

개인정보보호 통합법 제정의 필요성과 주요내용

법무법인 민후 김경환 변호사

목 차

- 통합법의 "철학"
- 철학1 : 분산에서 통합으로
- 철학2 : 차별에서 형평으로
- 철학3 : 경직에서 유연으로
- 철학4 : 엄격에서 엄격으로
- 통합법의 "구조"

- 통합법의 주요내용1 : 정의
- 통합법의 주요내용2 : 국가 등의 책무
- 통합법의 주요내용3 : 개인정보의 동의 없는 수집
- 통합법의 주요내용4 : 개인정보의 제공 동의
- 통합법의 주요내용5 : 개인정보의 국외 제공
- 통합법의 주요내용6 : 특례 조항
- 통합법의 주요내용7 : 개인정보의 목적외 이용 · 제공
- 통합법의 주요내용8 : 공공기관의 개인정보 제공
- 통합법의 주요내용9 : 동의의 철회
- 통합법의 주요내용10 : 개인정보의 비식별화

- 통합법의 주요내용11 : 개인정보의 파기
- 통합법의 주요내용12 : 개인영상정보의 증거사용
- 통합법의 주요내용13 : 바이오인식정보
- 통합법의 주요내용14 : 안전성 확보를 위한 보호조치
- 통합법의 주요내용15 : 업무처리기록
- 통합법의 주요내용16 : 개인정보취급자에 대한 조치
- 통합법의 주요내용17 : 징벌적 손해배상
- 통합법의 주요내용18 : 특별위원회와 전문위원회
- 통합법의 주요내용19 : 입법영향분석 보고서
- 통합법의 주요내용20 : 과징금

통합법의 "철학"

- **통합** : 분산(공급자 중심)되어 있는 개인정보 보호 법령을 하나로 통합
(수요자 중심)
 - **형평** : 사업자별로 차별적인 규율을 동일한 수준으로 맞춤
 - **유연** : 경직적인 태도를 지양하여 개인정보 활용의 길을 터 줌
 - **엄격** : 일정한 보호 수준을 맞추어 개인정보를 보호하는 한편 자기결정
권을 보장함
- 개인정보보호법, 정보통신망법, 위치정보법, 신용정보법, 전자금융거래법,
교육기본법, 의료법 등 ⇒ 개인정보보호 통합법(안)

철학1 : 분산에서 통합으로

○ 분산되어 있고 중첩적이고 제각각인 개인정보보호 법령들

주무기관	사업자	개인정보	법률
금융위원회	신용정보업자 금융회사	신용정보 금융거래정보	신용정보보호법 전자금융거래법
보건복지부	의료기관	의료정보	의료법
교육부	교육기관	교육정보	교육기본법
방송통신위원회	정보통신사업자 위치정보사업자	온라인정보 위치정보	정보통신망법 위치정보보호법
안전행정부	공공기관 오프라인사업자 CCTV 설치자	일반 개인정보 개인영상정보	개인정보보호법 (일반법)

- 법령 공급자 중심으로 된 법령체계
- 사업자에 대한 중복적 규제 (예 : 금융회사는 관리하는 개인정보에 관하여 신용 정보법, 전자금융거래법, 정보통신망법, 개인정보보호법의 4개의 법령을 준수하여야 함)
- 막대한 규제 비용
- 법령 파악이나 해석의 어려움으로 인한 법집행의 어려움 (예 : 개인정보 보호법에는 개인정보 위탁시 문서로써 위탁을 하도록 하지만 정보통신망법은 이러한 규정이 없는바, 온라인 기업은 문서로써 위탁을 해야 하는가?)
- 어렵고 제각각인 법령으로 인한 낮은 준법성 (예 : 개인정보 위탁시, 정보통신망법은 위탁사실에 대하여 정보주체의 동의를 얻게 하고 있지만, 개인정보보호법에 따르면 정보주체에게 공개만 하면 됨)
- 권리구제의 어려움

○ 하나의 개인정보보호 통합법

- 법령 수요자인 사업자나 정보주체 중심으로 된 법령체계
- 중복 규제의 해소
- 규제 비용의 감소
- 용이한 법해석이나 통일적인 법집행
- 준법의 용이성
- 손쉬운 권리구제

철학2 : 차별에서 형평으로

○ 제각각이고 비합리적으로 차별적이고 비형평적인 법령들

- 동일한 사안 : 동일한 개인정보 유출 사고에 대하여 정보통신망법이 적용되는 정보통신서비스제공자는 과징금 제재를 받는 반면, 금융회사는 1천만원 이하의 과태료에 처해짐
- 상이한 사안 : 실제로, 실수로 카페탈퇴자에 대하여 이메일을 발송한 카페장에게는 700만원의 과태료 처분이 나온 반면, 수백만 명의 개인정보를 유출한 금융기관에게는 600만원의 과태료 처분이 부과됨
- 불법수집시 금융회사에게는 과태료 부과, 온라인기업은 형사처벌됨
- 개정안 : 온라인기업은 법정손해배상제도, 금융회사는 징벌적손해배상

○ 통일되고 형평적인 규제나 책임을 부과하는 통합법

- 동일한 사안에 대하여 동질의 규제 부과
- 동일한 사안에 대하여 사업자별로 동일한 책임 부과
- 상이한 사안에 대하여 형평적인 규제나 책임 부과
- 정보주체는 사업자에 무관하게, 동일한 책임을 물을 수 있고 동일한 규제방법을 모색할 수 있음

철학3 : 경직에서 유연으로

○ 경직되고 활용 가능성을 극소화한 법령들

- 보호에만 치중하고 활용가능성을 고려하지 않은 경직함
- 예컨대 개인정보 국외제공을 위해서는 반드시 정보주체의 동의를 받아야 함
- 예컨대 반드시 개인정보를 제공하는 자만 정보주체의 동의를 받아야 함
- 예컨대 공공기관만 개인정보보호위원회의 심의·의결을 통하여 개인정보의 목적외 제공을 할 수 있음
- 예컨대 CCTV 영상정보를 파기 기한 때문에 증거로 활용하기 어려움

○ 유연하고 활용가능성을 높인 통합법

- ‘하나의 고개’ 대신에 ‘동일한 높이의 여러 개의 고개’를 만들어 줌
(고개의 높이가 보호 측면이라면, 고개의 수가 활용 측면임)
- 예컨대 개인정보 국외 제공시 정보주체의 동의 대신에 개보위의 심의
· 의결을 통하여 같은 목적을 달성할 수 있음
- 예컨대 개인정보 제공시 제공하는 자뿐만 아니라 제공받는 자도 정보
주체의 동의를 받아서 제공 목적을 달성할 수 있음
- 예컨대 사기업도 개보위의 심의·의결을 거쳐 목적외 이용·제공을
할 수 있음

철학4 : 엄격에서 엄격으로

- 유연성을 보충할 뿐, 엄격성은 그대로 유지하고 개인정보 자기결정권 보장
 - 통합법은 활용과 보호의 2마리 토끼를 모두 잡음
 - 예컨대 재위탁시 위탁자의 동의를 받게 함
 - 예컨대 임의적인 동의 철회 규정을 신설함
 - 예컨대 보유 개인정보 중 3/4 이상 유출시 피해자의 징벌적 손해배상 청구가 가능함
 - 예컨대 개인정보처리 등을 기록한 업무처리기록의 보존의무를 신설함

통합법의 "구조"

- 전체 체계 : 9장 100조
- 제1장 총칙 (1조 ~ 6조)
 - 목적, 정의, 개인정보 보호 원칙, 정보주체의 권리, 국가 등의 책무, 다른 법률과의 관계
- 제2장 개인정보 보호정책의 수립 (7조 ~ 12조)
 - 기본계획, 시행계획, 자료제출 요구 등, 개인정보 보호지침, 자율규제의 촉진 및 지원, 국제협력

○ 제3장 개인정보의 처리 (8조 ~ 44조)

- 제1절 개인정보의 수집 · 이용과 제공
- 제2절 개인정보의 목적 외 이용과 제공
- 제3절 개인정보의 위탁 등
- 제4절 정보주체의 동의
- 제5절 개인정보의 처리 제한
- 제6절 개인정보의 비식별화와 파기
- 제7절 개인영상정보와 바이오인식정보

○ **제4장 개인정보의 안전한 관리** (45조 ~ 54조)

- 안전성 확보를 위한 보호조치, 업무처리기록, 개인정보 처리방침, 개인정보 보호책임자, 개인정보취급자에 대한 조치, 공공기관의 개인정보파일, 공공기관의 개인정보 영향평가, 개인정보보호 관리체계의 인증, 개인정보 유출 통지 및 신고

○ **제5장 정보주체의 권리 보장** (55조 ~ 62조)

- 개인정보의 열람·제공, 개인정보의 정정·삭제, 개인정보의 처리정지, 권리행사의 방법 및 절차, 개인정보 이용내역의 통지

- 제6장 정보주체의 권리 구제 (63조 ~ 72조)
 - 제1절 단체소송
 - 제2절 손해배상소송
- 제7장 보호위원회와 분쟁조정 (73조 ~ 86조)
 - 제1절 개인정보 보호위원회
 - 제2절 개인정보 분쟁조정
- 제8장 보칙 (87조 ~ 97조)
- 제9장 벌칙 (98조 ~ 100조)

통합법의 주요내용1 : 정의

○ 개인정보 (제2조 제1항)

- 개보법의 정의 개념 그대로 사용
- 개인위치정보, 개인신용정보, 개인금융거래정보, 개인보건의료정보, 학생교육정보, 바이오인식정보를 포함하면서 각 개념정의함

○ 개인정보처리자 (제2조 제5호)

- 업무 목적으로 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 자
- 영상정보처리기기운영자, 온라인사업자, 위치정보사업자등, 신용정보회사 등, 금융회사등, 보건의료기관, 학교를 포함함

- **소관 분야 행정기관 (제2조 제8호)** : 공동 소관 법률, 기존 주무기관들의 전문성을 그대로 활용, 조직의 통합이나 변경이 아닌 법령의 통합임
 - 가. 방송통신위원회(정보통신서비스제공자 · 온라인사업자 · 위치정보사업자등)
 - 나. 금융위원회(신용정보회사등 · 금융회사등)
 - 다. 보건복지부(보건의료기관)
 - 라. 교육부(학교)
 - 마. 안전행정부(가목부터 라목까지 열거되지 않은 공공기관 및 개인정보처리자)

통합법의 주요내용2 : 국가 등의 책무

- 제5조 제3항 : 국가와 지방자치단체는 개인정보보호 또는 사생활보호 산업을 육성하여야 하며, 개인정보를 처리하는 체계를 설계할 때부터 개인정보 보호 또는 사생활보호가 도모될 수 있는 시책을 강구하여야 한다.
 - 프라이버시 산업 육성 (IT에 의한 침해는 IT로 방어)
 - Privacy by Design 개념 도입

통합법의 주요내용3 : 개인정보의 동의 없는 수집

- 제13조 제1항 제5호 : 정보주체의 서비스이용내역 · 접속기록 · 결제기록 · 통화내역 등과 같이 서비스 제공 과정에서 자동적으로 생성되고 해당 정보주체에 대한 서비스 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 현저히 곤란한 경우
 - － 정보통신망법 제22조 제2항 제1호가 근거
 - － 다만 통신자료 등에 해당하므로 원칙적으로 제공을 금지시킴

○ 제13조 제1항 제8호 : 정보주체 또는 정당한 권한이 있는 자에 의하여 모든 사람에게 목적의 제한 없이 공개된 경우. 다만 개인정보의 처리로 인하여 얻는 당해 정보주체 또는 공공의 이익이 현저히 큰 경우에 한한다.

- 오픈 데이터 수집에 대한 규정 신설
- 남용 방지를 위하여, 당해 정보주체 또는 공공의 이익이 현저히 큰 경우에 한함
- 예컨대 특정인에 대한 마케팅 목적이나 특정인의 정치성향 분석으로는 이용 불가
- 예컨대 공공기관이 고위 공무원의 임명을 준비하면서 공개된 SNS 정보를 수집하는 경우에는 가능

통합법의 주요내용4 : 개인정보의 제공 동의

○ 제16조 제3항 : 개인정보를 제공받는 자는 다음 각 호의 사항을 모두 갖춘 경우에 한하여 개인정보를 제공하는 자를 대신하여 정보주체로부터 동의를 받을 수 있고, 이 경우 제2항이 준용된다.

- 개인정보를 제공받는 자의 동의를 명문화
- 기존에 제공 동의를 받지 못한 데이터의 활용 길을 더 좁
- 남용 가능성 방지를 위해, 1. 법령에 의하여 개인정보의 제공이 금지되지 않을 것, 2. 정보주체의 이익 또는 편의를 위하여 필요한 경우일 것, 3. 동의를 받기 전에 개인정보를 제공하는 자와 개인정보를 제공받는 자 사이에 문서로 된 개인정보 제공에 관한 계약이 있을 것의 요건을 갖추도록 함

통합법의 주요내용5 : 개인정보의 국외 제공

- 제17조 제2항 : 개인정보처리자는 다음 각 호의 하나에 해당하는 경우 개인정보를 국외에 제공할 수 있다. (정보주체의 동의를 받은 경우, 서비스 제공 또는 계약의 이행을 위하여 필수적이고 정보주체의 동의를 받기 곤란한 경우로서 보호위원회의 심의·의결을 거친 경우)
 - 이미 수집을 마쳤으나 제공동의를 받지 못한 데이터의 활용 가능
 - 보호위원회의 재량을 높이면서, 유연한 법률 달성에 기여함

통합법의 주요내용6 : 특례 조항

○ 제16조(개인정보의 제공)

제17조(개인정보의 국외 제공)

제18조(개인정보를 제공받은 자의 이용·제공 제한)

제19조(개인위치정보의 제공 특례)

제20조(개인신용정보의 제공 특례)

- 일반 조항 뒤에 특례 조항을 부가하여 가독성을 높임
- 각 내용마다 각각 특례조항을 부가하여 이해도를 높임

통합법의 주요내용7 : 개인정보의 목적외 이용·제공

- 제23조 제1항 제4호 : 개인정보를 목적 외 용도로 이용하거나 제3자에게 제공하지 아니하면 계약을 이행할 수 없거나 법령상 주어진 업무를 수행하기 곤란한 경우로서 보호위원회의 심의·의결을 거친 경우
 - － 공공기관에 한정된 것을 사기업까지 확장함
 - － 요건을 완화시켜 조문의 활용 가능성을 높임
 - － 보호위원회의 재량성을 높이고, 데이터의 활용성을 증대시킴
 - － 개인정보를 제공받는 자가 개인정보를 제공하는 자를 대신하여 보호위원회의 심의·의결을 거칠 수 있도록 함 (제5항)

통합법의 주요내용8 : 공공기관의 개인정보 제공

- 제23조 제6항 : 제1항제6호에 따라 개인정보를 제3자에게 제공한 공공기관은 개인정보를 제공받은 검찰, 경찰, 그 밖의 수사기관이 그 수사가 종료되거나 공소제기 또는 공소유지가 필요하지 않게 되었음을 통보한 경우, 지체 없이 제공한 개인정보의 주요 내용, 이용 목적, 제공받은 자, 제공일, 제공근거 등을 정보주체에게 통지하여야 한다.
 - － 무분별한 공공기관의 개인정보 제공을 방지하기 위함
 - － 매 반기별로 개인정보의 제공요청 및 제공에 관한 자료를 보호위원회를 거쳐 국회 안전행정위원회에 보고하도록 하여 국회의 감시를 강화함

통합법의 주요내용9 : 동의의 철회

- 제34조 제1항 : 정보주체는 개인정보처리자에 대하여 언제든지 개인정보 수집·이용, 제공 등의 동의의 전부 또는 일부를 서비스별·개인정보별·처리단계별 등으로 구분하여 철회할 수 있다.
 - － 동의를 받은 방법 규정 뒤에 바로 동의의 철회 규정은 신설함
 - － 동의 철회의 자유와 그 효과를 명확히 함

통합법의 주요내용 10 : 개인정보의 비식별화

- 제39조 제2항 : 개인정보처리자가 개인정보를 비식별화하여 처리할 때에는 대통령령으로 정하는 바에 따라 개인정보가 재생성되지 않도록 하여야 한다.
 - － 비식별화 조치에 대한 명문 근거를 둠
 - － 비식별화에 대한 재식별화 위험성 기준을 제시함
 - － 비식별화된 개인정보에 대하여 보호조치를 취하게 함으로써, 비식별 정보보다 한 단계 높은 보호를 함

통합법의 주요내용 11 : 개인정보의 파기

- 제40조 제2항 : 제1항에도 불구하고 다음 각 호의 경우에는 개인정보를 파기하지 아니할 수 있다. (1. 다른 법령에 따라 보존할 의무가 있는 경우, 2. 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우, 3. 정보주체의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되거나 공공의 이익을 위하여 보존할 필요성이 매우 큰 경우, 4. 파기 사유가 존재함에도 보존의 필요성이 매우 크다고 보호위원회가 심의·의결하는 경우)
 - － 무조건적인 파기가 아닌 유연성 있는 파기 제도를 구현함

통합법의 주요내용 12 : 개인영상정보의 증거사용

- 제43조 제2항 : 영상정보처리기기운영자는 영상정보처리기기에 의하여 촬영된 개인영상정보를 최소 20일까지 보관하여야 하며 30일 이내에 파기하여야 한다. 다만 정보주체가 영상정보처리기기운영자에게 개인영상정보가 증거로 사용될 수 있는 수사 또는 재판이 진행 중임을 소명하거나 촬영된 정보주체가 모두 개인영상정보의 파기를 원하지 않는 경우에는 당해 개인영상정보의 목적을 다할 때까지 보존하여야 한다.
 - － 무조건적인 파기를 막아, 증거로서의 기능을 살림
 - － 보관기간을 20일 이상으로 하여 단서 조항의 조치가 현실적으로 가능하게 함

통합법의 주요내용 13 : 바이오인식정보

- 제44조 제2항 : 대통령령으로 정하는 개인정보처리자는 추출정보 외에 별도로 원본정보를 보관하여서는 아니된다. 다만 제42조제1항 각 호의 목적을 수행하기 위하여 원본정보를 수집한 경우에는 그러하지 아니하다.
 - － 바이오인식정보를 개념 정의함 (가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함하되, 다만 추출 과정을 거치지 아니하여 특징정보가 존재하지 않는 원본정보는 제외한다)
 - － 수집 목적에 따라 원본정보 보관 금지 원칙을 규정함

통합법의 주요내용 14 : 안전성 확보를 위한 보호조치

○ 제45조 :

- 2. 개인정보 접근·취급 권한의 처리단계별·업무별·직급별 차등 부여
- 3. 개인정보취급자 및 접근가능한 자에 대한 교육·관리·감독·사후점검
- 8. 개인정보의 출력(전자출력 포함)에 관한 모니터링 및 제한 조치
 - － 관리적 조치를 강화함
 - － 개인정보 출력시 모니터링을 강화함

통합법의 주요내용 15 : 업무처리기록

- 제46조 제1항 : 대통령령으로 정하는 개인정보처리자는 아래의 업무처리내용(개인정보는 제외한다)이 포함된 기록을 작성하여 처리 목적을 달성한 날로부터 3년간 보존하여야 한다.
 - － 개인정보의 처리를 의뢰한 자, 처리한 날짜, 처리 결과 등에 대한 기록을 보존하도록 함
 - － 사업자 부담을 줄이고자 일정 규모의 개인정보처리자가 적용함
 - － 신용정보법, 위치정보법에 관련 개념 규정이 존재함

통합법의 주요내용 16 : 개인정보취급자에 대한 조치

- 제50조 : ① 개인정보처리자는 개인정보취급자를 최소한으로 제한하여야 한다. ② 개인정보처리자는 개인정보취급자끼리 계정을 공유하게 하여서는 아니 된다.
 - 대부분의 보안사고가 개인정보취급자 관리 소홀로 발생하였음
 - 최소한 제한과 계정 공유 금지 규정

통합법의 주요내용 17 : 징벌적 손해배상

○ 제71조 제1항 : 정보주체는 개인정보처리자가 고의 또는 중대한 과실로 이 법 또는 상당한 보호조치 의무를 위반하여 보유하고 있는 전체 개인정보 중 4분의 3 이상(정보주체의 수를 기준으로 판단한다)이 분실·도난·유출됨으로써 손해를 입으면 그 개인정보처리자에게 손해액의 3배 배상을 청구할 수 있다. 이 경우 개인정보처리자는 고의 또는 중대한 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

- 유출당한 규모를 기준으로 징벌적 손해배상 인정함
- 제1심에 한하여 원고의 추가를 인정함 (제4항)
- 변론전체의 취지 등을 고려한 손해액 인정 (제2항)

통합법의 주요내용 18 : 특별위원회와 전문위원회

○ 제74조 제1항 : 보호위원회는 그 업무를 통일적이며 독립적이고 효율적으로 수행하기 위하여 다음 각 호의 특별위원회와 전문위원회를 둔다.

1. 각 개인정보 소관 분야 업무에 대하여 협의하며 주요 정책이나 소관 분야 행정기관이 입안한 이 법 관련 법령을 심의·의결하기 위한 개인정보 법령정책 특별위원회(이하 "특별위원회"라 한다)

2. 개인정보에 관한 분쟁의 조정(調停)을 위한 개인정보 분쟁조정 전문위원회(이하 "전문위원회"라 한다)

- 공동소관에 따른 보호위원회의 중재·조정기능을 강화함 (특별위원회)
- 분쟁조정 기능을 보호위원회에 귀속시킴 (전문위원회)

통합법의 주요내용 19 : 입법영향분석 보고서

- 제77조 제1항 : 보호위원회의 위원장은 소관 분야 행정기관의 장과 협의하여 이 법의 시행에 따른 상황 및 그 영향을 2년마다 평가하여 그 결과와 법령의 개선에 따른 보고서를 작성하여 국회에 제출하여야 한다. 이 때 국회는 보고서 내용에 대하여 의견을 제시할 수 있다.
 - － 입법영향분석 보고서 제도를 최초로 도입함
 - － 법령 개선에 실증적으로 기여하고, 국회의 감시 기능을 강화함

통합법의 주요내용 20 : 과징금

- 제96조 제1항 : 소관 분야 행정기관의 장은 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 소관 개인정보처리자에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
(동의 없는 수집·이용·제공 / 목적외 이용·제공 / 위탁자의 관리·감독 해태 / 주민등록번호나 개인정보의 유출)
 - － 정보통신망법의 규정을 근거 삼아 과징금 규정을 제정함
 - － 유출사고 발생시 보호조치 위반과의 인과관계를 밝힐 필요 없이 과징금 부과 가능
 - － 관련 매출액의 3% (정보통신망법, 신용정보법 참조)

감사합니다.

oalmephaga@minwho.kr