격과 고위험 AI 시스템의 위험에 비례하는 방식으로 출시 후 모니터링 시스템을 구축하고 문서화해야 한다.

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.

CHAPTER 2

SHARING OF INFORMATION ON INCIDENTS AND MALFUNCTIONING

Article 62
Reporting of serious incidents and of malfunctioning

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights to the market surveillance authorities of the Member States where that incident or breach occurred.

Such notification shall be made immediately after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning.

2. Upon receiving a notification related to a breach of obligations under Union law intended to protect fundamental rights, the market surveillance authority shall inform the national public authorities or bodies referred to in Article 64(3). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1. That guidance shall be issued 12 months after the entry into force of this Regulation, at the latest.

3. For high-risk AI systems referred to in point 5(b) of Annex III which are placed on the market or put into service by providers that are credit institutions regulated by Directive 2013/36/EU and for high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulation (EU) 2017/745 and Regulation (EU) 2017/746, the notification of serious incidents or malfunctioning shall be limited to those that that constitute a breach of obligations under Union law intended to protect fundamental rights.

2. 출시 후 모니터링 시스템은 사용자가 제공하거나 다른 소스를 통해 수집한 고위험 AI 시스템의 수명주기 전반에 걸친 수행에 관한 데이터를 적극적·체계적으로 수집, 기록, 분석하고, 제공자로 하여금 AI 시스템이 제3편 제2장에 명시된 요구사항을 지속적으로 준수하는지 평가할 수 있도록 해야 한다.

3. 출시 후 모니터링 시스템은 출시 후 모니터링 계획에 기초해야 한다. 출시 후 모니터링 계획은 부속서 IV에 언급된 기술 문서의 일부여야 한다. 유럽연합 집행위원회는 출시 후 모니터링 계획을 위한 템플릿과 계획에 포함될 요소들의 목록에 관한 세부 조항을 명시하는 실행 규정을 채택해야 한다.

4. 부속서 II에 언급된 법규가 적용되는 고위험 AI 시스템에 대해, 동 법규에 따라 출시 후 모니터링 시스템 및 계획이 이미 수립된 경우, 제1, 2, 3항에 기술된 요소들이 상황에 따라 해당 시스템 및 계획에 통합되어야 한다.

   제1항은 Directive 2013/36/EU에 의해 규제되는 신용 기관이 출시하거나 서비스 개시하는 부속서 III의 5(b)항에 언급된 고위험 AI 시스템에도 적용된다.

제2장

사건 및 오작동에 관한 정보의 공유

제62조

중대한 사건 및 오작동의 보고

1. 유럽 연합 시장에 출시된 고위험 AI 시스템의 제공자는 유럽 연합법에 따른 기본권 보호 의무의 위반을 구성하는 동 시스템의 중대한 사건 또는 오작동을 동 사건 또는 위반이 발생한 회원국의 시장 감시 기관에 보고해야 한다.

   상기한 통지는 제공자가 AI 시스템과 사건 또는 오작동 간의 인과관계 또는 그 합리적 가능성을 파악하는 즉시, 그리고 어떠한 경우에도 제공자가 중대한 사건 또는 오작동을 인지한 후 15일 이내에 이루어져야 한다.

2. 시장 감독 기관은 유럽 연합법에 따른 기본권 보호 의무의 위반과 관련된 통지를 수신하는 즉시 이를 제64(3)조에 언급된 국가 공공 기관 또는 기구에 통지한다. 유럽연합 집행위원회는 제1항에 명시된 의무의 준수를 촉진하기 위한 지침을 개발한다. 이 지침은 늦어도 본 규정이 발효된 지 12개월 후에 공표되어야 한다.

3. Directive 2013/36/EU에 의해 규제되는 신용 기관인 제공자가 출시하거나 서비스 개시한 부속서 III의 5(b)항에 언급된 고위험 AI 시스템 또는 Regulation (EU) 2017/745 및 Regulation (EU) 2017/746이 적용되는 장치의 안전 구성요소이거나 그 자체가 장치인 고위험 AI 시스템의 경우, 중대한 사건 또는 오작동의 통지는 유럽 연합법에 따른 기본권 보호 의무의 위반을 구성하는 경우로만 제한된다.

CHAPTER 3

ENFORCEMENT

Article 63
Market surveillance and control of AI systems in the Union market

1. Regulation (EU) 2019/1020 shall apply to AI systems covered by this Regulation. However, for the purpose of the effective enforcement of this Regulation:

   (a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified in Title III, Chapter 3 of this Regulation;

   (b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.

2. The national supervisory authority shall report to the Commission on a regular basis the outcomes of relevant market surveillance activities. The national supervisory authority shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules.

3. For high-risk AI systems, related to products to which legal acts listed in Annex II, section A apply, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts.

4. For AI systems placed on the market, put into service or used by financial institutions regulated by Union legislation on financial services, the market surveillance authority for the purposes of this Regulation shall be the relevant authority responsible for the financial supervision of those institutions under that legislation.

5. For AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6 and 7 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems.

6. Where Union institutions, agencies and bodies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority.

7. Member States shall facilitate the coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex II or other Union legislation that might be relevant for the high-risk AI systems referred to in Annex III.

제3장

집행

제63조

유럽 연합의 시장 감시 및 AI 시스템의 관리

1. 본 규정이 적용되는 AI 시스템에는 Regulation (EU) 2019/1020이 적용된다. 단, 본 규정의 효과적 집행 목적을 위해,

   (a) Regulation (EU) 2019/1020에 따른 경제 운영자에 대한 언급은 본 규정의 제3편 제3장에 명시된 모든 운영자를 포함하는 것으로 이해되어야 한다.

   (b) Regulation (EU) 2019/1020에 따른 제품에 대한 언급은 본 규정의 범위 내에 속하는 모든 AI 시스템을 포함하는 것으로 이해되어야 한다.

2. 국가 감독 기관은 관련 시장 감시 활동의 결과를 유럽연합 집행위원회에 정기적으로 보고해야 한다. 국가 감독 기관은 시장 감시 활동 과정에서 파악된, 경쟁 규칙에 관한 유럽 연합법의 적용에 중요할 수 있는 모든 정보를 유럽연합 집행위원회와 관련 국가 경쟁 당국(national competition authorities)에 지체 없이 보고해야 한다.

3. 부속서 II의 A절에 열거된 법규가 적용되는 제품과 관련된 고위험 AI 시스템의 경우, 본 규정의 목적을 위한 시장 감시 기관이 동 법규에 따라 지명된 시장 감시 활동을 책임지는 기관이 되어야 한다.

4. 금융 서비스에 관한 유럽 연합법에 의해 규제되는 금융 기관이 출시, 서비스 개시 또는 사용하는 AI 시스템의 경우, 본 규정의 목적을 위한 시장 감시 기관이 동 법률에 따라 동 기관의 금융 감독을 책임지는 기관이 되어야 한다.

5. 부속서 III의 1(a)항(시스템이 법 집행 목적으로 사용되는 경우), 제6항 및 7항에 열거된 AI 시스템의 경우, 회원국은 Directive (EU) 2016/680 또는 Regulation 2016/679에 따른 관할 데이터 보호 감독 기관 또는 법 집행 활동을 감독하는 국가 관할 기관 또는 동 시스템을 서비스 개시하거나 사용하는 이주·망명 기관을 본 규정의 목적을 위한 시장 감시 기관으로 지명해야 한다.

6. 유럽 연합 기관, 기구, 단체가 본 규정의 범위 내에 속하는 경우 유럽 데이터 보호 감독관이 이들의 시장 감시 기관 역할을 수행한다.

7. 회원국은 본 규정에 따라 지명된 시장 감시 기관과 부속서 II에 열거된 유럽 연합 조화 법령 또는 부속서 III에 언급된 고위험 AI 시스템과 관련될 수 있는 다른 유럽 연합법의 적용을 감독하는 다른 관련 국가 기관 또는 기구들 사이의 조율을 촉진한다.

Article 64
Access to data and documentation

1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.

2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

3. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of the competences under their mandate within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.

4. By 3 months after the entering into force of this Regulation, each Member State shall identify the public authorities or bodies referred to in paragraph 3 and make a list publicly available on the website of the national supervisory authority. Member States shall notify the list to the Commission and all other Member States and keep the list up to date.

5. Where the documentation referred to in paragraph 3 is insufficient to ascertain whether a breach of obligations under Union law intended to protect fundamental rights has occurred, the public authority or body referred to paragraph 3 may make a reasoned request to the market surveillance authority to organise testing of the high- risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within reasonable time following the request.

6. Any information and documentation obtained by the national public authorities or bodies referred to in paragraph 3 pursuant to the provisions of this Article shall be treated in compliance with the confidentiality obligations set out in Article 70.

Article 65
Procedure for dealing with AI systems presenting a risk at national level

1. AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned.

2. Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents a risk as referred to in paragraph 1, they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. When risks to the protection of fundamental rights are present, the market surveillance authority shall also inform the relevant national public authorities or bodies referred to in Article 64(3). The relevant operators shall cooperate as necessary with the market

제64조

데이터 및 문서에 대한 접근

1. 그 활동의 맥락에서 데이터 및 문서에 대한 접근. 시장 감시 기관은 애플리케이션 프로그래밍 인터페이스('API') 또는 원격 접근을 지원하는 기타 적절한 기술적 수단 및 도구를 포함하여 제공자가 사용하는 학습, 검증 및 테스트 데이터세트에 전면적으로 접근할 수 있어야 한다.

2. 고위험 AI 시스템이 제3편 제2장에 명시된 요구사항을 준수하는지 평가하는 데 필요하고 합리적으로 요청하는 경우, 시장 감시 기관은 AI 시스템의 소스 코드에 대한 접근이 허용되어야 한다.

3. 부속서 III에 언급된 고위험 AI 시스템의 사용과 관련하여 유럽 연합법에 따른 기본권 보호 의무의 이행을 감독하거나 집행하는 국가 공공 기관 또는 기구는, 해당 문서의 접근이 관할권의 제한 내에서 그들의 권한에 따른 직무를 이행하는 데 필요한 경우 본 규정에 따라 작성되거나 유지되는 문서를 요청하고 접근할 권한을 가진다. 관련 공공 기관 또는 기구는 그러한 요청을 관련 회원국의 시장 감시 기관에 통지해야 한다

4. 본 규정이 발효된 지 3개월 후까지 각 회원국은 제3항에 언급된 공공 기관 또는 기구를 파악하고 그 목록을 국가 감독 기관의 웹사이트에 공개해야 한다. 회원국은 목록을 유럽연합 집행위원회와 다른 모든 회원국에 통지하고 동 목록을 최신으로 유지해야 한다.

5. 3항에 언급된 문서가 유럽 연합법에 따른 기본권 보호 의무의 위반이 발생했는지 여부를 확인하는 데 불충분한 경우 제3항에 언급된 공공 기관 또는 기구는 시장 감시 기관에 대해 기술적 수단을 통해 고위험 AI 시스템의 테스트를 조직할 것을 합리적으로 요청할 수 있다. 시장 감시 기관은 요청 후 합리적인 시간 내에 요청하는 공공 기관 또는 기구의 긴밀한 관여 하에 테스트를 조직해야 한다.

6. 본 조에 따라 제3항에 언급된 국가 공공 기관 또는 기구가 획득한 모든 정보 및 문서는 제70조에 명시된 기밀 유지 의무를 준수하는 것으로 취급된다.

제65조

국가 수준에서 위험을 야기하는 AI 시스템을 취급하기 위한 절차

1. 위험을 야기하는 AI 시스템은 사람의 건강, 안전 또는 기본권에 대한 위험과 관련하여 Regulation (EU) 2019/1020의 제3항 19호에 정의된 위험을 야기하는 제품으로 이해된다.

2. 회원국의 시장 감시 기관이 특정 AI 시스템이 제1항에 언급된 위험을 야기한다고 간주할 충분한 이유를 가지는 경우에는 해당 AI 시스템이 본 규정에 명시된 모든 요구사항과 의무를 준수하는지 여부를 평가해야 한다. 기본권에 대한 위험이 존재하는 경우 시장 감시 기관은 제64(3)조에 언급된 관련 국가 공공 기관 또는 기구에 이를 통지해야 한다. 관련 운영자는 필요할 경우 시장 감시

surveillance authorities and the other national public authorities or bodies referred to in Article 64(3).

Where, in the course of that evaluation, the market surveillance authority finds that the AI system does not comply with the requirements and obligations laid down in this Regulation, it shall without delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the measures referred to in the second subparagraph.

3. Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the operator to take.

4. The operator shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the market throughout the Union.

5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market, to withdraw the product from that market or to recall it. That authority shall inform the Commission and the other Member States, without delay, of those measures.

6. The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant AI system, the origin of the AI system, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following:

   (a) a failure of the AI system to meet requirements set out in Title III, Chapter 2;

   (b) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity.

7. The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the AI system concerned, and, in the event of disagreement with the notified national measure, of their objections.

8. Where, within three months of receipt of the information referred to in paragraph 5, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed justified. This is without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020.

기관 및 제64(3)조에 언급된 기타 국가 공공 기관 또는 기구와 협력해야 한다.

상기한 평가 과정에서 AI 시스템이 본 규정에 명시된 요구사항과 의무를 준수하지 않는다고 판단되는 경우 시장 감시 기관은 지체 없이 관련 운영자에 대해 동 AI 시스템의 준수에 필요한 모든 시정 조치를 취하거나, 동 기관이 규정하는 위험의 성격에 상응하는 합리적 기간 내에 동 AI 시스템을 시장에서 회수하거나 리콜할 것을 요구해야 한다.

시장 감시 기관은 이를 관련 인증 기관에 통지한다. 제2항에 언급된 조치에는 Regulation (EU) 2019/1020 제18조가 적용된다.

3. 비준수가 국가 영토에 국한되지 않는다고 간주되는 경우, 시장 감시 기관은 평가 결과와 운영자에게 요구한 조치를 유럽연합 집행위원회와 다른 회원국에 통지해야 한다.

4. 운영자는 자신이 유럽 연합 전역에 걸쳐 출시한 모든 AI 시스템과 관련하여 필요한 모든 시정 조치가 취해지도록 보장한다.

5. AI 시스템의 운영자가 제2항에 언급된 기간 내에 충분한 시정 조치를 취하지 않는 경우 시장 감시 기관은 동 AI 시스템이 자국의 시장에 출시되는 것을 금지 또는 제한하는 데 필요한 모든 잠정적 조치를 취하거나, 제품을 시장에서 회수 또는 리콜해야 한다. 동 기관은 그러한 조치에 대해 유럽연합 집행위원회와 다른 회원국에 지체 없이 통지해야 한다.

6. 5항에 언급된 정보에는 특히 비준수 AI 시스템의 식별에 필요한 데이터, 동 AI 시스템의 원산지, 관련된 비준수와 위험의 성격, 취해진 국가적 조치의 성격과 기간, 관련 운영자가 제시한 논거 등 가용한 모든 세부사항이 포함되어야 한다. 특히 시장 감시 기관은 비준수가 다음 중 하나 이상으로 인한 것인지 여부를 밝혀야 한다.

   (a) AI 시스템이 제3편 제2장에 명시된 요구사항을 충족하지 않음

   (b) 준수 추정을 허용하는 제40조 및 41조에 언급된 조화 표준 또는 공통 규격의 결함.

7. 절차를 개시하는 회원국의 시장 감시 기관이 아닌 회원국의 시장 감시 기관은 채택한 조치와 관련 AI 시스템의 비준수에 관한 (그들이 처분할 수 있는) 추가 정보, 그리고 국가적 조치에 동의하지 않는 경우 반대 의사를 지체 없이 유럽연합 집행위원회 및 다른 회원국에 통지해야 한다.

8. 5항에 언급된 통지를 받은 후 3개월 이내에 회원국 또는 유럽연합 집행위원회가 해당 회원국이 취한 잠정 조치에 대해 아무런 이의를 제기하지 않는 경우, 동 조치는 정당화된 것으로 간주된다. 이는 Regulation (EU) 2019/1020 제18조에 따른 관련 운영자의 절차적 권리를 침해하지 않는다.

9. The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product concerned, such as withdrawal of the product from their market, without delay.

Article 66
Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 65(5), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without delay enter into consultation with the relevant Member State and operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within 9 months from the notification referred to in Article 65(5) and notify such decision to the Member State concerned.

2. If the national measure is considered justified, all Member States shall take the measures necessary to ensure that the non-compliant AI system is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is considered unjustified, the Member State concerned shall withdraw the measure.

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

Article 67
Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 65, the market surveillance authority of a Member State finds that although an AI system is in compliance with this Regulation, it presents a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

2. The provider or other relevant operators shall ensure that corrective action is taken in respect of all the AI systems concerned that they have made available on the market throughout the Union within the timeline prescribed by the market surveillance authority of the Member State referred to in paragraph 1.

3. The Member State shall immediately inform the Commission and the other Member States. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the AI system, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without delay enter into consultation with the Member States and the relevant operator and shall evaluate the national measures taken. On the basis

9. 모든 회원국의 시장 감시 기관은 해당 제품과 관련하여 예컨대 제품을 시장에서 회수하는 등의 적절한 제한 조치가 지체 없이 취해지도록 보장해야 한다.

제66조
유럽 연합 보호 절차

1. 제65(5)조에 언급된 통지를 받은 후 3개월 이내에, 특정 회원국이 취한 조치에 대해 다른 회원국이 이의를 제기하거나 동 조치가 유럽 연합법에 위배된다고 판단되는 경우 유럽연합 집행위원회는 지체 없이 관련 회원국 및 운영자와 협의를 벌이고 국가적 조치를 평가해야 한다. 유럽연합 집행위원회는 그러한 평가 결과를 토대로 제65(5)조에 언급된 통지로부터 9개월 이내에 국가적 조치가 정당화되는지 여부를 결정하고 이를 관련 회원국에 통지해야 한다.

2. 국가적 조치가 정당하다고 간주되는 경우 모든 회원국은 비준수 AI 시스템을 각국의 시장에서 회수하는 데 필요한 조치를 취하고 이를 유럽연합 집행위원회에 통지한다. 국가적 조치가 정당하지 않다고 간주되는 경우 관련 회원국은 조치를 취소한다.

3. 국가적 조치가 정당하다고 간주되고 AI 시스템의 비준수가 본 규정 제40조 및 41조에 언급된 조화 표준 또는 공통 규격의 결함에 기인한다고 간주되는 경우 유럽연합 집행위원회는 Regulation (EU) No 1025/2012 제11조에 규정된 절차를 적용한다.

제67조
위험을 야기하는 준수 AI 시스템

1. 회원국의 시장 감시 기관이 제65조에 따른 평가를 수행한 결과 AI 시스템이 본 규정을 준수하지만 사람의 건강 또는 안전, 유럽 연합 또는 국가 법률에 따른 기본권 보호 의무 준수, 또는 공익 보호의 기타 측면에 위험을 야기한다고 판단되는 경우 동 기관은 관련 운영자에 대해 관련 AI 시스템이 출시되거나 서비스 개시된 경우 더 이상 그러한 위험을 야기하지 않도록 보장하는 데 필요한 모든 조치를 취하거나, 동 기관이 규정하는 위험의 성격에 상응하는 합리적 기간 내에 동 AI 시스템을 시장에서 회수 또는 리콜할 것을 요구해야 한다.

2. 제공자 또는 기타 관련 운영자는 유럽 연합 전역에서 그들이 출시한 모든 관련 AI 시스템에 대해 제1항에 언급된 회원국의 시장 감시 기관이 규정하는 기간 내에 시정 조치가 취해지도록 보장한다.

3. 관련 회원국은 즉시 유럽연합 집행위원회와 다른 회원국에 통지한다. 이 정보에는 특히 관련 AI 시스템의 식별에 필요한 데이터, AI 시스템의 원산지와 공급망, 수반되는 위험의 성격, 취해진 국가적 조치의 성격과 기간 등 가용한 모든 세부사항이 포함되어야 한다.

4. 유럽연합 집행위원회는 지체 없이 회원국 및 관련 운영자와 협의를 벌이고 취해진 국가적 조치를 평가한다. 유럽연합 집행위원회는 그러한 평가 결과를 토대로 조치가

of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to the Member States.

Article 68
Formal non-compliance

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non- compliance concerned:

   (a) the conformity marking has been affixed in violation of Article 49;

   (b) the conformity marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

   (d) the EU declaration of conformity has not been drawn up correctly;

   (e) the identification number of the notified body, which is involved in the conformity assessment procedure, where applicable, has not been affixed;

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the high-risk AI system being made available on the market or ensure that it is recalled or withdrawn from the market.

TITLE IX

CODES OF CONDUCT

Article 69
Codes of conduct

1. The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems other than high-risk AI systems of the requirements set out in Title III, Chapter 2 on the basis of technical specifications and solutions that are appropriate means of ensuring compliance with such requirements in light of the intended purpose of the systems.

2. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.

3. Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

정당화되는지 여부를 결정하고 필요한 경우 적절한 조치를 제안한다.

5. 유럽연합 집행위원회는 상기한 결정을 회원국에 통지한다.

제68조

공식적 비준수

1. 회원국의 시장 감시 기관이 다음 사실 중 하나를 발견하는 경우에는 관련 제공자에게 관련 비준수를 중단할 것을 요구해야 한다.

(a) 제49조를 위반하여 적합성 마크를 부착한 사실

(b) 적합성 마크가 부착되지 않은 사실

(c) EU 적합성 선언이 작성되지 않은 사실

(d) EU 적합성 선언이 올바르게 작성되지 않은 사실

(e) 해당될 경우 적합성 평가 절차에 관여한 인증 기관의 식별 번호가 부착되지 않는 사실

2. 1항에 언급된 비준수가 지속되는 경우 관련 회원국은 해당 고위험 AI 시스템이 출시되는 것을 제한하거나 금지하는 데 필요한 모든 조치를 취하거나 시장에서 회수 또는 리콜되도록 보장해야 한다.

제9편

행동 지침

제69조

행동 지침

1. 유럽연합 집행위원회와 회원국은 시스템의 원래 목적에 비추어 제3편 제2장에 명시된 요구사항의 준수를 보장하는 적절한 수단인 기술 규격 및 솔루션을 토대로 그러한 요구사항을 고위험 AI 시스템이 아닌 AI 시스템에 자발적으로 적용하도록 촉구하는 행동 지침을 작성할 것을 장려하고 촉진해야 한다.

2. 유럽연합 집행위원회와 유럽 인공지능 위원회는 명확한 목표와 그러한 목표의 달성을 측정하는 핵심 성과 지표를 토대로 예컨대 환경의 지속가능성, 장애인의 접근성, AI 시스템의 설계·개발에 대한 이해관계자의 참여, 개발 팀의 다양성 등과 관련된 요구사항을 AI 시스템에 자발적으로 장려하도록 촉구하는 행동 지침을 작성할 것을 장려하고 촉진해야 한다.

3. 행동 지침은 AI 시스템의 개별 제공자 또는 그들을 대표하는 조직 또는 둘 모두에 의해 작성될 수 있으며, 사용자와 이해관계자 및 그들을 대표하는 조직이 관여할 수 있다. 행동 지침은 관련 시스템들의 원래 목적이 지닌 유사성을 고려하여 하나 이상의 AI 시스템에 적용될 수 있다.

4. The Commission and the Board shall take into account the specific interests and needs of the small-scale providers and start-ups when encouraging and facilitating the drawing up of codes of conduct.

TITLE X

CONFIDENTIALITY AND PENALTIES

Article 70
Confidentiality

1. National competent authorities and notified bodies involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

   (a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.

   (b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;(c) public and national security interests;

   (c) integrity of criminal or administrative proceedings.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardise public and national security interests.

   When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 63(5) and (6), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the parties concerned to provide information under criminal law of the Member States.

4. The Commission and Member States may exchange, where necessary, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.

4. 유럽연합 집행위원회와 유럽 인공지능 위원회는 행동 지침의 작성을 장려·촉진할 때 소규모 제공자 및 스타트업의 이해와 요구를 고려해야 한다.

제10편

기밀 유지 및 처벌

제70조

기밀 유지

1. 본 규정의 적용에 관여하는 국가 관할 기관과 인증 기관은 과업과 활동을 수행하는 과정에서 획득한 정보와 데이터의 기밀을 존중해야 하며, 특히 다음을 보호해야 한다.

   (a) 소스 코드를 포함한, 자연인 또는 법인의 지적 재산권, 기밀 비즈니스 정보 또는 영업 비밀. 단, 미공개 노하우 및 비즈니스 정보(영업 비밀)를 불법 획득, 사용 및 공개로부터 보호하는 데 대한 Directive 2016/943 제5조에 언급된 사례는 예외로 한다.

   (b) 특히 검사, 조사 또는 감사 목적을 위한 본 규정의 효과적 시행

   (c) 공공 안전 및 국가 안보 이해

   (d) 사법 또는 행정 절차의 무결성.

2. 제1항을 침해함이 없이, 부속서 III의 제1, 6, 7항에 언급된 고위험 AI 시스템이 법 집행 또는 이주·망명 기관에 의해 사용되고 그러한 공개가 공공 안전 및 국가 안보 이해를 위태롭게 할 수 있는 경우 국가 관할 기관들 사이 및 국가 관할 기관과 유럽연합 집행위원회 사이에 기밀 유지 원칙에 따라 교환된 정보를 원 출처인 국가 관할 기관 및 사용자와의 사전 협의 없이 공개해서는 안 된다.

   법 집행 또는 이주·망명 기관이 부속서 III의 제1, 6, 7항에 언급된 고위험 AI 시스템의 제공자인 경우 부속서 IV에 언급된 기술 문서를 각 구내에 보관해야 한다. 동 기관은 제63(5)조 및 (6)조에 언급된 시장 감시 기관이 요청하는 경우 즉시 상기한 기술 문서에 접근하거나 그 사본을 획득할 수 있도록 보장해야 한다. 오로지 적절한 수준의 보안 허가를 받은 시장 감시 기관의 직원만 동 문서 또는 그 사본에 접근할 수 있다.

3. 제1항 및 2항은 정보 교환 및 경고 발령과 관련된 유럽연합 집행위원회, 회원국 및 인증 기관의 권리와 의무, 그리고 회원국의 형법에 따라 정보를 제공해야 할 관계 당사자들의 의무에 영향을 주지 않는다.

4. 유럽연합 집행위원회와 회원국은 필요할 경우 충분한 수준의 기밀을 보장하는 양자 또는 다자간 기밀 유지 협정을 체결한 제3국의 규제 기관과 기밀 정보를 교환할 수 있다.

Article 71
Penalties

1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the interests of small-scale providers and start-up and their economic viability.

2. The Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. The following infringements shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:

   (a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

   (b) non-compliance of the AI system with the requirements laid down in Article 10.

4. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. The supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request shall be subject to administrative fines of up to 10 000 000 EUR or, if the offender is a company, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement and of its consequences;

   (b) whether administrative fines have been already applied by other market surveillance authorities to the same operator for the same infringement.

   (c) the size and market share of the operator committing the infringement;

7. Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts of other bodies as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

제71조

처벌

1. 회원국은 본 규정에 명시된 조건에 따라 본 규정의 위반에 적용되는 과징금을 포함한 처벌에 관한 규칙을 명시하고 그것이 적절하고 효과적으로 시행되도록 보장하는 데 필요한 모든 조치를 취해야 한다. 규정된 처벌은 효과적이고 비례적이며 억제적이어야 한다. 이는 소규모 제공자와 스타트업의 이해 및 경제적 생존 능력을 특별히 고려해야 한다.

2. 회원국은 상기한 규칙과 조치를 유럽연합 집행위원회에 통지하고, 그들에게 영향을 미치는 추후의 개정을 지체 없이 유럽연합 집행위원회에 통지해야 한다.

3. 다음과 같은 위반에는 최대 30 000 000 EUR, 또는 위반자가 기업인 경우 전년도 전세계 연매출의 최대 6% 중에서 더 높은 금액의 과징금이 부과된다.

   (a) 제5조에 언급된 인공 지능 관행의 금지를 준수하지 않는 위반

   (b) AI 시스템이 제10조에 명시된 요구사항을 준수하지 않는 위반

4. AI 시스템이 본 규정에 따른 요구사항 또는 의무(제5조 및 10조에 명시된 것 제외)를 준수하지 않는 경우 최대 20 000 000 EUR, 또는 위반자가 기업인 경우 전년도 전세계 연매출의 최대 4% 중에서 더 높은 금액의 과징금이 부과된다.

5. 인증 기관과 국가 관할 기관의 요청에 응답하여 부정확하거나 불완전하거나 오도하는 정보를 제공하는 경우 최대 10 000 000 EUR, 또는 위반자가 기업인 경우 전년도 전세계 연매출의 최대 2% 중에서 더 높은 금액의 과징금이 부과된다

6. 각 개별 사례에서 과징금의 액수를 결정할 때는 모든 관련 상황을 고려하고 특히 다음 사항에 유의해야 한다.

   (a) 위반과 그 결과의 성격과 중대성 및 지속 기간

   (b) 다른 시장 감시 기관이 동일한 위반에 대해 동일한 운영자에게 이미 과징금을 적용했는지 여부

   (c) 위반을 한 운영자의 규모와 시장 점유율

7. 각 회원국은 동 회원국에서 설립된 공공 기관 및 기구에 과징금이 부과될 수 있는지 여부와 금액에 관한 규칙을 명시해야 한다.

8. 회원국의 법률 체계에 따라, 과징금에 관한 규칙은 다른 기구의 관할 국내 법원이 동 회원국에서 적용되는 것처럼 벌금을 부과하는 방식으로 적용될 수 있다. 동 회원국에서 그러한 규칙을 적용할 경우 동등한 효과를 가진다.

Article 72
Administrative fines on Union institutions, agencies and bodies

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, agencies and bodies falling within the scope of this Regulation. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

   (a) the nature, gravity and duration of the infringement and of its consequences;

   (b) the cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection Supervisor against the Union institution or agency or body concerned with regard to the same subject matter;

   (c) any similar previous infringements by the Union institution, agency or body;

2. The following infringements shall be subject to administrative fines of up to 500 000 EUR:

   (a)) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

   (b) non-compliance of the AI system with the requirements laid down in Article 10.

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 250 000 EUR.

4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, agency or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.

5. The rights of defense of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

6. Funds collected by imposition of fines in this Article shall be the income of the general budget of the Union.

TITLE XI

DELEGATION OF POWER AND COMMITTEE PROCEDURE

Article 73
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

제72조

유럽 연합 기관, 기구, 단체에 대한 과징금

1. 유럽 데이터 보호 감독관은 본 규정의 범위 내에 속하는 유럽 연합 기관, 기구, 단체에 과징금을 부과할 수 있다. 각 개별 사례에서 과징금을 부과할지 여부와 과징금의 액수를 결정할 때는 모든 관련 상황을 고려하고 특히 다음 사항에 유의해야 한다.

   (a) 위반과 그 결과의 성격과 중대성 및 지속 기간

   (b) 유럽 데이터 보호 감독관이 동일한 주제와 관련하여 해당 유럽 연합 기관, 기구 또는 단체에 대해 이전에 명령한 조치의 준수를 포함하여, 위반을 구제하고 위반의 부정적 효과를 완화하기 위한 유럽 데이터 보호 감독관과의 협력.

   (c) 유럽 연합 기관, 기구 또는 단체에 의한 이전의 유사한 위반

2. 다음과 같은 위반에는 최대 500 000 EUR의 과징금이 부과된다.

   (a) 제5조에 언급된 인공 지능 관행의 금지를 준수하지 않는 위반

   (b) AI 시스템이 제10조에 명시된 요구사항을 준수하지 않는 위반

3. AI 시스템이 본 규정에 따른 요구사항 또는 의무(제5조 및 10조에 명시된 것 제외)를 준수하지 않는 경우 최대 250 000 EUR의 과징금이 부과된다.

4. 유럽 데이터 보호 감독관은 본 조에 따른 결정을 내리기 전에 유럽 데이터 보호 감독관이 실시하는 법적 절차의 대상인 유럽 연합 기관, 기구 또는 단체에게 위반과 관련된 주제에 관해 의견을 개진할 기회를 주어야 한다. 유럽 데이터 보호 감독관은 오로지 관계 당사자들이 의견을 개진할 수 있었던 요소 및 상황에 근거해서만 결정을 내려야 한다. 제소자(있을 경우)는 법적 절차와 긴밀한 관련을 가져야 한다.

5. 법적 절차에서 관계 당사자의 항변권이 충분히 존중되어야 한다. 개인 또는 사업체가 각자의 개인 데이터 또는 영업 비밀의 보호에 대한 적법한 이해를 가진다는 전제 하에, 이들은 유럽 데이터 보호 감독관의 파일에 접근할 권한을 가진다.

6. 본 조의 벌금을 부과하여 징수한 자금은 유럽 연합 일반 예산의 수입이 된다.

제11편

권한의 위임과 위원회(Committee) 절차

제73조

위임의 행사

1. 본 조문에 명시된 조건에 따라 유럽연합 집행위원회는 위임 규정을 채택할 수 있는 권한을 부여받는다.

2. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall be conferred on the Commission for an indeterminate period of time from [*entering into force of the Regulation*].

3. The delegation of power referred to in Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. Any delegated act adopted pursuant to Article 4, Article 7(1), Article 11(3), Article 43(5) and (6) and Article 48(5) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 74
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

TITLE XII

FINAL PROVISIONS

Article 75
Amendment to Regulation (EC) No 300/2008

In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:

"When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Chapter 2, Title III of that Regulation shall be taken into account."

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 76
Amendment to Regulation (EU) No 167/2013

In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:

2. 제4조, 제7(1)조, 제11(3)조, 제43(5) 및 (6)조, 제48(5)조에 언급된 권한의 위임은 [*규정 발효일*]로부터 무기한으로 유럽연합 집행위원회에 부여된다.

3. 제4조, 제7(1)조, 제11(3)조, 제43(5) 및 (6)조, 제48(5)조에 언급된 권한의 위임은 언제든지 유럽 의회 또는 이사회에 의해 취소될 수 있다. 취소 결정은 동 결정에 명시된 권한의 위임을 끝낸다. 동 결정은 *유럽 연합 관보(Official Journal of the European Union)*에 게재된 날의 다음날 또는 동 결정에 명시된 차후 날짜에 발효된다. 동 결정은 이미 시행 중인 위임 규정의 유효성에 영향을 주지 않는다.

4. 유럽연합 집행위원회는 위임 규정을 채택하는 즉시 유럽 의회와 이사회에 동시에 통지해야 한다.

5. 제4조, 제7(1)조, 제11(3)조, 제43(5) 및 (6)조, 제48(5)조에 따라 채택된 위임 규정은 오로지 동 규정을 유럽 의회와 이사회에 통지한 후 3개월 기간 내에 유럽 의회 또는 이사회가 반대를 표명하지 않거나, 동 기간의 만료 전에 유럽 의회와 이사회가 모두 반대하지 않을 것임을 유럽연합 집행위원회에 통지한 경우에만 발효된다. 동 기간은 유럽 의회 또는 이사회의 주도로 3개월 연장된다.

제74조

위원회 절차

1. 유럽연합 집행위원회는 위원회(committee)의 조력을 받는다. 동 위원회는 Regulation (EU) No 182/2011의 의미 내에서 위원회(committee)여야 한다.

2. 본 항에 대한 참조가 이루어질 경우 Regulation (EU) No 182/2011 제5항이 적용된다.

제12편

최종 조항

제75조

Regulation (EC) No 300/2008의 개정

Regulation (EC) No 300/2008 제4(3)조에 다음 호(subparagraph)를 추가한다.

"기술 규격과 승인 절차 및 [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 인공 지능 시스템과 관련된 보안 장비의 사용과 관련된 세부 조치를 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Chapter 2, Title III of that Regulation shall be taken into account)."

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

제76조

Regulation (EU) No 167/2013의 개정

Regulation (EU) No 167/2013 제17(5)조에 다음 호를 추가한다.

"When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 77
Amendment to Regulation (EU) No 168/2013

In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:

"When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX on [Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

Article 78
Amendment to Directive 2014/90/EU

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

"4. For Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Title III, Chapter 2 of that Regulation.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 79
Amendment to Directive (EU) 2016/797

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

"12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

"[인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 첫 호에 따라 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

제77조

Regulation (EU) No 168/2013의 개정

Regulation (EU) No 168/2013 제22(5)조에 다음 호를 추가한다.

"[인공 지능]에 관한 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 첫 호에 따라 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX on [Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

제78조

Directive 2014/90/EU의 개정

Directive 2014/90/EU 제8조에 다음 호를 추가한다.

"4. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템의 경우, 제1항에 따른 활동을 수행할 때 그리고 제2항 및 3항에 따른 기술 규격과 테스트 표준을 채택할 때 유럽연합 집행위원회는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(For Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Title III, Chapter 2 of that Regulation).

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

제79조

Directive (EU) 2016/797의 개정

Directive (EU) 2016/797 제5조에 다음 항을 추가한다.

"12. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항에 따른 위임 규정과 제11항에 따른 실행 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 80
Amendment to Regulation (EU) 2018/858

In Article 5 of Regulation (EU) 2018/858 the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council *, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 81
Amendment to Regulation (EU) 2018/1139

Regulation (EU) 2018/1139 is amended as follows:

(1) In Article 17, the following paragraph is added:

"3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [*on Artificial Intelligence*] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

_____

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

(2) In Article 19, the following paragraph is added:

"4. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(3) In Article 43, the following paragraph is added:

"4. When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(4) In Article 47, the following paragraph is added:

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(5) In Article 57, the following paragraph is added:

"When adopting those implementing acts concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account."

(6) In Article 58, the following paragraph is added:

제80조

Regulation (EU) 2018/858의 개정

Regulation (EU) 2018/858 제5조에 다음 항을 추가한다.

"4. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제3항에 따른 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council *, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

제81조

Regulation (EU) 2018/1139의 개정

Regulation (EU) 2018/1139를 다음과 같이 개정한다.

(1) 제17조에 다음 항을 추가한다.

"3. 제2항을 침해함이 없이, [*인공 지능에 관한*] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항에 따른 실행 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [*on Artificial Intelligence*] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …)."

(2) 제19조에 다음 항을 추가한다.

"4. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항 및 2항에 따른 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account)."

(3) 제43조에 다음 항을 추가한다.

"4. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항에 따른 실행 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account)."

(4) 제47조에 다음 항을 추가한다.

"3. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항 및 2항에 따른 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account)."

(5) 제57조에 다음 항을 추가한다.

"[인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 실행 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting those implementing acts concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence], the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account)."

(6) 제58조에 다음 항을 추가한다.

"3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] , the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.".

Article 82
Amendment to Regulation (EU) 2019/2144

In Article 11 of Regulation (EU) 2019/2144, the following paragraph is added:

"3. When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account.

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

Article 83
AI systems already placed on the market or put into service

1. This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

   The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.

2. This Regulation shall apply to the high-risk AI systems, other than the ones referred to in paragraph 1, that have been placed on the market or put into service before [*date of application of this Regulation referred to in Article 85(2)*], only if, from that date, those systems are subject to significant changes in their design or intended purpose.

Article 84
Evaluation and review

1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.

2. By [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

3. The reports referred to in paragraph 2 shall devote specific attention to the following:

   (a) the status of the financial and human resources of the national competent authorities in order to effectively perform the tasks assigned to them under this Regulation;

"3. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제1항 및 2항에 따른 위임 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] , the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account)."

제82조

Regulation (EU) 2019/2144의 개정

Regulation (EU) 2019/2144 제11조에 다음 항을 추가한다.

"3. [인공 지능에 관한] 유럽 의회 및 유럽 이사회 Regulation (EU) YYY/XX*의 의미에서 안전 구성요소인 인공 지능 시스템과 관련한 제2항에 따른 실행 규정을 채택할 때는 동 규정의 제3편 제2장에 명시된 요구사항을 고려해야 한다(When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components in the meaning of Regulation (EU) YYY/XX [on Artificial Intelligence] of the European Parliament and of the Council*, the requirements set out in Title III, Chapter 2 of that Regulation shall be taken into account).

---

* Regulation (EU) YYY/XX [on Artificial Intelligence] (OJ …).".

제83조

이미 출시되거나 서비스 개시된 AI 시스템

1. 본 규정은 *[제85(2)조에 언급된 본 규정이 적용된 날로부터 12개월 후]* 이전에 출시되거나 서비스 개시되고 부속서 IX에 열거된 법규에 의해 구축된 대규모 IT 시스템의 구성요소인 AI 시스템에는 적용되지 않는다. 단, 그러한 법규의 교체 또는 개정이 관련 AI 시스템의 설계 또는 원래 목적의 중대한 변경으로 이어지는 경우는 예외로 한다.

   부속서 IX에 열거된 법규의 규정에 따라 수행되는, 동 법규에 의해 구축된 대규모 IT 시스템에 대한 평가에서 본 규정에 명시된 요구사항을 고려해야 한다.

2. 본 규정은 *[제85(2)조에 언급된 본 규정이 적용된 날짜]* 이전에 출시되거나 서비스 개시된, 제1항에 언급된 것 이외의 고위험 AI 시스템이 상기한 날짜로부터 그 설계 또는 원래 목적의 중대한 변경을 수반하는 경우에 한하여 적용된다.

제84조

평가 및 검토

1. 유럽연합 집행위원회는 본 규정의 발효 후 연 1회에 걸쳐 부속서 III의 목록을 개정할 필요성을 평가한다.

2. [*제85(2)조에 언급된 본 규정이 적용되는 날로부터 3년 후*]에 그리고 이후로 4년마다 유럽연합 집행위원회는 본 규정의 평가 및 검토에 관한 보고서를 유럽 의회와 이사회에 제출한다. 보고서는 일반에 공개한다.

3. 2항에 언급된 보고서는 다음 사항에 특별히 주의를 기울여야 한다.

   (a) 본 규정에 따라 국가 관할 기관에 할당된 과업을 효과적으로 수행하기 위한 동 기관의 재정 및 인적 자원의 상태

(b) the state of penalties, and notably administrative fines as referred to in Article 71(1), applied by Member States to infringements of the provisions of this Regulation.

4. Within [*three years after the date of application of this Regulation referred to in Article 85(2)*] and every four years thereafter, the Commission shall evaluate the impact and effectiveness of codes of conduct to foster the application of the requirements set out in Title III, Chapter 2 and possibly other additional requirements for AI systems other than high-risk AI systems.

5. For the purpose of paragraphs 1 to 4 the Board, the Member States and national competent authorities shall provide the Commission with information on its request.

6. In carrying out the evaluations and reviews referred to in paragraphs 1 to 4 the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

7. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology and in the light of the state of progress in the information society.

Article 85
Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from [24 months following the entering into force of the Regulation].

3. By way of derogation from paragraph 2:

(a) Title III, Chapter 4 and Title VI shall apply from [three months following the entry into force of this Regulation];

(b) Article 71 shall apply from [twelve months following the entry into force of this Regulation].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

(b) 회원국이 본 규정의 위반에 적용한 처벌의 상태, 특히 71(1)조에 언급된 과징금.

4. [*제85(2)조에 언급된 본 규정이 적용되는 날로부터 3년 후*] 이내에 그리고 이후로 4년마다 유럽연합 집행위원회는 제3편 제2장에 명시된 요구사항과 고위험 AI 시스템이 아닌 AI 시스템에 대한 기타 추가 요구사항의 적용을 촉진하는 행동 지침의 영향과 효과를 평가한다.

5. 제1~4항의 목적을 위해, 유럽 인공지능 위원회, 회원국 및 국가 관할 기관은 유럽연합 집행위원회의 요청에 관한 정보를 유럽연합 집행위원회에 제공한다.

6. 1~4항에 언급된 평가와 검토를 수행하는 과정에서 유럽연합 집행위원회는 유럽 인공지능 위원회, 유럽 의회, 유럽 이사회 및 기타 관련 기구 또는 출처의 입장과 조사 결과를 고려한다.

7. 필요할 경우 유럽연합 집행위원회는 특히 기술의 발전과 정보 사회의 진보 상태를 고려하여 본 규정을 개정하기 위한 적절한 제안을 제출한다.

제85조
발표 및 적용

1. 본 규정은 *유럽 연합 관보*에 게재된 날로부터 12일째 되는 날에 발효된다.

2. 본 규정은 [규정이 발효된 지 24개월 후]부터 적용된다.

3. 제2항의 개정을 통해:

(a) 제3편 제4장 및 제6편은 [본 규정이 발효된 지 3개월 후]부터 적용된다.

(b) 제71조는 [본 규정이 발효된 지 12개월 후]부터 적용된다.

본 규정은 모든 회원국에서 완전한 구속력을 가지며 직접 적용된다. 브뤼셀에서 작성.

유럽 의회
의장

유럽 이사회
의장

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned

1.3. The proposal/initiative relates to:

1.4. Objective(s)

1.4.1. General objective(s)

1.4.2. Specific objective(s)

1.4.3. Expected result(s) and impact

1.4.4. Indicators of performance

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone

1.5.3. Lessons learned from similar experiences in the past

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

1.5.5 Assessment of the different available financing options, including scope for redeployment

1.6. Duration and financial impact of the proposal/initiative

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

입법 재정 설명서(LEGISLATIVE FINANCIAL STATEMENT)

1. 제안/이니셔티브의 프레임워크

1.1. 제안/이니셔티브의 제목

1.2. 관련 정책 분야

1.3. 다음과 관련된 제안/이니셔티브:

1.4. 목표

1.4.1. 일반적 목표

1.4.2. 구체적 목표

1.4.3. 예상되는 결과와 영향

1.4.4. 성과 지표

1.5. 제안/이니셔티브의 근거

1.5.1. 이니셔티브의 실행을 위한 세부 일정을 포함하여, 단기 또는 장기적으로 충족해야 할 요구사항

1.5.2. 유럽 연합의 관여에 따른 (조정 이득, 법적 확실성, 효과 개선, 상보성 등 다양한 요인에서 비롯되는) 부가 가치. 본 호(point)의 목적을 위해 '유럽 연합 관여의 부가 가치(added value of Union involvement)'는 유럽 연합의 개입에서 비롯되는, 회원국 단독으로 수행한 경우에 생성되었을 가치에 부가되는 가치를 말한다.

1.5.3. 과거의 유사한 경험에서 얻은 교훈

1.5.4. 다년간 재무 프레임워크(MFF)와의 양립성 및 다른 관련 기관들과의 시너지 효과

1.5.5 재배치의 범위를 포함한 다양한 자금 조달 옵션의 평가

1.6. 제안/이니셔티브의 지속 기간 및 재정적 영향

1.7. 계획된 관리 방식

2. 관리 수단

2.1. 모니터링 및 보고 규칙

2.2. 관리 및 통제 시스템

2.2.1. 제안된 관리 방식, 자금 조달 메커니즘, 지불 방식 및 제어 전략의 정당화

2.2.2. 파악된 위험에 관한 정보 및 이를 완화하기 위해 구축된 내부 통제 시스템

2.2.3. 통제의 비용 효과("통제 비용 ÷ 관리되는 관련 자금의 가치"의 비율) 추정 및 정당화, (지불 시 및 완료 시) 예상되는 오류 위험 수준의 평가

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

3.2.2. Estimated output funded with operational appropriations

3.2.3. Summary of estimated impact on administrative appropriations

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

2.3. 사기와 부정을 방지하기 위한 수단

3. 제안/이니셔티브의 재정적 영향 추정

3.1. 영향을 받는 다년간 재무 프레임워크 및 지출 예산선의 항목

3.2. 제안이 예산(appropriations)에 미치는 재정적 영향 추정

3.2.1. 운영 예산(operational appropriations)에 미치는 영향의 요약

3.2.2. 운영 예산을 통해 자금이 제공된 산출물(output) 추정

3.2.3. 행정 예산(administrative appropriations)에 미치는 영향의 요약

3.2.4. 현행 다년간 재무 프레임워크와의 양립성

3.2.5. 제3자 기여

3.3. 수익에 미치는 영향 추정

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

1.2. Policy area(s) concerned

Communications Networks, Content and Technology;

Internal Market, Industry, Entrepreneurship and SMEs;

The budgetary impact concerns the new tasks entrusted with the Commission, including the support to the EU AI Board;

Activity: Shaping Europe's digital future.

1.3. The proposal/initiative relates to:

X **a new action**

☐ **a new action following a pilot project/preparatory action**[64]

☐ **the extension of an existing action**

☐ **an action redirected towards a new action**

1.4. Objective(s)

1.4.1. General objective(s)

The general objective of the intervention is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy artificial intelligence in the Union.

1.4.2. Specific objective(s)

Specific objective No 1

To set requirements specific to AI systems and obligations on all value chain participants in order to ensure that AI systems placed on the market and used are safe and respect existing law on fundamental rights and Union values;

Specific objective No 2

To ensure legal certainty to facilitate investment and innovation in AI by making it clear what essential requirements, obligations, as well as conformity and compliance procedures must be followed to place or use an AI system in the Union market;

Specific objective No 3

To enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems by providing new powers, resources and clear rules for relevant authorities on conformity assessment and ex

[64] As referred to in Article 54(2)(a) or (b) of the Financial Regulation

입법 재정 설명서

1. 제안/이니셔티브의 프레임워크

1.1. 제안/이니셔티브의 제목

인공 지능에 관한 조화 규칙(인공지능법)을 제정하고 특정 유럽 연합 법규를 개정하는 유럽 의회 및 유럽 이사회의 규정

1.2. 관련 정책 분야

통신 네트워크, 콘텐츠 및 기술; 역내 시장, 산업, 기업가
활동 및 중소기업;
예산 책정은 유럽 인공지능 위원회에 대한 지원을 포함한 유럽연합 집행위원회의 새로운 과업에 영향을 미친다;
활동: 유럽의 디지털 미래 구축.

1.3. 다음과 관련된 제안/이니셔티브:

X **새로운 조치**

☐ **파일럿 프로젝트/예비 조치[64]에 이은 새로운 조치**

☐ **기존 조치의 연장**

☐ **새로운 조치로 방향 전환된 조치**

1.4. 목표

1.4.1. 일반적 목표

개입의 일반적 목표는 유럽 연합에서 신뢰할 수 있는 인공 지능의 개발과 사용을 위한 조건을 창출하여 단일 시장의 올바른 기능을 보장하는 것이다.

1.4.2. 구체적 목표

구체적 목표 No 1

출시된 AI 시스템이 안전하게 사용되고 기존의 기본권 법률과 유럽 연합의 가치를 존중하도록 보장하기 위해 AI 시스템에 특정한 요구사항과 가치 사슬의 모든 참가자들에게 부과되는 의무를 규정한다.

구체적 목표 No 2

AI 시스템을 유럽 연합 시장에서 출시하거나 사용하려면 어떠한 필수 요건, 의무, 그리고 적합성 및 준수 절차를 따라야 하는지 분명히 밝힘으로써 AI 에 대한 투자와 혁신을 촉진하는 법적 확실성을 보장한다.

구체적 목표 No 3

관련 기관을 위해 적합성 평가 및 사후 모니터링 절차, 그리고 국가와 EU 간의 거버넌스/감독 업무 구분에 관한 명확한 규칙과 새로운 권한 및 자원을

[64] Financial Regulation의 제54(2)(a) 또는 (b)항에 언급

post monitoring procedures and the division of governance and supervision tasks between national and EU levels;

Specific objective No 4

To facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation by taking EU action to set minimum requirement for AI systems to be placed and used in the Union market in compliance with existing law on fundamental rights and safety.

제공하여 AI 시스템에 적용되는 기존의 기본권 법률 및 안전 요구사항의 효과적 집행과 거버넌스를 강화한다.

구체적 목표 No 4

적법하고 안전하고 신뢰할 수 있는 AI 애플리케이션을 위한 단일 시장의 개발을 촉진하고 기본권과 안전에 관한 기존 법률을 준수하면서 유럽 연합 시장에서 출시되거나 사용되는 AI 시스템을 위한 최소 요건을 설정하는 EU 조치를 취하여 시장 파편화를 방지한다.

1.4.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

AI suppliers should benefit from a minimal but clear set of requirements, creating legal certainty and ensuring access to the entire single market.

AI users should benefit from legal certainty that the high-risk AI systems they buy comply with European laws and values.

Consumers should benefit by reducing the risk of violations of their safety or fundamental rights.

1.4.4. Indicators of performance

Specify the indicators for monitoring implementation of the proposal/initiative.

Indicator 1

Number of serious incidents or AI performances which constitute a serious incident or a breach of fundamental rights obligations (semi-annual) by fields of applications and calculated a) in absolute terms, b) as share of applications deployed and c) as share of citizens concerned.

Indicator 2

a) Total AI investment in the EU (annual)

b) Total AI investment by Member State (annual)

c) Share of companies using AI (annual)

d) Share of SMEs using AI (annual)

a) and b) will be calculated based on official sources and benchmarked against private estimates

c) and d) will be collected by regular company surveys

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Regulation should be fully applicable one year and a half after its adoption. However, elements of the governance structure should be in place before then. In particular, Member States shall have appointed existing authorities and/or established new authorities performing the tasks set out in the legislation earlier, and the EU AI Board should be set-up and effective. By the time of applicability, the European database of AI systems should be fully operative. In parallel to the adoption process, it is therefore necessary to develop the database, so that its development has come to an end when the regulation enters into force.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

An emerging patchy framework of potentially divergent national rules will hamper the seamless provision of AI systems across the EU and is ineffective in ensuring the

1.4.3. 예상되는 결과와 영향

제안/이니셔티브가 수혜자/대상 그룹에 미치는 효과 명시.

AI 공급자는 법적 확실성과 전체 단일 시장에 대한 접근을 보장하는 명확하면서도 최소화된 요구사항의 혜택을 입는다.
AI 사용자는 구매하는 고위험 AI 시스템이 유럽의 법률과 가치를 준수한다는 법적 확실성의 혜택을 입는다.
소비자는 안전 또는 기본권이 침해될 위험이 완화되는 혜택을 입는다.

1.4.4. 성과 지표

제안/이니셔티브의 실행 모니터링을 위한 지표 명시.

지표 1
애플리케이션 분야별로 중대한 사건 또는 기본권 의무의 위반을 구성하고, a) 절대값, b) 배포된 애플리케이션의 점유율, c) 관련 시민의 점유율로 계산한 중대한 사건 또는 AI 수행의 수(연 2회).
지표 2
a) EU의 AI에 대한 총 투자(연간)
b) 회원국의 AI에 대한 총 투자(연간)
c) AI를 사용하는 기업의 점유율(연간)
d) AI를 사용하는 중소기업의 점유율(연간)
a) 및 b)는 공식 자료를 토대로 계산하고 민간 추정치를 기준으로 벤치마킹한다.
c) 및 d)는 기업의 정기 설문조사를 통해 수집한다

1.5. 제안/이니셔티브의 근거

1.5.1. 이니셔티브의 실행을 위한 세부 일정을 포함하여, 단기 또는 장기적으로 충족해야 할 요구사항

규정은 채택 1년 반 후에 완전히 적용되어야 한다. 단, 그 전에 거버넌스 구조의 요소들이 갖춰져야 한다. 특히 회원국은 이전의 법률에 명시된 과업을 수행할 기존 기관을 임명하거나 새로운 기관을 설립해야 하며, 유럽 인공지능 위원회가 수립·운영되어야 한다.
규정이 적용되는 시점에 AI 시스템의 유럽 데이터베이스가 완전히 가동되어야 한다.
따라서 채택 프로세스와 병행하여 데이터베이스의 개발에 착수하고 규정이 발효될 때 개발이 완료되도록 해야 한다.

1.5.2. 유럽 연합의 관여에 따른 (조정 이득, 법적 확실성, 효과 개선, 상보성 등 다양한 요인에서 비롯되는) 부가 가치. 본 호(point)의 목적을 위해 '유럽 연합 관여의 부가 가치(added value of Union involvement)'는 유럽 연합의 개입에서 비롯되는, 회원국 단독으로 수행한 경우에 생성되었을 가치에 부가되는 가치를 말한다.

제각각 일치하지 않는 새로운 국가 규칙들은 AI 시스템과 관련된 제품과 서비스가 EU 전역에서 매끄럽게 유통되는 데 방해가 되고 다양한 회원국

safety and protection of fundamental rights and Union values across the different Member States. A common EU legislative action on AI could boost the internal market and has great potential to provide European industry with a competitive edge at the global scene and economies of scale that cannot be achieved by individual Member States alone.

1.5.3. Lessons learned from similar experiences in the past

The E-commerce Directive 2000/31/EC provides the core framework for the functioning of the single market and the supervision of digital services and sets a basic structure for a general cooperation mechanism among Member States, covering in principle all requirements applicable to digital services. The evaluation of the Directive pointed to shortcomings in several aspects of this cooperation mechanism, including important procedural aspects such as the lack of clear timeframes for response from Member States coupled with a general lack of responsiveness to requests from their counterparts. This has led over the years to a lack of trust between Member States in addressing concerns about providers offering digital services cross-border. The evaluation of the Directive showed the need to define a differentiated set of rules and requirements at European level. For this reason, the implementation of the specific obligations laid down in this Regulation would require a specific cooperation mechanism at EU level, with a governance structure ensuring coordination of specific responsible bodies at EU level.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The Regulation Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts defines a new common framework of requirements applicable to AI systems, which goes well beyond the framework provided by existing legislation. For this reason, a new national and European regulatory and coordination function needs to be established with this proposal.

As regards possible synergies with other appropriate instruments, the role of notifying authorities at national level can be performed by national authorities fulfilling similar functions sunder other EU regulations.

Moreover, by increasing trust in AI and thus encouraging investment in development and adoption of AI, it complements Digital Europe, for which promoting the diffusion of AI is one of five priorities.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The staff will be redeployed. The other costs will be supported from the DEP. envelope, given that the objective of this regulation – ensuring trustworthy AI – contributes directly to one key objective of Digital Europe – accelerating AI development and deployment in Europe.

사이에서 기본권과 유럽 연합 가치를 보호하는 데 효과적이지 못할 것이다. AI에 관한 EU 공통의 법규는 역내 시장을 활성화하고, 개별 회원국이 단독으로 성취할 수 없는 글로벌 경쟁 우위와 규모의 경제를 유럽 산업에 제공할 수 있다.

1.5.3. 과거의 유사한 경험에서 얻은 교훈

E-commerce Directive 2000/31/EC는 원칙적으로 디지털 서비스에 적용되는 모든 요구사항을 망라하는, 단일 시장의 기능과 디지털 서비스의 감독을 위한 핵심 프레임워크와 회원국들 사이의 일반적 협력 메커니즘을 위한 기본 구조를 규정한다. Directive의 평가는 회원국의 응답을 위한 명확한 기한의 결여 및 상대방의 요청에 대한 응답성의 일반적 결여와 같은 중요한 절차적 측면을 포함한 몇 가지 측면에서 이러한 협력 메커니즘의 결함을 지적했다. 이는 다년간에 걸쳐 국가간 디지털 서비스 제공자들에 관한 문제를 처리하는 과정에서 회원국 간의 신뢰 부족으로 이어졌다. Directive의 평가는 유럽 수준에서 차별화된 일련의 규칙과 요구사항을 정의해야 할 필요성을 보여주었다. 이런 이유로, 본 규정에 명시된 의무를 이행하기 위해서는 EU 수준에서 담당 기관들을 조율하는 거버넌스 구조를 갖춘 EU 수준의 협력 메커니즘이 필요할 것이다.

1.5.4. 다년간 재무 프레임워크(MFF)와의 양립성 및 다른 관련 기관들과의 시너지 효과

인공 지능에 관한 조화 규칙(인공지능법)을 제정하고 특정 유럽 연합 법규를 개정하는 유럽 의회 및 유럽 이사회의 규정은 기존 법규에 규정된 프레임워크를 뛰어넘는 AI 시스템에 적용되는 요구사항의 새로운 공통 프레임워크를 정의한다. 이런 이유에서, 본 제안을 통해 새로운 국가 및 유럽 수준의 규제·조율 기능이 수립되어야 한다.

다른 기관들과의 시너지 효과와 관련하여, 국가 수준에서 통보 기관의 역할을 다른 EU 규정에 따라 유사한 기능을 담당하는 국가 기관이 수행할 수 있다.

나아가, AI에 대한 신뢰를 증진하고 AI의 개발과 채택에 대한 투자를 장려함으로써, AI의 보급을 촉진하는 것이 5대 우선 과제의 하나인 디지털 유럽(Digital Europe) 프로젝트를 보완한다.

1.5.5. 재배치의 범위를 포함한 다양한 자금 조달 옵션의 평가

직원은 재배치된다. 신뢰할 수 있는 AI를 보장한다는 본 규정의 목표가 Digital Europe의 주요 목표—유럽에서 AI의 개발과 배포를 가속화하는 것—에 직접 기여하는 점을 감안하여, 기타 비용은 DEP. 엔벨로프(envelope)에서 지원한다.

1.6. Duration and financial impact of the proposal/initiative

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

X **unlimited duration**

– Implementation with a start-up period from one/two (tbc) year,

– followed by full-scale operation.

1.7. Management mode(s) planned[65]

X **Direct management** by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐ the EIB and the European Investment Fund;

– ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

Comments

[65] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

1.6. 제안/이니셔티브의 지속 기간 및 재정적 영향

☐ **지속 기간 제한**

– [DD/MM]YYYY부터 [DD/MM]YYYY까지 시행

– 재정적 영향: 사업 예산(commitment appropriations)의 경우 YYYY부터 YYYY까지 및 지출 예산(payment appropriations)의 경우 YYYY부터 YYYY까지.

X **지속 기간 무제한**

– 1/2(추후 확정)년부터 착수 기간(start-up period)을 두고 실행

– 이후 완전 가동.

1.7. 계획된 관리 방식[65]

X 유럽연합 집행위원회의 **직접 관리**

– 부서를 통해(유럽 연합 대표부 직원 포함)

– 집행 기관을 통해

☐ 회원국들의 **공동 관리**

☐ 예산 집행 업무를 다음에 위탁하여 **간접 관리**:

– 제3국 또는 그들이 지명한 단체

– 국제 조직 및 그 기관(추후 명시)

– 유럽투자은행(EIB) 및 유럽투자기금(EIF)

– 재무 규정(Financial Regulation) 제70조 및 71조에 언급된 단체

– 공법상 단체

– 공공 서비스 임무를 부여받고 충분한 재정 보증을 제공하는, 사법(私法)에 의해 관리되는 단체

– 민관 협력 사업의 시행을 위임받고 충분한 재정 보증을 제공하는, 회원국의 사법(私法)에 의해 관리되는 단체

– TEU 제5편에 따라 CFSP에서 특정 조치의 시행을 위임받고 관련 기본법에 명시된 사람.

– *둘 이상의 관리 방식을 표시하는 경우 '논평' 섹션에 상세히 기재.*

논평

65 관리 방식의 세부사항과 Financial Regulation에 대한 참조는 BudgWeb 사이트에서 확인할 수 있다: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The Regulation will be reviewed and evaluated five years from the entry into force of the regulation. The Commission will report on the findings of the evaluation to the European Parliament, the Council and the European Economic and Social Committee.

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

The Regulation establishes a new policy with regard to harmonised rules for the provision of artificial intelligence systems in the internal market while ensuring the respect of safety and fundamental rights. These new rules require a consistency mechanism for the cross-border application of the obligations under this Regulation in the form of a new advisory group coordinating the activities of national authorities.

In order to face these new tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the new Regulation is estimated to require 10 FTE à regime (5 FTE for the support to the activities of the Board and 5 FTE for the European Data Protection Supervisor acting as a notifying body for AI systems deployed by a body of the European Union).

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

In order to ensure that the members of the Board have the possibility to make informed analysis on the basis of factual evidence, it is foreseen that the Board should be supported by the administrative structure of the Commission and that an expert group be created to provide additional expertise where required.

2.2.3. Estimate and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

For the meeting expenditure, given the low value per transaction (e.g. refunding travel costs for a delegate for a meeting), standard control procedures seem sufficient. Regarding the development of the database, contract attribution has a strong internal control system in place in DG CNECT through centralised procurement activities.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.

2. 관리 수단

2.1. 모니터링 및 보고 규칙

빈도 및 조건 명시.

본 규정은 발효일로부터 5년 후에 검토·평가한다. 유럽연합 집행위원회는 평가 결과를 유럽 의회, 이사회 및 유럽 경제 사회 위원회에 보고한다.

2.2. 관리 및 통제 시스템

2.2.1. 제안된 관리 방식, 자금 조달 메커니즘, 지불 방식 및 제어 전략의 정당화

규정은 역내 시장에서 안전과 기본권을 보호하면서 인공 지능 시스템을 제공하는 데 대한 조화 규칙과 관련하여 새로운 정책을 수립한다. 이 새로운 규칙은 국가 기관들의 활동을 조율하는 새로운 자문 그룹의 형태로 본 규정에 따른 의무의 국가간 적용을 위한 일관성 메커니즘을 요구한다. 이 새로운 과업을 감당하기 위해서는 유럽연합 집행위원회의 업무에 적절한 자원을 제공할 필요가 있다. 새로운 규정의 집행에는 10 FTE가 필요할 것으로 추정된다(유럽 인공지능 위원회의 활동 지원을 위해 5 FTE, 유럽 연합의 단체가 배포하는 AI 시스템에 대한 통보 기관 역할을 하는 유럽 데이터 보호 감독관을 위해 5 FTE).

2.2.2. 파악된 위험에 관한 정보 및 이를 완화하기 위해 구축된 내부 통제 시스템

유럽 인공지능 위원회의 위원들이 사실 증거에 근거한 분석을 수행할 수 있도록 보장하기 위해 유럽연합 집행위원회의 행정 구조를 통해 지원을 받고 필요할 경우 추가적 전문지식을 제공하는 전문가 그룹을 구성해야 할 것으로 생각된다.

2.2.3. 통제의 비용 효과("통제 비용 ÷ 관리되는 관련 자금의 가치"의 비율) 추정 및 정당화, (지불 시 및 완료 시) 예상되는 오류 위험 수준의 평가

건당 금액이 낮은 점을 고려할 때(예: 회의 대표를 위한 여행 비용 환불), 회의 경비에 대해서는 표준 제어 절차로 충분해 보인다. 데이터베이스의 개발과 관련하여, 계약 귀속(contract attribution)은 중앙 집권화된 조달 활동을 통해 DG CNECT에 강력한 내부 통제 시스템을 구축했다.

2.3. 사기와 부정을 방지하기 위한 수단

구상 중인 방지 및 보호 수단 명시(예: 사기 방지 전략).

유럽연합 집행위원회에 적용되는 기존의 사기 방지 수단은 본 규정에 필요한 추가 예산(appropriations)을 망라할 것이다.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[66]	from EFTA countries [67]	from candidate countries[68]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
7	20 02 06 Administrative expenditure	Non-diff.	NO	NO	NO	NO
1	02 04 03 DEP Artificial Intelligence	Diff.	YES	NO	NO	NO
1	02 01 30 01 Support expenditure for the Digital Europe programme	Non-diff.	YES	NO	NO	NO

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on expenditure on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– X The proposal/initiative requires the use of operational appropriations, as explained below:

EUR million (to three decimal places)

66 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

67 EFTA: European Free Trade Association.

68 Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3. 제안/이니셔티브의 재정적 영향 추정

3.1. 영향을 받는 다년간 재무 프레임워크 및 지출 예산선의 항목

- 기존 예산선

순서: 다년간 재무 프레임워크 항목 및 예산선

다년간 재무 프레임워크의 항목	예산선	지출유형	기여			
	번호	Diff./Non-diff.[66]	EFTA 국가[67]	후보 국가[68]	제3국	재무 규정 제21(2)(b)조의 의미 내에서
7	20 02 06 행정 지출	Non-diff.	NO	NO	NO	NO
1	02 04 03 DEP 인공 지능	Diff.	YES	NO	NO	NO
1	02 01 30 01 Digital Europe 프로그램을 위한 지원 지출	Non-diff.	YES	NO	NO	NO

3.2. 제안이 예산(appropriations)에 미치는 재정적 영향 추정

3.2.1. 운영 예산에 미치는 영향의 요약

– 제안/이니셔티브는 운영 예산의 사용을 요구하지 않는다.

– X 제안/이니셔티브는 운영 예산의 사용을 요구한다(아래에 설명).

100만 EUR(소수점 이하 세 자리)

66 Diff. = 차별화된 예산(Differentiated appropriations) / Non-diff. = 비 차별화된 예산(Non-differentiated appropriations).
67 EFTA: 유럽 자유 무역 연합(European Free Trade Association).
68 후보 국가 및 해당될 경우 서부 발칸 반도의 잠재적 후보 국가.

Heading of multiannual financial framework	1	

DG: CNECT				Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**[69]	**TOTAL**	
• Operational appropriations											
Budget line[70] 02 04 03	Commitments	(1a)			1.000						**1.000**
	Payments	(2a)			0.600	0.100	0.100	0.100	0.100		**1.000**
Budget line	Commitments	(1b)									
	Payments	(2b)									
Appropriations of an administrative nature financed from the envelope of specific programmes[71]											
Budget line 02 01 30 01		(3)			0.240	0.240	0.240	0.240	0.240		**1.200**
TOTAL appropriations for DG CNECT	Commitments	=1a+1b +3			**1.240**		**0.240**	**0.240**	**0.240**		**2.200**
	Payments	=2a+2b +3			**0.840**	**0.340**	**0.340**	**0.340**	**0.340**		**2.200**

69 Indicative and dependent on budget availability.
70 According to the official budget nomenclature.
71 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

다년간 재무 프레임워크의 항목	1	

DG: CNECT				2022년	2023년	2024년	2025년	2026년	2027년[69]	합계	
• 운영 예산											
예산선[70] 02 04 03		사업 예산	(1a)		1.000						**1.000**
		지출 예산	(2a)		0.600	0.100	0.100	0.100	0.100		**1.000**
예산선		사업 예산	(1b)								
		지출 예산	(2b)								
특정 프로그램의 엔벨로프에서 재정 지원을 받는 행정적 성격의 예산[71]											
예산선 02 01 30 01			(3)		0.240	0.240	0.240	0.240	0.240		**1.200**
DG CNECT에 대한 총 예산		사업 예산	=1a+1b +3		**1.240**		**0.240**	**0.240**	**0.240**		**2.200**
		지출 예산	=2a+2b +3		**0.840**	**0.340**	**0.340**	**0.340**	**0.340**		**2.200**

69 예산 가용성을 나타내고 그에 좌우됨.
70 공식 예산 명명법에 따름.
71 EU 프로그램 및 조치의 시행(전 'BA' 라인), 간접 연구, 직접 연구를 지원하는 기술·행정 지원 및 지출.

• TOTAL operational appropriations	Commitments	(4)		1.000						**1.000**
	Payments	(5)		0.600	0.100	0.100	0.100	0.100		**1.000**
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)		**0.240**	**0.240**	**0.240**	**0.240**	**0.240**		**1.200**
TOTAL appropriations under HEADING 1 of the multiannual financial framework	Commitments	=4+ 6		1.240	0.240	0.240	.0.240	0.240		**2.200**
	Payments	=5+ 6		0.840	0.340	0.340	0.340	0.340		**2.200**

If more than one heading is affected by the proposal / initiative, repeat the section above:

• TOTAL operational appropriations (all operational headings)	Commitments	(4)								
	Payments	(5)								
• TOTAL appropriations of an administrative nature financed from the envelope for specific programmes (all operational headings)		(6)								
TOTAL appropriations under HEADINGS 1 to 6 of the multiannual financial framework (Reference amount)	Commitments	=4+ 6								
	Payments	=5+ 6								

• 총 운영 예산	사업 예산	(4)		1.000						**1.000**
	지출 예산	(5)		0.600	0.100	0.100	0.100	0.100		**1.000**
• 특정 프로그램의 엔벨로프에서 재정 지원을 받는 행정적 성격의 총 예산		(6)		**0.240**	**0.240**	**0.240**	**0.240**	**0.240**		**1.200**
다년간 재무 프레임워크의 **항목 1에 따른 총 예산**	사업 예산	=4+ 6		1.240	0.240	0.240	.0.240	0.240		**2.200**
	지출 예산	=5+ 6		0.840	0.340	0.340	0.340	0.340		**2.200**

2개 이상의 항목이 제안/이니셔티브의 영향을 받는 경우 위 섹션 반복:

• 총 운영 예산(모든 운영 항목)	사업 예산	(4)								
	지출 예산	(5)								
• 특정 프로그램의 엔벨로프에서 재정 지원을 받는 행정적 성격의 총 예산(모든 운영 항목)		(6)								
다년간 재무 프레임워크의 **항목 1~6에 따른 총 예산** (참조 금액)	사업 예산	=4+ 6								
	지출 예산	=5+ 6								

Heading of multiannual financial framework	7	'Administrative expenditure'

This section should be filled in using the 'budget data of an administrative nature' to be firstly introduced in the Annex to the Legislative Financial Statement (Annex V to the internal rules), which is uploaded to DECIDE for interservice consultation purposes.

EUR million (to three decimal places)

		Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**After 2027**[72]	**TOTAL**
DG: CNECT								
• Human resources		0.760	0.760	0.760	0.760	0.760	0.760	**3.800**
• Other administrative expenditure		**0.010**	**0.010**	**0.010**	**0.010**	**0.010**	**0.010**	**0.050**
TOTAL DG CNECT	**Appropriations**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**3.850**
European Data Protection Supervisor								
• Human resources		0.760	0.760	0.760	0.760	0.760	0.760	**3.800**
• Other administrative expenditure								
TOTAL EDPS	**Appropriations**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**3.800**
TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	1.530	1.530	1.530	1.530	1.530	1.530	**7.650**

EUR million (to three decimal places)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**		**TOTAL**
TOTAL appropriations	Commitments		2.770	1.770	1.770	1.770	1.770		**9.850**

[72] All figures in this column are indicative and subject to the continuation of the programmes and availability ofappropriations

다년간 재무 프레임워크의 항목	7	'행정 지출'

이 섹션은 서비스간 협의의 목적으로 DECIDE에 업로드되는 입법 재정 설명서의 부속서(내규의 부속서 V)에 처음 첫번째로 소개되는 '행정적 성격의 예산 데이터'를 사용하여 기재해야 한다.

100만 EUR(소수점 이하 세 자리)

		2023년	2024년	2025년	2026년	2027년	2027년 이후[72]	합계
DG: CNECT								
• 인적 자원		0.760	0.760	0.760	0.760	0.760	0.760	**3.800**
• 기타 행정 지출		**0.010**	**0.010**	**0.010**	**0.010**	**0.010**	**0.010**	**0.050**
총 DG CNECT	**예산**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**3.850**
유럽 데이터 보호 감독관								
• 인적 자원		0.760	0.760	0.760	0.760	0.760	0.760	**3.800**
• 기타 행정 지출								
총 EDPS	**예산**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**3.800**
다년간 재무 프레임워크의 **항목 7에 따른 총 예산**	(총 사업 예산 = 총 지출 예산)	1.530	1.530	1.530	1.530	1.530	1.530	**7.650**

100만 EUR(소수점 이하 세 자리)

		2022년	2023년	2024년	2025년	2026년	2027년		합계
총 예산	사업 예산		2.770	1.770	1.770	1.770	1.770		**9.850**

[72] 이 칼럼의 모든 수치는 프로그램의 지속과 예산의 가용성을 나타내며 그에 좌우된다.

under HEADINGS 1 to 7 of the multiannual financial framework	Payments		2.370	1.870	1.870	1.870	1.870	**9.850**

다년간 재무 프레임워크의 **항목 7 에 따른 총 예산**	지출 예산		2.370	1.870	1.870	1.870	1.870	**9.850**

3.2.2. Estimated output funded with operational appropriations

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2022**		Year **2023**		Year **2024**		Year **2025**		Year **2026**		Year **2027**		After **2027**[73]		**TOTAL**	
	OUTPUTS																	
	Type	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Tota l No	Total cost
SPECIFIC OBJECTIVE No 1[74]…																		
Database					1	1.000	1		1		1		1		1	0.100	1	1.000
Meetings- Output					10	0.200	10	0.200	10	0.200	10	0.200	10	0.200	10	0.200	50	1.000
Communication activities					2	0.040	2	0.040	2	0.040	2	0.040	2	0.040	2	0.040	10	0.040
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS					13	0.240	13	0.240	13	0.240	13	0.240	13	0.240	13	0.100	65	2.200

[73] All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations

[74] As described in point 1.4.2. 'Specific objective(s)…'

3.2.2. 운영 예산을 통해 자금이 제공된 산출물(output) 추정

사업 예산 100만 EUR(소수점 이하 세 자리)

목표 및 산출물 표시			**2022년**		**2023년**		**2024년**		**2025년**		**2026년**		**2027년**		**2027년 이후**[73]		**합계**	
	산출물																	
	유형	평균 비용	은	비용	은	비용	은	비용	은	비용	은	비용	은	비용	은	비용	총 No	총 비용
구체적 목표 No 1[74]…																		
데이터베이스					1	1.000	1		1		1		1		1	0.100	1	1.000
회의 – 산출물					10	0.200	10	0.200	10	0.200	10	0.200	10	0.200	10	0.200	50	1.000
의사소통 활동					2	0.040	2	0.040	2	0.040	2	0.040	2	0.040	2	0.040	10	0.040
구체적 목표 No 1의 소계																		
구체적 목표 No 2 ...																		
- 산출물																		
구체적 목표 No 2의 소계																		
합계					13	0.240	13	0.240	13	0.240	13	0.240	13	0.240	13	0.100	65	2.200

[73] 이 칼럼의 모든 수치는 프로그램의 지속과 예산의 가용성을 나타내며 그에 좌우된다.

[74] 제1.4.2항에 기술된 '구체적 목표…'

3.2.3. *Summary of estimated impact on administrative appropriations*

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– X The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**Yearly after 2027**[75]	**TOTAL**
HEADING 7 of the multiannual financial framework								
Human resources		1.520	1.520	1.520	1.520	1.520	**1.520**	**7.600**
Other administrative expenditure		0.010	0.010	0.010	0.010	0.010	**0.010**	**0.050**
Subtotal HEADING 7 of the multiannual financial framework		1.530	1.530	1.530	1.530	1.530	**1.530**	**7.650**
Outside HEADING 7[76] **of the multiannual financial framework**								
Human resources								
Other expenditure of an administrative nature		0.240	0.240	0.240	0.240	0.240	**0.240**	**1.20**
Subtotal outside HEADING 7 of the multiannual financial framework		0.240	0.240	0.240	0.240	0.240	**0.240**	**1.20**
TOTAL		**1.770**	**1.770**	**1.770**	**1.770**	**1.770**	**1.770**	**8.850**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

75 All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations.

76 Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

3.2.3. 행정 예산에 미치는 영향의 요약

1. 제안/이니셔티브는 행정적 성격의 예산의 사용을 요구하지 않는다.

2. X 제안/이니셔티브는 행정적 성격의 예산의 사용을 요구한다(아래에 설명).

100만 EUR(소수점 이하 세 자리)

	2022년	2023년	2024년	2025년	2026년	2027년	2027년 이후 매년[75]	합계
다년간 재무 프레임워크의 항목 7								
인적 자원		1.520	1.520	1.520	1.520	.520	**1.520**	**7.600**
기타 행정 지출		.010	0.010	0.010	0.010	0.010	**0.010**	**0.050**
다년간 재무 프레임워크의 항목 7 소계		1.530	1.530	1.530	1.530	1.530	**1.530**	**7.650**

다년간 재무 프레임워크의 항목 7 외[76]								
인적 자원								
행정적 성격의 기타 지출		0.240	0.240	0.240	.240	0.240	**0.240**	**1.20**
다년간 재무 프레임워크 항목 7 외 소계		0.240	0.240	0.240	0.240	0.240	**0.240**	**1.20**

합계		**1.770**	**1.770**	**1.770**	**1.770**	**1.770**	**1.770**	**8.850**

인적 자원 및 행정적 성격의 기타 지출에 소요되는 예산은 조치의 관리에 이미 할당되거나 DG 내에 재배치된 DG의 예산을 통해, 그리고 필요할 경우 연간 할당 절차에 따라 예산상의 제약을 고려하여, 관리하는 DG에 수여될 수 있는 추가 할당과 함께 충족된다.

75 이 칼럼의 모든 수치는 프로그램의 지속과 예산의 가용성을 나타내며 그에 좌우된다.

76 EU 프로그램 및 조치의 시행(전 'BA' 라인), 간접 연구, 직접 연구를 지원하는 기술·행정 지원 및 지출.

3.2.3.1. Estimated requirements of human resources

– ☐ The proposal/initiative does not require the use of human resources.

– X The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

.		Year **2023**	Year **2024**	Year **2025**	**2026**	**2027**	**After 2027**[77]	
• Establishment plan posts (officials and temporary staff)								
20 01 02 01 (Headquarters and Commission's Representation Offices)		10	10	10	10	10	10	
20 01 02 03 (Delegations)								
01 01 01 01 (Indirect research)								
01 01 01 11 (Direct research)								
Other budget lines (specify)								
• External staff (in Full Time Equivalent unit: FTE)[78]								
20 02 01 (AC, END, INT from the 'global envelope')								
20 02 03 (AC, AL, END, INT and JPD in the delegations)								
XX 01 xx **yy zz**[79]	- at Headquarters							
	- in Delegations							
01 01 01 02 (AC, END, INT - Indirect research)								
01 01 01 12 (AC, END, INT - Direct research)								
Other budget lines (specify)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

EDPS is expected to provide half of the resources required.

Description of tasks to be carried out:

Officials and temporary staff	To prepare a total of 13-16 meetings, draft reports, continue policy work, e.g. regarding future amendments of the list of high-risk AI applications, and maintain relations with Member States' authorities will require four AD FTE and 1 AST FTE. For AI systems developed by the EU institutions, the European Data Protection Supervisor is responsible. Based on past experience, it can be estimated that 5 AD FTE are reuqired to fulfill the EDPS responsibilites under the draft legislation.

[77] All figures in this column are indicative and subject to the continuation of the programmes and availability of appropriations.

[78] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

[79] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

3.2.3.1. 인적 자원의 요구사항 추정

– 제안/이니셔티브는 인적 자원의 사용을 요구하지 않는다.

– X 제안/이니셔티브는 인적 자원의 사용을 요구한다(아래에 설명).

FTE(Full Time Equivalent) 단위로 표시

.		2023년	2024년	2025년	2026년	2027년	2027년 이후[77]	
• 설립 계획 직위(임원 및 임시 직원)								
20 01 02 01 (본부 및 유럽연합 집행위원회의 대표 사무소)		10	10	10	10	10	10	
20 01 02 03 (대표부)								
01 01 01 01 (간접 연구)								
01 01 01 11 (직접 연구)								
기타 예산선(명시)								
• 외부 직원(FTE 단위로 표시)[78]								
20 02 01 ('글로벌 엔벨로프'의 AC, END, INT)								
20 02 03 (대표부의 AC, AL, END, INT, JPD)								
XX 01 xx **yy zz**[79]	- 본부							
	- 대표부							
01 01 01 02 (AC, END, INT – 간접 연구)								
01 01 01 12 (AC, END, INT – 직접 연구)								
기타 예산선(명시)								
합계		**10**	**10**	**10**	**10**	**10**	**10**	

XX는 관련 정책 분야 또는 예산 항목이다.

필요한 인적 자원은 조치의 관리에 이미 할당되거나 DG 내에 재배치된 DG의 직원을 통해, 그리고 필요할 경우 연간 할당 절차에 따라 예산상의 제약을 고려하여, 관리하는 DG에 수여될 수 있는 추가 할당과 함께 충족된다.

EDPS는 필요한 자원의 절반을 제공할 것으로 예상된다.

수행해야 할 과업의 설명:

임원 및 임시 직원	총 13-16개의 회의를 준비하고, 보고서 초안을 작성하고, 예컨대 고위험 AI 애플리케이션의 목록의 향후 개정과 관련한 정책 작업을 계속하고, 회원국 당국들과 관계를 유지하기 위해서는 4인의 AD FTE와 1인의 AST FTE가 필요할 것이다. EU 기관이 개발한 AI 시스템에 대해서는 유럽 데이터 보호 감독관이 책임을 진다. 과거의 경험에 비추어, 법안에 따른 EDPS 책임을 이행하려면 5인의 AD FTE가 필요할 것으로 추정된다.

77 이 칼럼의 모든 수치는 프로그램의 지속과 예산의 가용성을 나타내며 그에 좌우된다.

78 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations.

79 운영 예산(전 'BA' 라인)이 적용되는 외부 직원에 대한 하위 한계.

External staff	

외부 직원	

3.2.4. Compatibility with the current multiannual financial framework

The proposal/initiative:

– X can be fully financed through redeployment within the relevant heading of the Multiannual Financial Framework (MFF).

No reporgramming is needed.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation.

Explain what is required, specifying the headings and budget lines concerned, the corresponding amounts, and the instruments proposed to be used.

– ☐ requires a revision of the MFF.

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts.

3.2.5. Third-party contributions

The proposal/initiative:

– X does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **N**[80]	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[80] Year N is the year in which implementation of the proposal/initiative starts. Please replace "N" by the expected first year of implementation (for instance: 2021). The same for the following years.

3.2.4. 현행 다년간 재무 프레임워크와의 양립성

제안/이니셔티브:

– X 다년간 재무 프레임워크(MFF)의 관련 항목 내에서 재배치를 통해 충분한 재정 지원을 받을 수 있다.

재프로그래밍 불필요.

– MFF의 관련 항목 아래의 할당되지 않은 마진 사용 및/또는 MFF 규정에 정의된 특별한 수단의 사용이 필요하다.

무엇이 필요한지 설명하고, 관련 항목 및 예산선, 해당 금액, 제안된 수단 등을 명시.

– MFF의 개정이 필요하다.

무엇이 필요한지 설명하고, 관련 항목 및 예산선과 해당 금액을 명시.

3.2.5. 제3자 기여

제안/이니셔티브:

– X 제3자의 공동 재정 지원을 규정하지 않는다.

– 아래에 추정된 제3자의 공동 재정 지원을 규정한다.

예산 100만 EUR(소수점 이하 세 자리)

	N년[80]	**N+1년**	**N+2년**	**N+3년**	영향 지속 기간에 해당하는 연도 모두 입력(제1.6항 참조)			합계
공동 재정 지원 단체 명시								
공동 재정 지원을 받은 총 예산								

[80] N년은 제안/이니셔티브의 실행이 개시되는 연도이다. "N"을 실행 첫해(예: 2021)로 대체할 것. 이어지는 연도에 대해서도 동일.

3.3. Estimated impact on revenue

– ☐ The proposal/initiative has the following financial impact:

– ☐ The proposal/initiative has the following financial impact:

– ☐ on other revenue

– ☐ on other revenue

– Please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[81]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[81] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

3.3. 수익에 미치는 영향 추정

– ☐ 제안/이니셔티브는 다음과 같은 재정적 영향을 미친다:

– ☐ 제안/이니셔티브는 다음과 같은 재정적 영향을 미친다:

– ☐ 다른 수익에 대해

– ☐ 다른 수익에 대해

– 수익이 지출선에 할당된 경우 명시 ☐

100만 EUR(소수점 이하 세 자리)

예산 수익선:	현 회계 연도에 가용한 예산	제안/이니셔티브의 영향[81]						
		N년	**N+1년**	**N+2년**	**N+3년**	영향 지속 기간에 해당하는 연도 모두 입력(제1.6항 참조)		
조 …….								

할당된 수익에 대해 영향을 받는 예산 지출선 명시.

기타 비고(예: 수익에 미치는 영향을 계산하는 데 사용된 방법/공식 또는 기타 정보).

[81] 전통적 자체 재원(관세, 설탕 부담금 등)의 경우, 표시되는 금액은 반드시 순액, 즉 수금비로 20%를 공제한 후의 총액이어야 한다.