Kdata 19-004	2019. 11.

MyData 서비스의 개인동의 방식 개선 연구

2019. 11.

수행기관 : 법무법인(유한) 광장

한국데이터산업진흥원
Korea Data Agency

제 출 문

한국데이터산업진흥원 원장 귀하

본 보고서를 “MyData 서비스의 개인동의 방식 개선 연구”에 관한 최종보고서로 제출합니다.

2019. 11.

수 행 기 관 : 법무법인(유한) 광장
총괄 책임자 : 고 환 경 (법무법인(유한) 광장 파트너 변호사)
참여 연구원 : 손 경 민 (법무법인(유한) 광장 파트너 변호사)
차 현 정 (법무법인(유한) 광장 변호사)
김 지 훈 (법무법인(유한) 광장 변호사)
지 용 환 (법무법인(유한) 광장 변호사)

요 약 문

■국내외 법제도 현황 및 문제점 분석

1. 외국 법제도 현황 분석

가. 유럽연합 일반 개인정보보호법(GDPR)

(1) 적법 처리 조건

유럽연합의 GDPR에서는 개인정보처리에 적용이 가능한 적법 처리 조건으로 정보주체의 동의를 포함한 6가지를 두고 있다. 이는 우리나라 개인정보보호법과 유사하나, 동의가 원칙인 점에서 우리나라와 차이가 있다.

특히, GDPR은 개인정보 수집 목적 외 처리가 개인정보를 수집한 목적과 양립하는 목적인 경우 별도의 동의 없이 추가적인 이용 및 제공을 허용한다는 점은 우리 법과 구별된다.

(2) 동의 제도

GDPR에서 동의는 “정보주체가 진술 또는 적극적 행동을 통하여 자신의 개인정보처리에 대한 긍정의 의사를 표현하는 것”을 의미하는데, 이를 위해서는 ① 자유롭게 부여된 동의, ② 개별적으로 특정한 동의, ③ 사전 정보가 제공된 동의, ④ 정보주체의 모호하지 않은 의사 표시가 요건이 충족되어야 한다.

(3) 고지 사항

정보주체는 ① 개인정보처리자의 기관명과 연락처, ② 개인정보보호책임자의 세부연락처, ③ 개인정보처리의 목적·근거, ④ 개인정보처리자의 정당한 이익, ⑤ 수령인 ⑥ 국외이전이 발생하는 경우 적합성 평가 등 국외이전의 근거를 통보받을 권리를 가진다. 정보주체 이외로부터 개인정보를 수집하는 경우에도 개인정보처리자는 위 정보를 제공하여야만 한다. 이때 고지사항인 수령인과 관련하여, 컨트롤러는 수령인의 전체 목록 또는 수령인의 유형을 고지할 의무가 있는 것으로 해석된다.

나. 독일 연방개인정보보호법(BDSG)

유럽연합의 GDPR이 제정됨에 따라 유럽연합 회원국에서는 2017년에 독일이 처음으로 GDPR을 반영하여 신속하게 연방개인정보보호법('BDSG')을 전면 개정했다. BDSG 동의의 요건은 사실상 GDPR과 유사하다.

다. 미국 캘리포니아주 소비자프라이버시법(CCPA)

캘리포니아주의 '캘리포니아주 소비자프라이버시법은 개인정보 처리에 정보주체의 동의를 요하기보다는 삭제 요구권과 판매 금지권을 통해 정보주체, 즉 소비자가 '옵트아웃'을 할 수 있는 방식으로 구성되어 있다. 다만, 13세 미만으로부터 수집한 개인정보를 판매하고자 하는 경우에는 부모나 후견인의, 13세 이상 16세 미만의 경우 본인의 옵트인 동의가 필요하다.

라. 일본 개인정보의 보호에 관한 법률

일본의 개인정보의 보호에 관한 법률(이하 '개인정보보호법')의 동의 제도를 보면, 허위 기타 부정한 수단에 의한 취득을 금지하고 있을 뿐이므로 수집 · 이용은 원칙적으로 허용된다는 해석이 가능하다. 개인정보 제3자 제공의 경우 정보주체의 사전 동의를 원칙으로 하고 있으나, 일정한 요건을 갖춘 경우 옵트아웃 방식의 제3자 제공이 가능하다는 점에서 우리 법과 다르다. 또한, 일본 개인정보보호법은 우리 법과는 달리 개인정보 제3자 제공 시 정보주체에게 고지해야 하는 사항에 대해 구체적으로 규정하고 있지 않고, 단지 "미리 본인의 동의를 받을 것"만을 요건으로 하고 있다. 대신, 2015년 개정으로 제3자 제공에 관한 기록 및 확인 의무가 도입되었다.

일본에서는 이러한 법제도를 바탕으로 개인과 데이터 활용에 관한 계약 등에 기반하여 PDS 등의 시스템을 활용하여 개인 데이터를 관리하고, 개인의 지시 또는 미리 지정한 조건에 따라 개인을 대신하여 타당성을 판단한 후, 데이터를 제3자(다른 사업자)에게 제공하는 사업인 '정보은행' 서비스가 제공되고 있는데, 이는 마이데이터 산업과 유사하면서도 일본의 특징이 반영된 것이라고 할 수 있다.

2. 국내 법제도 현황 분석

가. 국내 개인정보처리에 대한 동의 제도의 현황

개인정보처리자는 원칙적으로 정보주체의 동의가 있어야 개인정보를 처리할 수 있으며, 정보주체의 동의를 위해 정보주체에게 관련 내용을 충실히 알려야 하고, 정보주체의 동의는 사전에 명시적, 개별적으로 받아야 한다.

나. 동의 원칙

정보통신망법은 개인정보 처리에 관하여 정보주체의 동의를 받을 것을 원칙으로 하고 있으며 몇 가지 예외를 두고 있으나 그 사유는 엄격하게 해석된다. 또한, 개인정보 동의를 받지 않아도 되는 경우에 관하여 개인정보보호법과 정보통신망법의 규정이 통일되어 있지 않으며 각각의 법에서도 수집 · 이용과 제3자 제공 등 처리 유형에 따라 예외 사항이 다르다.

다. 법정고지사항

우리 법은 개인정보처리자로 하여금 정보주체로부터 동의 받을 때 고지 의무를 규정하고 있고, 고지하는 방법도 법령에 정해져 있다. 정보통신망법에는 위와 같은 내용이 구체적으로 규정되어 있지 않으나, 법정 고지사항은 쉽고 명확하게 이해가 될 수 있도록 기재되어야 하는 점은 동일하다. 한편, 개인정보 제3자 제공의 경우 '정보를 제공받는 자'에 대해 고지할 의무가 있는데, 이른바 '유형고지'는 허용되지 않는 것으로 해석된다.

라. 사전 · 명시 · 구분 동의

(1) 사전 동의

우리 법의 동의 제도가 사전 동의를 전제로 하고 있다는 점에는 이론이 없다. 개인정보보호법은 정보주체의 동의를 '받은' 경우 개인정보를 수집 · 이용 · 제공할 수 있다고 규정하고 있다.

(2) 명시적 동의

일반적으로 우리 법상 개인정보처리에 대한 동의는 묵시적 동의가 아닌 명시적 사전 동의를 요구하는 것으로 인식되고 있다. 실제로 개인정보보호법이나 정보통신망법 시행령에서 규정한 방식으로 볼 때 명시적 동의를 요구하는 것으로 해석된다.

(3) 구분 동의

우리 법의 동의 제도는 구분 동의를 원칙으로 하고 있다. 개인정보보호법은 개인정보의 처리에 대하여 동의를 받을 때에는 각각의 동의 사항을 구분하여 동의받을 것을 규정하고 있다. 정보통신망법 역시 마찬가지다. 또, 개인정보보호법은 고유식별정보를 처리할 때에는 '고유식별정보 처리에 대한 동의'를, 민감정보를 처리할 때에는 '민감정보 처리에 대한 동의'를 별도로 분리해서 목적 등을 고지하고 동의를 받아야 한다. 참고로 신용정보

법은 원칙적으로는 개인신용정보를 제공할 때마다 미리 개별 동의를 받아야 한다는 엄격한 입법태도를 취하고 있다.

마. 변경 동의

개인정보처리자는 정보주체의 동의를 받았을 때 정보주체에게 고지했던 법정고지사항이 변경되는 경우에는, 사소한 변경의 경우에도 다시 동의를 받아야 하므로 실무적으로 상당한 부담이 된다.

바. 필수적 · 선택적 동의 사항

또한 우리 법은 필수적 · 선택적 동의 사항을 구별하여, 개인정보보호법은 정보주체가 선택적 동의 사항에 동의를 하지 않는다는 이유로 개인정보처리자가 정보주체에게 재화 또는 서비스 제공을 거부할 수는 없다고 한다.

사. 정보통신망법의 개인정보 처리위탁 동의

개인정보보호법상 개인정보의 처리위탁은 정보주체의 동의를 요하지 않는다. 그러나 정보통신망법은 일정한 예외를 두고는 있으나, 원칙적으로 개인정보처리위탁의 경우에도 이용자, 즉 정보주체의 동의를 받도록 규정하고 있다.

사. 형사처벌

현행 법령상, 동의 제도를 위반하였을 경우 형사처벌도 가능하다. 개인정보보호법의 경우 정보주체의 동의 없이 개인정보를 제3자에게 제공한 경우는 형사처벌 대상이고 정보통신망법의 경우 정보주체의 동의 없이 개인정보를 수집 · 이용 · 제공 · 위탁한 경우 모두 형사처벌이 가능하다.

3. 국내법상 동의 제도의 문제

가. 정보 활용범위의 제한 관련

(1) 지나치게 엄격하고 복잡한 동의 제도

우리 법은 엄격한 원칙에 따라 동의를 받을 것을 요구하고 있다. 이는 비교법적으로도 매우 지나친 규제라는 비판이 있다. 특히 법률의 규정 뿐 아니라 실무상 해석과 법원의 판결도 매우 엄격하게 이루어지고 있다. 이에 더하여 정보보호에 관한 법률이 지나치게 다양하고 규정도 상이하여 수범자로 하여금 혼란스럽게 한다. GDPR과 달리 법정고지사

항 고지의무는 별도로 규정된 개인정보처리방침 공개의무와 구별되는, 정보주체의 동의 시 명시적으로 이루어져야 하는 의무사항이라는 점에서, 정보활용의 폭을 더욱 제한하고 있다.

(2) 변경 동의의 문제

우리 법에서는 개인정보처리에 대한 동의 시 고지한 법정고지사항이 변경되는 경우에도 다시 동의를 받도록 하고 있다. 이는 정보 활용의 범위를 지나치게 제한하는 것이므로 GDPR과 같이 당초 수집 목적과 양립하는 목적, 즉 합리적으로 관련된 범위 내인 경우에는 정보주체 동의 없이 추가 처리를 허용해야 한다는 비판이 제기된다.

(3) 형사처벌 중심의 제재

우리 법은 형사처벌까지 가능한, 강력한 제재 수단을 동원하고 있다. 정보주체의 권리를 강력하게 보호하고 있다는 평가를 받는 GDPR도 적법 처리 조건 없이 개인정보를 처리한 경우 형사처벌을 하고 있지 않다. 일본의 개인정보보호법 역시 마찬가지다.

(4) 정보통신서비스 분야의 강한 규제

마이데이터 산업을 비롯한 데이터산업 분야에서 동의 제도가 가장 크게 문제되는 부분은 바로 정보통신망법의 규제가 개인정보보호법보다 오히려 엄격하다는 점이다. 마이데이터 산업 등 데이터산업 분야에는 큰 장애로 기능하게 되며, 현실적으로도 맞지 않다는 비판이 제기될 수 있다. 게다가 정보통신 분야에서의 동의 제도는 오히려 오프라인에서의 동의 제도에 비해 비현실적인 측면이 있다.

나. 개인정보자기결정권 보호 관련

(1) 동의규제의 역설

우리 법이 보호하려고 했던 개인정보자기결정권을 현행 동의 제도가 오히려 제대로 보호하지 못하고 있다. 그 이유는 '동의규제의 역설(paradox)' 즉, 동의서가 길고 복잡해질수록 정보주체는 고지사항을 제대로 읽지 않아 정보를 제공하는지도 모른 채 개인정보를 제공하고 사업자들은 면죄부를 받기 때문이다. 역설적으로 강한 동의제도는 동의를 더욱 형식적으로 만들고, 정보주체의 소외를 키운다. 개인정보 처리 동의는 서비스 제공받기를 포기하지 않는 이상 정보처리에 동의하지 않을 수 없으므로 실질적으로 자유가 제약된 상태에서 행해진다. 이는 동의가 알고 하는, 자유로운 상태에서의 동의인지 실질적인 판단을 하지 않기 때문에 일어나는 현상이라고 할 수 있다.

(2) 동의 형식화의 현실

설문 조사 결과, 정보주체는 동의서를 제대로 읽지 않고 필수적 · 선택적 동의사항을 구별하지 않고 동의를 하고 있었으며 그 이유는 동의서가 지나치게 어렵고 복잡하고 길 뿐만 아니라, 어차피 동의를 하지 않으면 서비스를 받지 못한다는 점에 있었다.

5. 산업 분야별 마이데이터 관련 법제도 현황 분석

가. 통신분야

현행 정보통신망법 하에서는 이용자가 직접 자신의 개인정보를 정보통신서비스 제공자로부터 제공받아 마이데이터 사업자에게 해당 정보를 관리하고 제3자에게 제공하도록 하는 방식, 마이데이터 사업자가 이용자의 위임을 받아 그를 대행/대리하여 정보통신서비스 제공자로부터 개인정보를 제공받는 방식, 마이데이터 사업자가 (마이데이터 사업자에 대한) 제3자 제공 동의를 받아 서비스를 제공하는 방식이 가능할 것으로 보인다.

전기통신사업법이 규율하고 있는 번호이동성제란, 이용자가 자신이 가입한 통신서비스의 제공사업자를 변경하는 경우에도 이용자가 사용하던 기존의 전기통신번호를 유지할 수 있도록 해주는 제도인데, 이는 번호를 유지한 채로 사업자를 변경한다는 점에서, GDPR의 정보이동권과 유사한 면이 있다.

나. 금융분야

현행 신용정보법 하에서는 정보주체가 자신의 신용정보를 신용정보회사등으로부터 제공받아 마이데이터 사업자에게 해당 정보를 관리하고 제3자에게 제공하도록 하는 방식, 마이데이터 사업자가 정보주체로부터 위임을 받아 상기 권리를 대리하여 행사하는 방법, 마이데이터 사업자가 (마이데이터 사업자에 대한) 신용정보법에 따른 제3자 제공 동의를 받는 방식이 가능할 것으로 보인다.

다. 의료분야

의료정보에 대해서도 정보주체가 열람 청구권을 행사하고 이를 마이데이터 사업자에게 제공하는 방식, 마이데이터 사업자가 정보주체의 위임을 받아 대리/대행의 방식, 마이데이터 사업자가 (의료정보 제공자의 마이데이터 사업자에 대한) 개인정보보호법에 따른 제3자 제공 동의를 받는 방안을 고려할 수 있다.

참고로 최근 보건복지부는 2019. 10. 16. “진료기록 열람 및 사본발급 업무 지침”을 배포하였다. 위 지침은 의료법 제21조에 따른 진료기록 열람 및 사본 등의 제공 방식에 대하여,

“환자의 편의 및 의료기관 행정 효율 제고를 위해 각 의료기관 여건에 맞는 온라인 본인인증 시스템 구축 및 온라인 신청 접수 시행을 권고함”으로 안내하고 있다. 위 지침에 따라 향후 의료분야에서 마이데이터 서비스가 보다 활성화 될 수 있을지를 지켜볼 필요가 있을 것이다.

■ 국내외 마이데이터 사업자의 동의 방식

1. 국내 마이데이터 사업자

가. 토스

토스를 이용하기 위해서는 개인정보 수집이용과 개인정보 제3자 제공에 대해 동의하여야 하는데, 이에 대해 일괄동의 기능을 운영하고 있다. 이외에 서비스 이용에 필수적이지 않은 개인정보 처리(맞춤형 광고와 마케팅 정보 수신)에 대한 동의사항이 있다. 동의서 분량은 상당한 편으로, 핸드폰 화면을 통해 구체적 고지사항을 확인하는 것이 가능하다.

나. 뱅크샐러드

뱅크샐러드를 이용하기 위해서는 개인정보 수집 및 이용, 개인정보 제3자 제공에 필수적으로 동의하여야 하며, 뉴스레터 및 마케팅 정보 수신에는 선택적으로 동의할 수 있다. 구체적인 동의서의 내용을 보면 토스와 달리 “고객 신용정보 세부 내역”과 같이 개인정보의 유형을 기재하는 방법을 택했다.

2. 해외 마이데이터 사업자

가. Credit Karma

미국의 신용정보업 관련 마이데이터 서비스 제공자인 Credit Karma는 한국의 마이데이터 사업자와 같은 복잡한 동의절차를 두고 있지 않다. 서비스 제공을 위하여 필요한 정보를 입력하고 이용약관과 개인정보 처리방침에 동의한다는 상자를 체크하면 된다.

나. ClearScore

영국 마이데이터 사업자인 ClearScore 역시 개인정보 처리에 대한 개별적 동의서를 두고 있지 않고, “개인정보 및 쿠키 정책”에 동의하면 바로 서비스 사용을 시작할 수 있도록 하고 있다.

다. MINT

미국과 캐나다에서 사용 가능한 마이데이터 서비스인 MINT는 개인정보 처리를 위한 동의를 별도로 받지 않고, 계정을 생성하면 자동으로 이용약관과 개인정보 처리방침에 동의하는 것으로 간주된다.

■ 개선 방안

제1절 개인정보 보호 관련 법률 개정안 검토

1. 개인정보보호법 개정안(인재근 의원안)

가. 주요 내용

인재근 등 14인의 국회의원은 개인정보보호법 일부개정법률안(이하 '인재근 의원안')을 발의하였다. 본 개정안은 수집 목적과 양립하는 목적의 경우 추가 처리를 허용한 GDPR 조항과 유사한 취지의 규정을 신설하고자 한다. 그러나 정보통신서비스 제공자가 개인정보를 처리위탁할 때 원칙적으로 이용자의 동의를 받아야 한다는 규정을 그대로 두고, 개인정보 처리에 대하여 정보주체의 동의를 받는 방법을 개정하지 않는다.

나. 개정안에 대한 평가

우선, 마이데이터 서비스의 성공적 정착을 위해서는 개인정보 활용 범위를 합리적인 수준에서 최대한 넓힐 필요가 있으며, 인재근 의원안은 이를 달성하는데 도움이 될 것이다. 그러나 인재근 의원안은 개인정보 처리를 위한 동의를 받는 방법과 정보통신서비스 제공자가 개인정보 처리위탁할 때 정보주체의 동의를 받도록 한 규정을 그대로 두었다는 한계가 있다.

2. 정보통신망법 개정안(노웅래 의원안)

노웅래 등 10인의 국회의원이 발의한 정보통신망법 개정안의 목표는 개인정보보호와 관련된 정보통신망법 조항을 모두 개인정보보호법으로 옮겨 일원화하는 것에 있다.

2. 신용정보법 개정안(김병욱 의원안)

가. 주요 내용

김병욱 등 13인의 국회의원은 2018. 11. 15. 신용정보법 일부개정법률안(이하 '김병욱 의원안')을 발의하였다. 내용 중, 개인신용정보 활용 동의를 받을 때 중요사항을 우선적으로 고지할 수 있다는 취지의 조항과 동의 등급제가 개인정보 처리 동의 제도와 가장 연관성이 크다.

나. 개정안에 대한 평가

고지사항 중 일부를 생략하거나 중요한 사항만을 알리도록 하는 것은 동의규제의 역설을 해결할 수 있는 하나의 좋은 방안이 될 것이다. 특히, 정보제공의 단순화는 정보제공의 실질화를 유도하여 알고 하는 동의가 구현되는 것에 도움이 될 것이다. 사업자의 입장에서는 동의서 작성에 소요되는 시간과 비용을 절약할 수 있다. 정무위원회는 역시 마찬가지 취지로 평가하였다.

제2절 개인정보 보호 관련 제도 개선방안 검토

1. 동의 방식 개선 방안

가. 일괄(포괄) 동의 도입 방안

현행 개인정보보호 법령은 일괄 동의를 금지하고 있으므로 일괄적 동의를 위해서는 법률의 개정이 필요하다. 단, 이를 무조건적인 대안으로 받아들이기 보다는, 이에 대해 보다 면밀한 검토를 선행하는 것이 바람직할 것이다. 개인정보처리방침의 고지 및 정보처리 유형을 불문한 포괄 동의 허용 방식은 동의 절차 자체는 단순하지만 간접적으로 확인 가능한 개인정보처리방침 자체의 정보는 방대하기 때문에, 개인정보자기결정권 행사를 적정하고 실질적으로 보장하는지에 대하여 부정적인 견해가 제기될 수도 있을 것이기 때문이다.

나. 유형고지 도입 방안

개인정보의 실질화를 위해서는 정보제공을 단순화하여야 한다는 주장을 참고할 필요가 있다. 이를 위한 대안에는 유형고지의 도입이 있다. GDPR에서 말하는 사전에 정보를 제공받은 동의가 이루어지기 위해서는 개인정보 항목이 아닌 유형을 알리는 것도 가능하다는

것이 EU 규제기관의 입장이다.

국내 규제기관은 현행 법령상 유형 고지를 허용하지 않는 입장이다. 따라서 유형 고지 방안을 하나의 유효한 수단으로 인정하기 위해서는 이를 명시적으로 인정하는 입법 작업이 필요할 것으로 생각된다.

다. 동의제도 위반에 따른 형사처벌 규정의 개정

과징금이나 과태료와 같은 행정적 제재뿐만이 아니라 징역 또는 벌금과 같은 형사적 제재까지 동원하여 동의제도 위반을 규율한다는 것은 GDPR에서조차 발견되지 않는 우리 법의 주요 특징 중 하나이다. 그 개정 방안으로는 예를 들어 단순히 이용자의 동의를 받지 아니하고 개인정보를 수집한 자를 형사처벌 할 것이 아니라, 동의를 받지 않는 것에 더하여 “부정한 목적”등을 갖는 등 추가적인 사실관계가 인정되는 경우에만 형사적 수단을 활용하는 것을 생각할 수 있다.

라. 정당한 이익에 근거한 개인정보 처리의 도입

현재와 같이 전적으로 동의제도에 의존하는 것은 데이터 경제의 시대에 부합하지 않는다. GDPR과 같이 정당한 이익에 기초하여 개인정보를 처리하도록 하는 방안을 고려하여야 한다. 우리나라는 이와 유사한 규정을 개인정보보호법에 두고 있지만, 한정적인 적용만을 허용한다. 추후 입법 작업을 통하여 개인정보처리자의 정당한 이익에 근거한 개인정보 처리를 허용하는 것이 필요하다. 참고로 대통령직속 4차 산업혁명위원회 역시 는 정당한 이익에 따른 개인정보 처리를 허용하여야 한다는 취지의 선언을 했다.

2. 현행 법령 내에서의 동의 제도 개선 방안

가. 현행 법률 하에서 개인정보 처리 동의권의 포괄적인 대리행사를 위임하는 것이 가능한지 여부

정보주체가 개인정보 처리에 관한 동의권 행사를 마이데이터 서비스 제공자들에게 포괄적으로 대리행사 하도록 하는 것이 가능하다면 사업자들은 하나의 동의서를 통해 필요한 모든 개인정보 처리를 할 수 있어서, 동의 제도의 문제를 극복하면서 마이데이터 서비스를 제공할 가능성이 열릴 것이다. 단, 개인정보보호법은 개인정보 처리에 대한 동의권 행사를 대리할 수 있다는 취지의 규정을 두고 있지 않으므로, 대리에 대한 논의를 좀 더 구체적으로 살펴볼 필요가 있다.

일반적으로 대리는 법률행위를 대리하는 것이기 때문에 법률행위 내지 의사표시에 한

하여 허용된다. 하지만 대리에 친하지 않은 법률행위에는 대리가 허용되지 않는다. 판례는 인격권의 일종인 저작인격권은 대리하거나 위임하는 것은 가능하지만 포괄적으로 대리하는 것은 실질적으로 이를 양도하는 것이기 때문에 가능하지 않다고 하였다.

개인정보 자기결정권과 이에 근거한 개인정보 처리에 대한 동의권은 인격권에 해당한다는 견해가 유력하다. 그렇다면 위 판례에 근거하여 인격권인 개인정보 처리에 대한 동의권은 대리가 허용된다는 결론을 도출할 수 있다. 실무상 개인정보 수집 행위의 위탁 및 동의를 대신해서 받는 것이 가능하다는 점을 고려하면, 개인정보 처리에 대한 동의를 대리는 가능할 것이다.

그러나 개인정보보호법에 따른 법정 고지사항을 고지하지 않은 상황에서 동의권에 대한 포괄적인 대리행사 위임이 가능한지 여부에 대해 해석상 논란의 여지가 있을 것인 점, 인격권의 포괄적 대리는 허용된다고 보기 어려운 점, 개인정보의 처리에 대한 동의에 대하여는 대리를 허용하는 규정이 없다는 점을 고려하면, 동의권의 포괄적인 대리행사를 위임하는 것이 가능한지에 대해서는 반론의 여지가 있고, 결국 법원의 판결을 통한 해석 또는 입법적 해결이 필요한 사안이다.

이와 같은 해석상의 논란을 극복하고 마이데이터 사업자에게 포괄적으로 대리권을 부여하고자 한다면, 이를 허용하는 법률 개정을 하는 방안을 고려하여 볼 필요가 있겠다.

나. 스마트 컨트랙트를 통한 개인정보 동의절차 도입 가능 여부

스마트 컨트랙트란, 인간의 개입 없이 계약 조건이 자동적으로 이행 및 집행되는, 디지털화되고 컴퓨터 입력이 가능한 계약서다.

이러한 스마트 컨트랙트는 역동적인 동의체계를 개발하는 것이 가능하다는 점, 자동적인 계약의 이행 및 집행이 가능하다는 점, 블록체인과의 연동이 가능하다는 점에서 개인정보 처리를 위한 동의 제도에서 유용하다고 생각할 수 있다. 다만 스마트 컨트랙트를 곧바로 마이데이터 서비스에 도입하는 것은 보다 깊은 추가 검토가 필요할 것으로 보인다.

< 목 차 >

제1장 서론 ····· 1

1. 4차 산업혁명 시대 개인데이터 활용의 필요성 증대 ····· 1
2. 개인정보자기결정권과 정보이동권 - 마이데이터 서비스와의 관계 ····· 2
3. 기존 개인정보 동의 방식의 한계와 마이데이터 환경에서 동의 방식 개선 필요성 ····· 5

제2장 연구 방법 ····· 5

1. 연구의 대상 : 개인정보 수집 및 이용, 제3자 제공 등 개인정보 처리 시 동의 방식 ····· 5
2. 비교 범위: 해외(미국, EU, 일본 등)와 국내 ····· 6
3. 비교기준: 동의 시기, 동의 방법, 동의 대상 ····· 6

제3장 국내외 마이데이터 사업자의 동의 방식 ····· 6

1. 국내 마이데이터 사업자 ····· 6
2. 해외 마이데이터 사업자 ····· 9

제4장 국내외 법제도 현황 및 문제점 분석 ····· 12

1. 외국 법제도 현황 분석 ····· 12
2. 국내 법제도 현황 분석 ····· 34
3. 국내법상 동의 제도의 문제 ····· 40
4. 시사점 ····· 54
5. 산업 분야별 마이데이터 관련 법제도 현황 분석 ····· 55

제5장 개선 방안 ····· 59

제1절 개인정보 보호 관련 법률 개정안 검토 ····· 59

1. 개인정보보호법 개정안(인재근 의원안) ····· 59
2. 정보통신망법 개정안(노웅래 의원안) ····· 63
3. 신용정보법 개정안(김병욱 의원안) ····· 63

제2절 개인정보 보호 관련 제도 개선방안 검토 ····· 67
1. 동의 방식 개선 등 관련 법령의 개정을 통한 제도 개선 방안 ····· 67
2. 현행 법령 내에서의 동의 제도 개선 방안 ····· 73

제6장 결론 ····· 77

참고문헌 ····· 80

< 표 목차 >

<표 4-1> 개인정보 동의서 확인 ····· 47
<표 4-2> 동의서 미확인 이유 ····· 48
<표 4-3> 개인정보처리방침 인지 여부 ····· 48
<표 4-4> 동의서를 읽어보지 않는 이유 ····· 50
<표 4-5> 업종별 개인정보 수집 · 이용 동의관련 행태 ····· 50
<표 4-6> 필수/선택적 동의사항에 관한 동의 행태 ····· 51

< 그림 목차 >

<그림 3-1> 토스의 동의 화면 ····· 7
<그림 3-2> 토스의 선택 동의사항 ····· 7
<그림 3-3> 뱅크샐러드의 동의 화면 ····· 8
<그림 3-4> 뱅크샐러드의 동의서 내용 ····· 9
<그림 3-5> Credit Karma의 가입 화면 ····· 10
<그림 3-6> ClearScore의 가입 화면 ····· 11
<그림 3-7> MINT의 가입 화면 ····· 12
<그림 4-1> 개인정보 수집 · 이용 동의에 대한 소비자의 행동 ····· 49

제1장 서 론

1. 4차 산업혁명 시대 개인데이터 활용의 필요성 증대

4차 산업혁명 시대인 현재, 데이터는 사람, 자본 등 기존의 생산요소를 능가하는 핵심 자원으로 부상하고 있다. 데이터는 사물인터넷, 인공지능 등으로 대표되는 4차 산업혁명의 흐름 속에서 혁신성장의 토대가 될 뿐만 아니라, 누구나 기회를 갖고 자유로이 경쟁할 수 있는 공정한 시장경제를 구축하는 데 기여할 것으로 기대되고 있는 것이다. 이에 세계의 주요 국가들은 미래 경쟁력을 좌우하는 데이터의 중요성을 인식하고 데이터 산업 육성 정책 추진에 박차를 가하고 있다. 우리나라 역시 '데이터 경제'로의 전환을 선언하고 이에 필요한 제반 정책을 추진하고 있다. 과학기술정보통신부는 20180년 5월, 6월에 각각 "데이터 산업 활성화 전략"과 "IKorea 4.0 실현을 위한 인공지능(AI) R&D 전략"을 발표하였고, 2018년 8월에는 대통령이 직접 데이터 경제로의 전환을 천명하기도 하는 등[1] 정부는 2018년부터 데이터 및 AI 산업 활성화 정책을 본격적으로 추진하고 있다.

특히, 정보주체 중심의 '마이데이터(My Data)' 서비스는 의료, 교육, 금융, 통신, 에너지 등 다양한 분야에서 논의가 이루어지고 있다. '마이데이터'란, 정보주체가 기업·기관으로부터 자기정보를 직접 내려 받거나, 타 기관 등으로 이동을 요청하여 해당 정보를 활용하는 것을 의미한다.[2] 현재 국내외에는 개인(신용)정보를 활용하여 해당 정보주체에게 각종 정보를 제공하는 서비스들이 존재한다.

서구권에는 마이데이터 산업이 각국의 사정에 맞게 발전하고 있다.[3] 영국은 정부가 주도하여 '마이데이터(Midata)' 프로젝트를 추진하였고, 금융 등 일정한 서비스분야에서 제3자가 고객정보에 접근할 수 있는 법적 근거를 마련함에 따라 은행상품 비교서비스를 제공하는 '고컴페어(Go-Compare)' 등이 등장하였다. 미국도 정부가 주축이 되어 '스마트 디스클로저(Smart Disclosure)'를 추진한 점은 영국과 유사하지만, 비금융분야를 중심으로 추진되고 있다는 점에서는 차이를 보인다. 미국에서는 2016년 기준으로 16,000개 의료기관이 블루버튼(의료 분야 마이데이터 서비스) 기능을 지원하고 있다. 또한 '민트(Mint)'와 같이 은행 등 금융회사의 정보를 취득하여 종합적으로 제공하는 서비스도 존재한다. 반면 프랑스는 정부가 아닌 민간 주도의 '메젱포[MesInfos(Self-Data)] 프로젝트'가 진행된 점에서 영미의 사례와 다르다.[4] 스웨덴의 경우 인구 약 1천만 명 중 약 410만 명이 의료공

1) 관계부처 합동, "-혁신성장 전략투자- 데이터•AI경제 활성화 계획['19~'23년]", 2019. 1. 16., 2면
2) 과학기술정보통신부 2018. 8. 31. 보도자료 "데이터를 가장 안전하게 잘 쓰는 나라를 만들겠습니다."
3) 이하의 내용 외 자세한 사항과 관련해서는 고환경 · 손경민 · 주성환, 정보이동권과 마이데이터 산업, BFL 제93호(2019. 1), 24~25면을 참조.
4) 고연희, 본인신용정보 관리업 도입과 해외사례, NICE Credit Insight(2018 Autumn), NICE평가정보 CB연구소, 58-66면.

공기관(Inera)이 만든 의료정보 포탈에 가입되어 있다.

우리나라에서는 개인신용정보를 활용한 비즈니스를 가장 활발하게 운영하는 신용조회회사(CreditBureau, CB)가 개인고객에게 '본인신용평점 및 변동내역, 신용평점 산정근거가 되는 연체정보, 대출정보, 카드사용 내역정보 등'을 제공하고 있다. 공공분야에서는 금융감독원의 '연금포털', 금융결제원의 '계좌통합관리(어카운트인포)', 생명보험·손해보험협회의 '내보험찾아줌', 신용정보원의 '내보험다보여', 여신금융협회의 '카드포인트통합조회' 등의 서비스가 있다. 또한 '토스' 등 일부 핀테크업체는 고객을 대신하여 은행 등 금융회사의 계좌정보를 일괄조회하는 서비스를 제공하고 있다.[5)]

그러나 우리나라의 개인정보 규제는 세계적으로 높은 수준이고, 이로 인한 데이터 활용 역시 크게 위축되어 있는 것이 현실이다. 게다가 높은 수준인 개인정보 규제에도 불구하고 실질적인 개인정보 보호는 제대로 이루어지지 못하고 있다는 비판도 많다. 특히, 개인정보처리에 대한 정보주체의 동의 절차, 즉 '동의 제도'는 후술하는 바와 같이 우리나라 정보보호 관련 규제의 핵심이라고 할 만하다. 그리고 제3장에서 자세히 소개하겠지만 우리나라에서 현재 이루어지고 있는 마이데이터 서비스는, 정보주체의 개인정보 열람권과 개인정보 동의를 법적 기반으로 하고 있다. 따라서 마이데이터 산업 발전을 위하여 동의 제도를 어떻게 개선해야 하는지 논의가 필수적이며 가장 시급하고 중요한 것으로 판단된다.

다만 그에 앞서, 마이데이터 서비스의 기반으로서 우리 법제 하에서도 유럽연합에서 인정하는 정보이동권을 반드시 필수적인 전제조건이라고 할 것인지에 대해 간략히 살펴보도록 한다.

2. 개인정보자기결정권과 정보이동권 - 마이데이터 서비스와의 관계

헌법재판소는 2005년 이른바 '열 손가락 지문등록 사건'에서 개인정보자기결정권을 인정하면서 개인정보자기결정권에 대해 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리", 즉 "정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리"라고 정의한 바 있다.[6)]

한편, 정보이동이란, 말 그대로 "어느 개인의 정보를 정보주체의 요구에 따라 다른 정보처리자에게 고스란히 이전하는 것"[7)]으로, 정보이동권은 유럽연합 일반 개인정보보호법

5) 고연희, 앞의 논문, 56면.
6) 헌법재판소 2005. 5. 26 자 99헌마513, 2004헌마190(병합) 결정
7) 박훤일, 정보이동권의 국내 도입방안 - EU GDPR의 관련 규정을 중심으로, 경희법학 제52권 제3호, 경희대학교 법학연구소, 2017. 212면.

(General Data Protection Regulation, 이하 'GDPR')에서 도입한 개념이다. GDPR이 정보이동권을 도입한 목적은 정보주체의 개인정보자기결정권을 강화하고, 개인정보처리자와 정보주체 사이 관계의 균형(선택권)을 보장할 뿐만 아니라, 이를 통하여 온라인 서비스 제공자 사이의 경쟁을 강화하기 위한 것으로, 정보주체가 자신의 정보가 특정 사업자에게 고착(Lock-In)되는 것을 피해 경쟁관계에 있는 다른 서비스 제공자에게 정보를 이전할 수 있도록 하는 경쟁 개선 및 촉진 측면을 고려한 결과이다.[8)]

정보이동은 우리나라에서도 생소한 개념은 아니다. 이동통신 서비스에 있어서 2004년부터 가입자가 기존 전화번호를 그대로 유지한 채 이동통신 사업자 및 서비스 내용을 변경할 수 있게 하는 번호이동성제가 시행되고 있으며, 2015년에는 자동이체(자동납부 및 자동송금 포함) 항목을 새 은행계좌로 그대로 이전할 수 있는 계좌이동 서비스를 이용할 수 있게 되었다.[9)]

마이데이터 서비스는 기존에 개인정보를 보유한 기관들로부터 마이데이터 사업자가 개인정보를 이전 받아 이를 통합·집적한 후 맞춤형 서비스 등을 정보주체에게 제공하는 것을 전제로 하므로[10)] 마이데이터 산업만을 놓고 본다면 정보이동권이 인정되면 서비스 활성화에 도움이 될 것으로 생각된다.

다만 정보이동권이 헌법상 개인정보자기결정권에서 도출되어 법률상 규정 없이 당연히 인정되는 권리라고 보기는 어렵다.

즉, 기본권의 대사인적 효력의 인정 여부 및 범위에 관하여는 여전히 논란이 있고, 개인정보자기결정권을 배타적 · 절대적 기본권으로 보기 어려운데다[11)12)] 개인정보자기결정권은 법률을 통하여 그 보호 대상 및 범위를 구체화할 필요가 있기 때문이다. 특히, 현행법상 개인정보 제3자 제공은 개인정보처리자가 제공(공유) 여부를 결정하고, 이용자의

---

8) Article 29 DATA PROTECTION WORKING PARTY, Guidelines on the Right to Data Portability (2017. 4. 5.), pp. 3~4

9) 박훤일, 앞의 논문, 212면.

10) 고환경 · 손경민 · 주성환, 앞의 논문, 27면.

11) 개인정보자기결정권을 절대권 내지 지배권으로 규정하는 이론적 구도에서는 개인정보자기결정권은 인간의 존엄과 가치라는 헌법 최고 이념으로부터 도출되는 것이므로 절대적인 권리라고 보는 견해도 있으나(이러한 견해에 대하여는 권영준, 개인정보자기결정권과 동의 제도에 대한 고찰, 법학논총 제36권 제1호, 2016, 689면을 참조), 개인정보자기결정권 역시 헌법 제37조 제2항에 의해 제한될 수 있다고 보는 것이 타당하다. 헌법재판소 역시 "개인정보의 종류 및 성격, 수집목적, 이용형태, 정보처리방식 등에 따라 개인정보자기결정권의 제한이 인격권 또는 사생활의 자유에 미치는 영향이나 침해의 정도는 달라지므로 개인정보자기결정권의 제한이 정당한지 여부를 판단함에 있어서는 위와 같은 요소들과 추구하는 공익의 중요성을 헤아려야" 한다('NEIS 교육정보시스템 사건', 헌법재판소 2005. 7. 21.자 2003헌마282 결정)는 등 공공의 이익을 위해 개인정보자기결정권의 제한이 인정된다는 취지의 판시를 여럿 내린 바 있다.

12) 유럽연합의 GDPR 역시 전문 (4)에서 "개인정보보호권은 절대적 권리가 아니며, 개인정보보호권은 사회에서의 개인정보보호 기능과 관련하여 고려되어야 하며 비례의 원칙에 입각하여 다른 기본권과 균형을 이루어야 한다."라고 규정하고 있다. ("The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.")

동의를 받는 체계로 구성{개인정보보호법 제17조 제1항, 정보통신망의 이용촉진 및 정보보호에 관한 법률(이하 '정보통신망법') 제24조의2 제1항, 신용정보의 이용 및 보호에 관한 법률(이하 '신용정보법') 제32조 제1항 등}되어 있으므로, 현행법 상으로는 정보주체가 직접 개인정보의 전송을 요구할 권리가 있으며 개인정보처리자가 이를 수락해야 할 의무가 있다고 해석하기는 어렵다. 유럽연합 또한 GDPR 제20조에서 별도로 명시함으로써 정보이동권을 규정하고 있다는 점도 고려할 필요가 있다.

또한 정보이동권이 마이데이터 서비스 제공을 위해 반드시 필수적으로 전제되어야 하는 개념이나 권리라고 보기는 어렵다.

마이데이터 사업자는 원칙적으로 (현재 서비스를 제공하는 방식이기도 하나) 정보주체의 위임을 받아 그 권리를 대리 행사 하는 방식으로 마이데이터 서비스를 제공할 수 있다. 정보통신망법은 이용자의 권리를 대리 행사할 수 있는지에 대하여 명시적으로 규정하고 있지 않으나, 이는 법률행위에 해당하므로, 다른 별도의 법률규정이 없는 한 대리 또는 사자(使者)에 친하지 않은 행위로 보기는 어렵다. 개인정보보호법 제38조 역시 정보주체가 그 권리를 대리인에게 행사할 수 있다는 명시적인 규정을 두고 있다.[13]

마이데이터 사업자가 정보주체로부터 (마이데이터 사업자에 대한) 개인정보 제3자 제공 동의를 받는 방법으로 사업을 진행할 수도 있다. 금융위원회 역시 '개인정보를 제공받고자 하는 자가 정보주체의 동의를 받아 해당 정보주체의 개인정보를 보유하고 있는 자에게 제공 요청을 할 수 있는지 여부'에 대해 "해당 개인정보를 제공하는 자와 제공받고자 하는 자가 상호 협의한 경우에는 개인정보를 제공받고자 하는 자가 개인정보를 제공하는 자에게 정보주체의 동의 의사를 대신 제출한 후 개인정보를 제공받는 것은 가능"하다고 설명하고 있다.[14]

물론 전술한 바와 같이 정보이동권이 도입된다면 마이데이터 서비스 제공과 산업활성화에 큰 도움이 될 것이라는 데 이견을 제기하기는 어려울 것이다.[15] 하지만 정보이동권을 도입한다면 개인정보처리자의 영업의 자유, 재산권 등 다른 기본권과 충돌상황이 발생할 수 있는 점[16]을 충분히 고려할 필요가 있다. 즉, 정보이동권 도입은 마이데이터 사업자의 정보획득 능력을 강화하여 마이데이터 산업 활성화를 촉진시킬 것으로 보이나 서비스 제공을 위해 반드시 필수적인 전제는 아니라고 보이며, 그보다 마이데이터 서비스를

13) 현재 국내 마이데이터 사업자의 경우 보다 정확하게는, 정보주체로부터 대리권을 수여받아 대리인으로서 정보주체의 권리를 대리 행사하는 방식을 취하기보다는, 대리권을 수여받은 후 대리권을 표시하지 않고 본인이 행사하는 것처럼 대행하는 경우가 일반적이다.

14) 금융위원회, 금융분야 개인정보보호 가이드라인, 2017, 90면.

15) 후술하는 바와 같이 김병욱 의원이 대표발의한 신용정보법 일부개정법률안(의안번호 16636)에는 정보이동권 도입도 포함되어 있다.

16) 예컨대 개인정보처리자가 고객유치 등 정보주체의 개인정보 수집을 위해 비용을 투입하였더라도 정보주체가 정보이동권을 행사한다면 개인정보처리자가 비용을 회수하기 어려워진다는 문제가 발생한다. 이는 전술한 이동통신 서비스의 번호이동성제 도입 이후 업계에서 나타나는 문제점이기도 하다.

보다 안정적으로 제공하고 발전시키기 위해서는 개인정보 관련 동의 제도를 합리적으로 개선하는 것이 필수적이며 시급한 과제라고 생각된다.

3. 기존 개인정보 동의 방식의 한계와 마이데이터 환경에서 동의 방식 개선 필요성

아래 제3장에서 자세히 설명하겠으나 현재의 개인정보 관련 법률상의 동의 제도는 여러 면에서 비판을 받고 있다. 이른바 동의만능주의에 의한 '동의규제의 역설'이 일어나고 있다는 것이 그 대표적인 예이다. 개인정보보호법, 정보통신망법, 신용정보법 등 개인정보에 대한 중복적인 규율 역시 문제다. 법해석 실무 역시 균형을 잃었다는 비판을 받고 있다.

이러한 상황에서 전술한 바와 같이 현재 국내 마이데이터 산업은 현행법 상의 동의 제도를 법적 기반으로 하고 있으며, 이는 비록 신용정보법 개정안이 금융분야에서 제도적으로 정보이동권을 도입하고 있으나 여전히 개인정보 동의 제도가 마이데이터 사업의 제도적 근간으로 그 역할을 이어나갈 것으로 생각된다. 4차 산업혁명을 맞이하는 지금, 동의 제도의 개선이 마이데이터 산업을 비롯한 데이터 산업 전반의 성패를 좌우할 수 있다고 말해도 과언이 아닌 것이다.

제2장 연구 방법

1. 연구의 대상 : 개인정보 수집 및 이용, 제3자 제공 등 개인정보 처리 시 동의 방식

앞서 살펴봤듯이, 마이데이터 산업의 성패는 개인정보 처리 시 동의 규제를 개선하는 것에 달려있을 것이다. 이에 따라 본 연구는 현행 개인정보 처리 시 동의 방식을 자세히 살펴볼 것이다.

연구대상은 이른바 데이터 3법이라고 불리는 개인정보보호법, 정보통신법, 그리고 신용정보법이다. 구체적으로 데이터 3법의 개인정보 처리 동의에 대한 규정에는 어떠한 것이 있는지, 이와 관련된 규제기관의 해석과 법원의 입장은 어떠한지 살펴보는 방식으로 현행 법률 및 제도를 분석할 것이다. 이에 기초하여 현행 법률 및 제도의 문제를 검토하겠다. 그 과정에서 해외 마이데이터 사업자는 어떠한 방식으로 개인정보를 처리하는지, 해외 법률 및 제도는 어떻게 구성되어 있는지도 살펴보겠다.

위에 기초하여 마이데이터 산업의 성공적 정착을 위한 제도 개선 방안을 살펴볼 것이

다. 우선, 인재근 의원이 발의한 개인정보보호법 개정안과 김병욱 의원이 발의한 신용정보법 개정안이 현재 국회에 계류 중인데, 위 개정안과 이들에 대한 검토보고서를 살펴봄으로써 위 개정안만으로도 마이데이터 산업의 성공적 도입을 이룰 수 있는지 아니면 추가적인 개정이 필요한지에 대하여 분석하겠다.

추가적인 개정이 필요하다면 어떠한 내용을 담고 있어야 하는지, 특히 포괄 동의 또는 "유형 고지" 도입 방안, 장기적으로는 이른바 합법적인 또는 정당한 이익(Legitimate Interest)에 근거한 개인정보 처리를 허용하는 방안에 대하여 논의하겠다.

개인정보 동의 절차 개선에 관하여는, 현행 법률 하에서 개인정보 처리 동의권의 포괄적인 대리행사를 위임하는 것이 가능한지 그리고 보다 합리적인 동의 규제 개선 방안이 무엇인지에 대하여 살펴보겠다.

2. 비교 범위: 해외(미국, EU, 일본 등)와 국내

현재 대표적인 국내 마이데이터 사업자에는 "토스"를 운영하는 주식회사 비바리퍼블리카, "뱅크샐러드"의 제공업자인 주식회사 레이니스트, "보맵" 앱의 개발사인 보맵 주식회사 등이 있다. 우리나라보다 앞서 마이데이터 서비스를 제공하고 있는 회사에는 미국의 Credit Karma사, 영국의 ClearScore사, 미국의 MINT사 등이 있다. 이러한 다양한 국적의 사업자가 마이데이터 서비스를 어떻게 제공하고 있는지 비교하도록 하겠다.

3. 비교기준: 동의 시기, 동의 방법, 동의 대상

국내 마이데이터 사업자와 해외 마이데이터 사업자가 각각 어떤 절차를 통해 필요한 개인정보를 처리하는지 살펴보는 것은 현재 데이터 3법이 가지고 있는 문제점 그리고 마이데이터 산업의 성공을 위하여 나아가야 할 방향에 대한 주요한 시사점을 제공할 것이다. 따라서 본 연구는 이러한 해외와 국내 마이데이터 사업자가 개인정보 처리를 위한 동의를 취득하는 시기, 동의를 취득하는 방법, 동의를 받은 항목 등을 비교하여 분석하도록 하겠다.

제3장 국내외 마이데이터 사업자의 동의 방식[17)]

1. 국내 마이데이터 사업자

17) 이하 내용은 본 연구과제가 진행 되었던 2019. 9. ~ 11.경 사이의 동의 방식을 기준으로 설명한 것이다. 그 이후에 사업자들은 동의 방식을 변경하였을 수 있음을 참고할 필요가 있겠다.

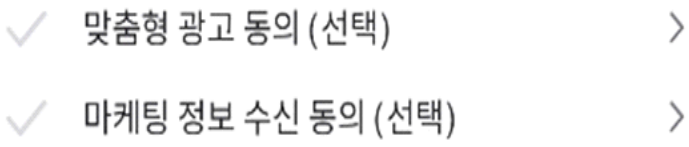
가. 토스

주식회사 비바리퍼블리카가 운영하는 토스는 송금과 관련된 마이데이터 서비스에 해당한다. 토스를 이용하기 위해서는 개인정보 수집이용과 개인정보 제3자 제공에 대해 동의하여야 하는데, 토스는 필수 동의사항, 즉 서비스 이용약관, 통합 금융정보 서비스 약관, 개인정보 수집이용 동의, 개인정보 제3자 제공 동의에 대해 일괄동의 기능을 운영하고 있다.

<그림 3-1> 토스의 동의 화면

이외에 서비스 이용을 위하여 필수적이지 않은, 맞춤형 광고와 마케팅 정보 수신을 위한 개인정보 처리에 대한 동의사항이 있다.

<그림 3-2> 토스의 선택 동의사항



동의서 분량은 상당한 편으로, 핸드폰 화면을 통해 구체적 고지사항을 확인하는 것이 가능하다.

나. 뱅크샐러드

주식회사 레이니스트는 뱅크샐러드를 통해 자산관리 서비스를 제공하고 있다. 뱅크샐러드를 이용하기 위해서는 개인정보 수집 및 이용, 개인정보 제3자 제공에 필수적으로 동의하여야 하며, 뉴스레터 및 마케팅 정보 수신에는 선택적으로 동의할 수 있다.

<그림 3-3> 뱅크샐러드의 동의 화면

구체적인 동의서의 내용은 다소 간략하다. 예를 들어, 수집하는 개인신용정보 항목에는 “신용조회 회사로부터 수집하는 신용점수, 신용등급, 신용정보 변동여부 및 변동내역, 타기관에 의한 신용정보 조회내역, 카드보유현황, 대출현황, 연체현황, 연대보증 현황 등의 고객 신용정보 세부 내역”이라고 되어 있어, 개인정보의 유형을 기재하는 방법을 택했다.

<그림 3-4> 뱅크샐러드의 동의서 내용

수집 항목	이용목적	보유기간
* 신용조회 회사로부터 수집하는 신용점수, 신용등급, 신용정보 변동여부 및 변동내역, 타기관에 의한 신용정보 조회내역, 카드보유현황, 대출현황, 연체현황, 연대보증 현황 등의 고객 신용정보 세부 내역	* 신용등급 및 신용점수 확인 등 고객의 신용정보 관리를 위한 정보 제공 * 기타 고객에게 유익하다고 판단되는 정보의 제공	해당 서비스 해지취소 시 또는 회원탈퇴 시 까지

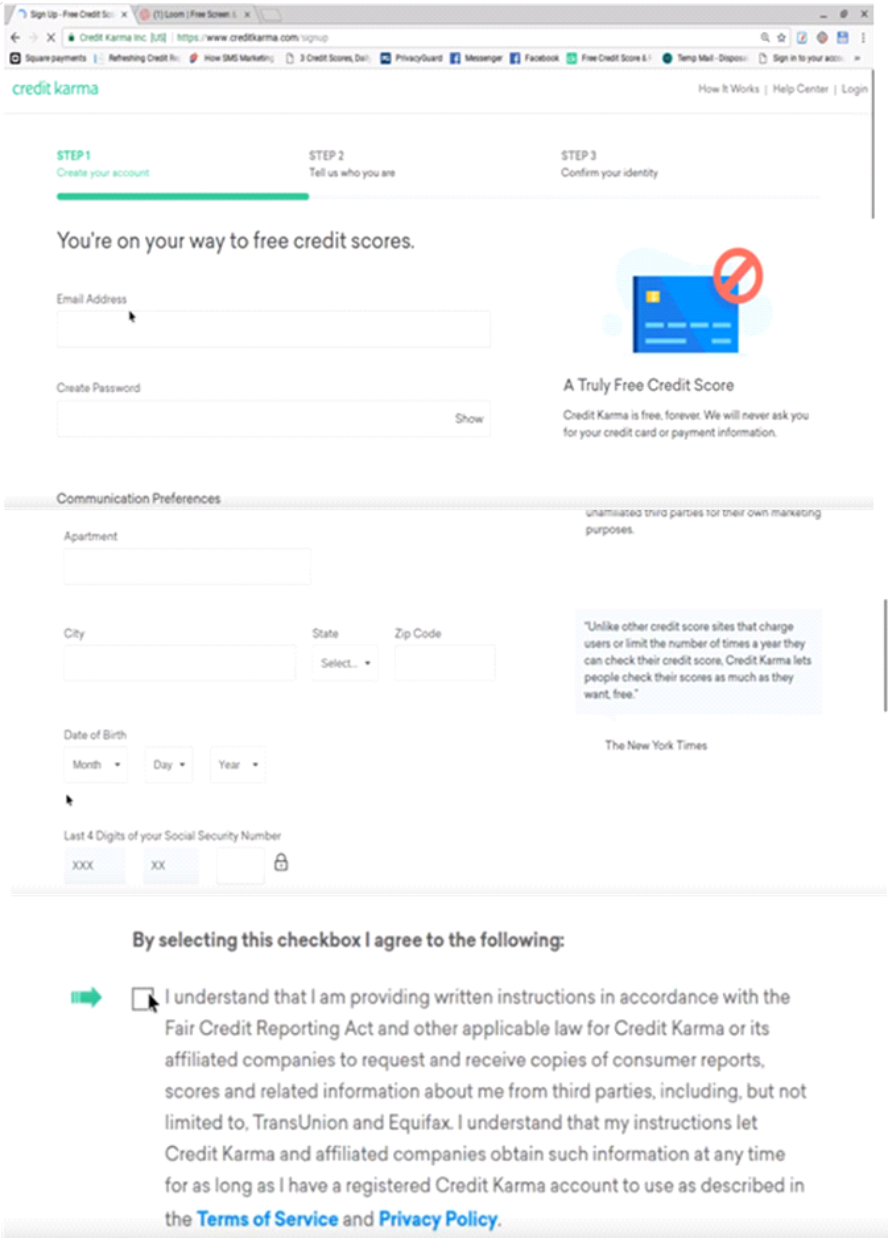
2. 해외 마이데이터 사업자

가. Credit Karma

미국의 신용정보업 관련 마이데이터 서비스 제공자인 Credit Karma는 한국의 마이데이터 사업자와 같은 복잡한 동의절차를 두고 있지 않다. 서비스 제공을 위하여 필요한 정보를 입력하고 이용약관과 개인정보처리방침에 동의한다는 상자를 체크하면 된다. 아래 화면은 Credit Karma의 이용방법을 안내한 동영상의 캡쳐 화면이다[18].

18) 참고로 미국에 거주하지 않는 자는 사용이 불가능하며, 한국에서 접속할 경우 서비스가 제공되지 않는다는 화면이 출력된다.

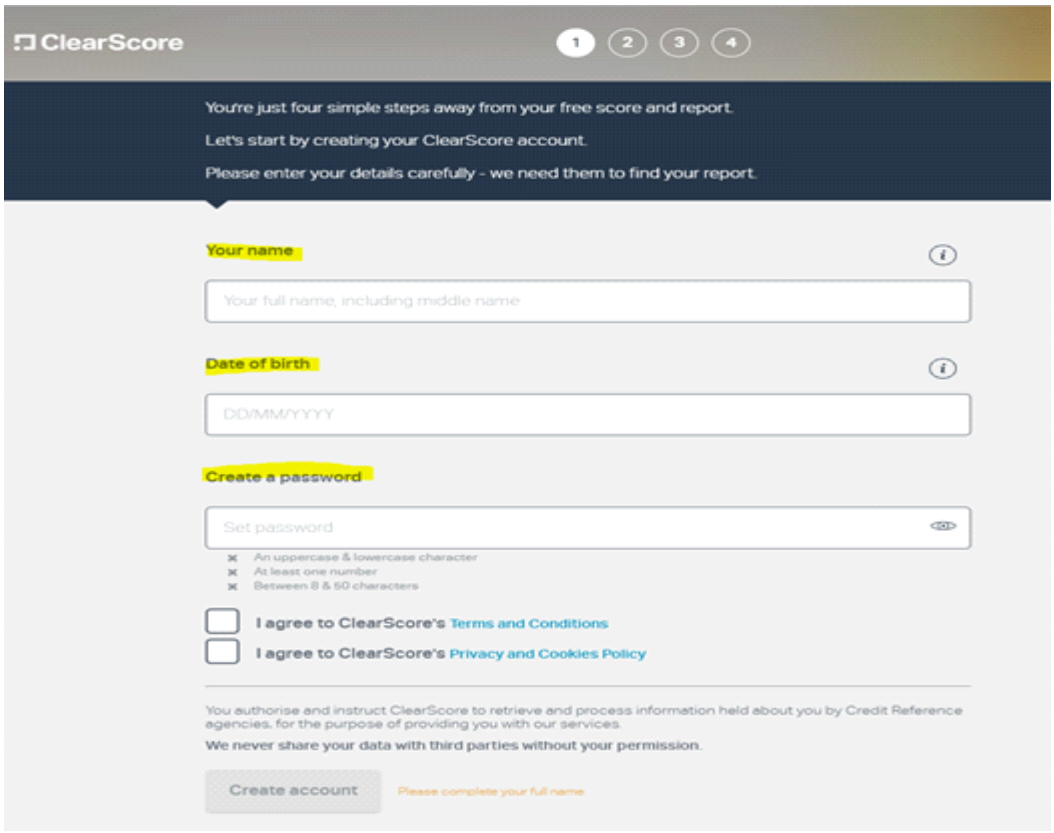
<그림 3-5> Credit Karma의 가입 화면



나. ClearScore

Credit Karma와 유사한 서비스를 제공하는 영국 마이데이터 사업자인 ClearScore 역시 간편한 개인정보 처리 절차를 두고 있다. 즉, 개인정보 처리에 대한 개별적 동의서를 두고 있지 않고, “개인정보 및 쿠키 정책”(Privacy and Cookies Policy)에 동의하면 바로 서비스 사용을 시작할 수 있도록 하고 있다.

<그림 3-6> ClearScore의 가입 화면



다. MINT[19)]

MINT는 미국과 캐나다에서 이용할 수 있는 마이데이터 서비스로 예금잔액, 공과금 및 각종 고지서, 대출내역, 신용카드 사용내역, 신용등급 등과 같은 개인 재무활동 정보를 이용자에게 제공한다. 회원가입을 진행하기 위해서는 이메일 주소와 비밀번호를 입력하면 된다. 개인정보 처리를 위한 동의를 별도로 받지 않고, 계정을 생성하면 자동으로 이용약관과 개인정보처리방침에 동의하는 것으로 간주된다.

19) NICE평가정보, Credit Insight 2018년 가을호, https://www.credit.co.kr/ib20/mnu/BZWCACMAG03

<그림 3-7> MINT의 가입 화면

〈Mint.com〉

제4장 국내외 법제도 현황 및 문제점 분석

1. 외국 법제도 현황 분석

가. 유럽연합 일반 개인정보보호법(GDPR)

(1) 적법 처리 조건

유럽연합의 GDPR에서는 개인정보처리에 적용이 가능한 적법 처리 조건(Lawfulness of processing)으로 정보주체의 동의를 포함한 6가지를 두고 있다. GDPR에서 제시하는

적법 처리 조건은 ① 정보주체가 하나 이상의 특정한 목적을 위하여 개인정보 처리에 동의한 경우, ② 정보주체가 당사자인 계약의 이행을 위하여 또는 계약 전 정보주체 요청에 응하기 위한 처리, ③ 컨트롤러에게 적용되는 법적 의무 이행을 위하여 필요한 처리, ④ 정보주체 또는 제3자의 중대한 이익을 보호하기 위하여 처리가 필요한 경우, ⑤ 공익을 위하여 수행되는 직무의 이행 또는 컨트롤러에게 부여된 공적 권한의 행사에 필요한 처리, ⑥ 컨트롤러 또는 제3자의 적법한 이익 추구 목적을 위하여 필요한 경우(정보주체가 아동인 경우와 같이 정보주체의 이익과 권리 또는 자유가 그 이익보다 중요한 경우는 제외) 등이다.[20]

<GDPR 번역문[21]>

제6조 처리의 적법성
1. 개인정보 처리는 적어도 다음 각 호의 하나에 해당되고 그 범위에서만 적법하다.
(a) 개인정보주체가 하나 이상의 특정 목적에 대해 본인의 개인정보 처리를 동의한 경우
(b) 개인정보주체가 계약 당사자가 되는 계약을 이행하거나 계약 체결 전 개인정보주체가 요청한 조치를 취하기 위해 처리가 필요한 경우
(c) 개인정보처리자의 법적 의무를 준수하는데 개인정보 처리가 필요한 경우
(d) 개인정보주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 개인정보 처리가 필요한 경우
(e) 공익을 위하거나 개인정보처리자의 공식권한을 행사하여 이루어지는 업무수행에 처리가 필요한 경우
(f) 개인정보처리자 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우로서, 개인정보가 보호되어야 할 개인정보주체의 이익 또는 기본적 권리와 자유가 우선되는 경우는 제외한다. 개인정보주체가 어린이인 경우에는 특히 그러하다.
제1항 (f)호는 공공기관이 소관 업무를 수행하기 위해 개인정보를 처리하는 경우에는 적용되지 않는다.

2. 회원국은 본 규정의 규칙을 적용하기 위하여 더욱 구체적인 조문을 유지하거나 도입할 수 있다. 이는 개인정보 처리를 위한 구체적 요건과, 제IX장에서 규정하는 특정 처리 상황등과 같이 적법하고 공정한 처리를 보장하기 위한 여타 조치들을 더욱 엄밀히 결정함으로써 제1항 (c)호 및 (e)호의 준수를 담보하기 위한 내용에 관한 것이다.

3. 제1항의 (c)호 및 (e)호에서의 개인정보 처리의 근거는 다음 각 호를 통해 규정되어야 한다.
(a) 유럽연합 법률
(b) 개인정보처리자에게 적용되는 유럽연합 회원국의 법률

20) 한국인터넷진흥원, 우리 기업을 위한 'EU일반 개인정보보호법(GDPR)' 가이드북 개정판, 2018, 47~48면.
21) 번역문은 개인정보보호위원회, 유럽 일반 개인정보보호법(GDPR) 번역본, 2017.을 참조하였음. 이하 동일함.

처리목적은 상기의 법적 근거에 의해 결정되어야 한다. 제1항 (e)호의 처리는 공익을 위하거나 개인정보처리자의 공식권한을 행사하여 이루어지는 업무수행에 필요한 것이다.
해당 법적 근거로는 본 규정의 규칙을 적절히 적용하기 위한 특정 조문이 있을 수 있으며, 특히, 개인정보처리자의 개인정보 처리 적법성에 대한 일반적인 조건, 해당 처리의 대상이 되는 개인정보의 유형, 관련 개인정보주체, 관련 개인정보의 제공 대상 및 목적, 목적 제한, 보관기간, 제IX장에서 규정하는 특정 처리상황을 위한 조치 등 합법적이고 공정한 처리를 보장하는 조치를 포함한 처리작업 및 처리절차가 이에 해당한다. 유럽연합 또는 회원국 법률은 공익의 목적을 달성하고 추구하는 적법한 목표에 비례해야 한다.

4. 개인정보를 수집한 목적 외로 처리하는 것이 개인정보주체의 동의 또는 제23조(1)의 목적을 보장하기 위한 민주사회의 필요하고 비례적인 조치를 구성하는 유럽연합 또는 회원국 법률에 근거하지 않는 경우, 개인정보처리자는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려해야 한다.
(a) 수집 목적과 의도된 추가처리 목적 간의 연관성
(b) 특히 개인정보주체와 개인정보처리자 간의 관계와 관련해서 등의 개인정보가 수집된 상황
(c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격

이는 우리나라의 개인정보보호법 제15조 제1항의 제1호 내지 제6호에서 개인정보처리의 조건을 정보주체의 동의를 포함하여 6가지 두고 있는 것과 유사하다. 그러나 후술하는 바와 같이 우리 개인정보보호법령, 특히 정보통신망법에서는 동의가 원칙인 것으로 규정하고 해석되는 점 등에서 큰 차이점이다.

특히, GDPR에서는 개인정보 수집 목적 외 처리가 정보주체의 동의 또는 법적 의무 준수에 근거하지 않는 경우라도 개인정보를 수집한 목적과 양립하는 목적(compatible purpose)인 경우 별도의 동의 없이 추가적인 이용 및 제공을 허용한다는 점은 우리 법과 구별되는 사항이다. 후술하는 바와 같이 이는 개인정보보호법 일부개정안(인재근 의원 대표발의, 의안번호 16621)에 반영되어 있으나 현행법에서는 이와 같은 규정을 두고 있지 않다.

<GDPR 번역문>

전문

(50) 원래 수집 목적 이외의 개인정보 처리는 해당 개인정보의 처리가 원래의 수집 목적과 양립 가능한(compatible) 경우에 한해서만 허용되어야 한다. 목적이 양립 가능한 경우, 당초 정보

수집을 허용한 법적 근거 이외의 별도의 법적 근거는 불필요하다. (목적이 양립가능하다면 별다른 근거 없이도 추가적으로 정보처리가 가능하다.)

공익을 추구하거나 컨트롤러에게 내재된 공적권한을 행사하여 시행되는 직무 이행에 처리가 필요한 경우, 유럽연합 또는 회원국 법률은 추가 처리가 양립 가능하고 적법하다고 간주되는 직무 및 목적을 결정하여 명시할 수 있다. 공익상의 기록 보존 목적, 과학·역사 연구 목적 또는 통계 목적으로의 추가 처리는 양립 가능의 적법한 처리 작업으로 간주되어야 한다. 유럽연합 또는 회원국 법률이 규정하는 개인정보 처리의 법적 근거는 추가 처리의 법적 근거도 될 수가 있다.

(2) 동의 제도

GDPR에서 적법 처리 조건으로서의 정보주체의 동의와 우리 법의 동의 제도는 몇 가지 차이점이 있다. GDPR에서 동의는 "정보주체가 진술 또는 적극적 행동을 통하여 자신의 개인정보처리에 대한 긍정의 의사를 표현하는 것"을 의미하는데, 이때 정보주체의 동의는 '진정한(genuine)' 것이어야 하며, 형식적인 요건의 충족만으로 달성할 수 없다. 특히 강제, 압박, 자유 의지 행사 제한 등과 같은 요소가 존재하는 경우의 동의는 자유롭게 제공한 것이 아니므로 유효한 동의가 될 수 없다.[22]

<General Data Protection Regulation>

Recital

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

22) 위 가이드북, 49면.

If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

<GDPR 번역문>

전문

(32) 동의는 전자적 방법을 포함한 서면진술이나 구두진술 등으로, 정보주체가 개인정보의 처리에 대해 자유롭게 제공하여야 하는데, 구체적으로, 고지된 명확한 합의를 나타내주는 적극적인 행위로써 제공되어야 한다. 동의표현방법에는 인터넷 웹사이트의 개인정보처리 동의란 체크, 정보사회서비스에 대한 기술적 설정 선택 또는 본인의 개인정보처리 수락을 의미하는 정보주체의 행동이나 기타 진술이 포함된다. 따라서 침묵, 사전 자동체크 된 개인정보처리동의나 부작위는 동의에 해당되지 않는다. 동의는 단일 또는 복수의 동일한 목적을 위한 모든 처리 활동에 유효하다. 복수의 목적으로 개인정보를 처리하는 경우, 각 목적에 대한 동의를 받아야 한다. 만약 정보주체의 동의를 전자방식의 요청에 따라 제공하는 경우, 그 요청은 명확하고 간결하게 제공되어야 하며, 관련 서비스 이용을 불필요하게 방해해서는 안된다.

위와 같은 맥락에서 GDPR의 동의 제도에는 네 가지 유효 조건(valid consent)이 있는데, ① 자유롭게 부여된 동의, ② 개별적으로 특정한 동의, ③ 사전 정보가 제공된 동의, ④ 정보주체의 모호하지 않은 의사표시가 그것이다. 이하에서는 각 조건에 대해 살펴보도록 하겠다.[23]

<General Data Protection Regulation>

Article 4 Definitions

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

23) 이하의 내용에 관하여는 위 가이드북 50~54면 참조.

<GDPR 번역문>

(11) 개인정보주체의 동의는 본인과 관련된 개인정보의 처리에 대해 합의한다는 개인정보주체의 희망을 진술 또는 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 의사표시를 가리킨다.

㈎ 자유롭게 부여된 동의(Free/Freely given)

GDPR에서의 동의란 정보주체에게 본인의 개인정보처리에 대하여 실질적인 선택권과 통제권을 부여하는 것을 의미한다. 정보주체가 반드시 동의하여야 한다고 강제적인 느낌을 받는 등 개인에게 실질적 선택권이 없다면 유효한 동의로 보지 않는다. 즉 동의가 자유롭게 제공되도록 보장하기 위하여 정보주체와 컨트롤러 사이에 명백한 불균형이 있는 특정 상황의 경우에는 동의를 개인정보처리에 유효한 법적 근거로 볼 수 없으며 컨트롤러는 정보주체가 불이익 없이(without detriment) 동의를 거부 또는 철회할 수 있다는 것을 입증하여야 한다.

<General Data Protection Regulation>

Recital

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC1 a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid

legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
<GDPR 번역문> 전문 (42) 개인정보 처리가 정보주체의 동의에 근거하는 경우, 정보처리자는 정보주체가 처리 방식에 대해 동의를 제공하였음을 입증할 수 있어야 한다. 특히 처리되는 사안이 아닌 다른 사안에 대해 서면 진술로 동의하는 경우, 정보주체가 어떤 정보가 어떤 범위로 제공된다는 사실을 인지할 수 있도록 보장하여야 한다. 유럽의회 지침 93/13/EEC1에 따라, 정보처리자가 제공하는 사전동의서 서식은 명확·평이한 언어를 사용하여 이해하기 쉽고 열람이 가능하도록 하여야 하며 불공정한 용어를 포함해서는 안된다. 동의를 고지 받기 위해서는 정보주체는 최소한 정보처리자의 신원과 개인정보 처리 목적에 대해 인지하고 있어야 한다. 정보주체가 진심으로 동의하지 않았다거나, 자유로운 선택으로 동의하지 않았다거나, 손실 없이는 동의를 거절하거나 철회할 수 없는 경우에는 해당 동의는 자유롭게 제공된 것이라고 간주되지 않는다. (43) 동의가 자유롭게 제공되기 위해서는, 정보주체와 정보처리자 간의 명백한 불균형이 존재하는 특정 상황과 같은 경우에는 동의를 합법적인 근거로 제시해서는 안된다. 특정상황이란 특히 정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 개별적인 사례에서 적절하다고 판단되는 경우도 있겠으나, 별개의 개인정보처리행위에 대해 별도의 동의를 받지 않는 경우이거나, 서비스 제공 등의 계약의 이행이 동의없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.

㈏ 개별적으로 특정한 동의(Specific)

정보주체의 이용자 통제권 및 투명성을 확보하기 위하여 동의의 내용은 개별적으로 특정되어야 한다. 해당 요건을 충족하기 위해서는, ① 목적 명확화 및 ② 동의 메커니즘의 상세화, ③ 동의 획득과 관련한 정보와 다른 정보의 명확한 분리의 사항이 모두 적용되어야 한다.

여기서 목적 명확화란, 개인정보처리의 목적이 점진적으로 확대되거나 불명확해지는 기능 확대 현상[24]이 발생하여 정보주체가 예상할 수 없는 개인정보처리를 발생시키는 것을 대비한 안전조치로서의 성격을 갖는다. 또한 동의 메커니즘의 상세화란 컨트롤러가 개별 처리 목적에 대한 개별적 옵트인(opt-in)을 제공해야 함을 의미한다. 또한 동의 획득과 관련한 정보와 다른 정보의 명확한 분리란 서로 다른 목적을 지닌 각각의 동의 항목에 따라 개별적으로 특정한 정보가 제공되어야 함을 의미한다.

㈐ 사전 정보가 제공된 동의(Informed)

GDPR은 동의 조건으로 정보주체에게 동의에 대한 정보를 제공하는 것(requirement that consent must be informed)을 강조하고 있다. 이를 위해 GDPR에서는 컨트롤러로 하여금 정보주체의 선택을 도울 수 있는 핵심 요소를 알려주도록 규정하고 있는데, 핵심 요소는 최소한 ① 컨트롤러의 신원, ② 동의를 구하는 개별 처리 활동의 목적, ③ 수집 및 이용되는 개인정보 또는 개인정보의 유형, ④ 동의 철회권의 존재, ⑤ 제22조제2항에 따른 프로파일링 등 자동화된 개인정보처리를 바탕으로 한 결정에 사용되는 개인정보에 대한 정보, ⑥ (개인정보 이전에 대한 동의인 경우) 적정성 결정 및 적절한 보호조치가 존재하지 않는 제3국으로의 개인정보 전송에 따라 발생 가능한 위험에 대한 정보의 사항을 포함하여야 한다. 다만 이 중 ① 또는 ⑥에 대한 정보는 개인정보처리방침(Privacy Policy)에 포함되어 제시될 수 있다.

<General Data Protection Regulation>

Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

24) 프로젝트가 시작한 시점 이후 프로젝트의 범위가 지속적으로 또는 통제되지 않은 채 확대되는 현상

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

<GDPR 번역문>

제7조 동의의 조건

1. 처리가 동의를 기반으로 이루어지는 경우, 개인정보처리자는 개인정보주체가 본인의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.

2. 개인정보주체의 동의가 기타의 사안과도 관련된 서면의 진술서로 제공되는 경우, 동의 요청은 그 기타의 사안과 분명히 구별되는 방식으로, 이해하기 쉽고 입수가 용이한 형태로, 명확하고 평이한 문구를 사용한 방식으로 제시되어야 한다. 진술서의 어느 부분이라도 본 규정을 위반하는 경우 그 구속력이 인정되지 않는다.

3. 개인정보주체는 언제든지 본인의 동의를 철회할 권리를 가진다. 동의의 철회는 철회 이전에 동의를 기반으로 한 처리의 적법성에 영향을 미치지 않는다. 개인정보주체는 동의를 제공하기 전에 이 사실에 대해 고지 받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.

4. 동의가 자유롭게 제공되는지 여부를 평가할 때, 무엇보다 서비스 제공 등의 계약의 이행이 해당 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 한다.

㈑ 정보주체의 모호하지 않은 의사표시(Unambiguous indication)

GDPR에서 동의는 동의 조건을 읽었음을 확인하는 것만으로는 부족하며, 명확한 긍정 행위(clear affirmative act)가 있어야 한다. 여기서 명확한 긍정 행위란, 특정한 처리 행위에 대하여 동의를 의식적 행동으로 표시하는 것을 의미한다. 이에 따라 ① 사전에 선택되어 있는 체크박스(pre-ticked boxes)를 제시하는 것, ② 암묵적(silence) 동의나 부작위(inactivity)를 동의로 보는 것, ③ 서비스가 제시하는 절차를 동의 의사 표시 없이 단순히

진행하는 것, ④ 일반적 이용 약관에 포괄적 수용(이른바 'blanket acceptance') 의사를 표현한 것은 동의를 위한 명확한 표시로 인정되지 않을 수 있다. 아울러 동의 철회 방식이 동의 획득 방식과 동일한 수준으로 용이하여야 한다.

가령 동의 문구를 포함하는 이용 약관을 화면에 노출하여 이용자가 이를 연속적으로 내리거나 스크린을 넘기도록(scrolling down or swiping) 하는 것은 동의의 명확성 요건을 충족하지 못할 수 있다. 많은 약관 내용이 연속적으로 노출될 경우 정보주체가 동의 문구를 열람하지 못한 채 화면의 하단까지 이르게 될 수 있기 때문에 충분히 명확한 것으로 볼 수 없기 때문이다.

다만, 이는 '명시적 동의(explicit consent)'와는 다른 개념이다. '명시적 동의'에서 말하는 '명시적'의 개념은 정보주체가 동의를 표현하는 방식을 의미하여, 정보주체가 명확한 의사 표시를 해야 함을 의미한다. '명시적 동의'의 구체적 방법으로는 서면진술이나 동의 의사가 표명된 이메일 발송, 정보주체의 서명이 포함된 스캔 문서의 업로드, 전자서명, 동의에 대한 2단계 검증 등이 있다.

GDPR은 일정한 경우에 대해 명시적 동의를 요구하고 있다. 민감정보의 처리, 역외 이전 시 특정 상황, 프로파일링을 포함한 자동화된 의사결정 등이 그러한 경우이다.[25]

㈐ 동의 제도 위반 시 제재

GDPR 제83조 제5항 (a)에 따라, 동의에 관한 규정을 위반할 경우 최대 2,000만 유로, 기업의 경우 2,000만 유로와 '전년도 전세계 연매출(total worldwide annual turnover of the preceding financial year)'의 최대 4% 중에서 더 높은 금액의 과징금(administrative fines)이 부과될 수 있다. GDPR에 규정된 가장 과중한 처벌이 적용되지만, 형사처벌 대상은 아니다.

㈑ 소결론

전체적으로 유럽연합의 1995년 개인정보보호지침(Data Protection Directive 95/46/ec)과 비교하였을 때 기업 등이 개인정보의 수집 등에 관하여 정보주체의 동의를 얻는 것이 보다 어렵게 되었다고 볼 수 있다. GDPR에서 정보주체는 동의를 하는 것과 마찬가지로 철회를 언제라도 쉽게 할 수 있게 규정되었고, 정보주체와 개인정보처리자 사이에 '중대한 불균형(a significant imbalance)'이 존재하면 동의가 자유로이 주어진 것이 아니어서 그 동의는 개인정보처리의 법적으로 유효한 근거가 되지 못한다. 이 점에서 정보주체의

25) 한국인터넷진흥원, 앞의 가이드북, 54~55면.

동의의 요건이 강화되었다고 볼 수 있다.[26]

(3) 고지사항

GDPR은 개인정보를 수집함에 있어서 어떠한 사항이 정보주체에게 고지되어야 하는지를 정보주체의 권리로서 접근하고 있다. 이는 개인정보보호법이 고지의무를 정보주체의 권리가 아닌 개인정보처리자의 의무로서 접근하는 방식과 다르다. 먼저, 정보주체로부터 개인정보가 수집되는 경우를 규정한 GDPR 제13조에 따라 정보주체는 ① 개인정보처리자의 기관명과 연락처, ② 개인정보보호책임자(data protection officer, 'DPO')의 세부연락처, ③ 개인정보처리의 목적·근거, ④ 개인정보처리자의 정당한 이익(legitimate interests), ⑤ 수령인(recipient) ⑥ 국외이전이 발생하는 경우 적합성 평가 등 국외이전의 근거를 통보받을 권리를 가진다. GDPR 제14조에 따라 정보주체 이외로부터 개인정보를 수집하는 경우에도 개인정보처리자는 상기 제13조에 따른 정보를 제공하여야만 한다.

이때 고지사항인 수령인(recipient)과 관련하여, 컨트롤러는 수령인의 전체 목록 또는 수령인의 유형을 고지할 의무가 있는 것으로 해석된다{(전략)controllers will need to provide a full list of recipients or categories of recipients including processors(후략)}.[27] 이는 후술하는 바와 같은 우리 법의 해석과는 구별되는 점이다.

<General Data Protection Regulation>

Article 13 Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;

26) 위 연구보고서, 78면.

27) Article 29 DATA PROTECTION WORKING PARTY, Guidelines on consent under Regulation (2017. 11. 28.), p. 13; "…Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors."

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the

data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

<GDPR 번역문>

제13조 개인정보가 개인정보주체로부터 수집되는 경우 제공되는 정보

1. 개인정보주체에 관련된 개인정보를 개인정보주체로부터 수집하는 경우, 개인정보처리자는 개인정보를 취득할 당시 개인정보주체에게 다음 각 호의 정보 일체를 제공해야 한다.
(a) 개인정보처리자 또는 해당되는 경우, 개인정보처리자의 대리인의 신원 및 상세 연락처
(b) 해당되는 경우, 개인정보보호 담당관의 상세 연락처
(c) 해당 개인정보의 예정된 처리의 목적뿐 아니라 처리의 법적 근거
(d) 제6조(1)의 (f)호에 근거한 처리의 경우, 개인정보처리자 또는 제3자의 정당한 이익
(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주
(f) 해당되는 경우, 개인정보처리자가 제3국이나 국제기구의 수령인에게 개인정보를 이전할 예정이라는 사실과 집행위원회가 내린 적정성 결정의 유무, 또는 제46조, 제47조, 제49조(1)의 두 번째 단락에 명시된 이전의 경우, 적절하고 적합한 안전조치, 그 사본을 입수하기 위한 수단, 안전조치가 사용 가능하게 되는 경우에 대한 언급

2. 제1항의 정보와 함께, 개인정보처리자는 개인정보가 입수될 때 공정하고 투명한 처리를 보장하는 데 필요한, 다음 각 호의 추가 정보를 개인정보주체에 제공해야 한다.
(a) 개인정보의 보관기간, 또는 이것이 여의치 않을 경우, 해당 기간을 결정하는 데 사용하는 기준
(b) 개인정보처리자에게 본인의 개인정보에 대한 열람, 정정, 삭제를 요구하거나 개인정보주체 본인에 관한 처리의 제한이나 반대를 요구할 권리, 그리고 본인의 개인정보를 이전할 수 있는 권리의 유무
(c) 해당 처리가 제6조(1)의 (a)호나 제9조(2)의 (a)호에 근거하는 경우, 철회 이전에 동의를 기반으로 하는 처리의 적법성에 영향을 주지 않고 언제든지 동의를 철회할 수 있는 권리의 유무
(d) 감독기관에 민원을 제기할 수 있는 권리
(e) 개인정보의 제공이 법정 또는 계약상의 요건이거나 계약 체결에 필요한 요건인지의 여부 및 개인정보주체가 개인정보를 제공할 의무가 있는지의 여부, 그리고 해당 정보를 제공하지 않을 경우 발생할 수 있는 결과
(f) 제22조(1) 및 (4)에 규정된 프로파일링 등, 자동화된 의사결정의 유무. 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 그 같은 처리가 개인정보주체에 미치는 중대성 및 예상되는 결과

3. 개인정보처리자가 개인정보를 수집한 목적 외로 추가 처리할 예정인 경우, 개인정보처리자는 추가 처리 이전에, 개인정보주체에게 해당하는 기타 목적에 관한 정보와 제2항의 관련 추가 정보 일체를 제공해야 한다. 4. 개인정보주체가 이미 관련 정보를 보유하고 있는 경우, 제1항, 제2항 및 제3항은 적용되지 않는다.

나. 독일 연방개인정보보호법(BDSG)

유럽연합의 GDPR이 제정됨에 따라 유럽연합 회원국에서는 2017년에 독일이 처음으로 GDPR을 반영하여 신속하게 연방개인정보보호법(Bundesdatenschutzgesetz, 이하 'BDSG')을 전면 개정했다. BDSG는 크게 GDPR이 그대로 적용되는 영역에 관하여 세부적인 시행 방법을 규정한 부분과, 입법재량이 있는 영역에 관한 부분으로 나뉜다. 그 중 동의 제도와 관련하여 BDSG는 과거 방식과는 달리 정보주체의 동의에 대해 별도 조문 없이 GDPR을 직접 적용하는 방식으로 법 개정이 이루어졌다. 즉, 개정 BDSG의 GDPR 이행 규정인 제2장(Part 2 : Implementing provisions for processing for purposes in accordance with Article 2 of Regulation (EU) 2016/679)의 제22조~제44조에는 GDPR의 동의와 관련된 개념규정이 따로 존재하지 않는다. 그리고 BDSG 제51조에서는 동의의 요건을 규정하고 있는데 이는 사실상 GDPR 제7조와 큰 차이를 보이고 있지 않다.[28]

<Bundesdatenschutzgesetz> (Federal Data Protection Act)	<General Data Protection Regulation>
Section 51 Consent	*Article 7 Conditions for consent*
(1) If personal data may be processed by law on the basis of consent, the controller must be able to present evidence of the data subject's consent.	1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
(2) If the data subject's consent is given in the context of a written declaration	2. If the data subject's consent is given in the context of a written declaration which

28) 홍선기, 일반개인정보보호규정(GDPR) 발효에 따른 독일 개인정보보호법제의 입법동향 및 시사점, 정보법학 제22권 제1호, 2018, 176-188

which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.	also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
(3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The data subject shall be informed of this before giving consent.	3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.
(4) Consent shall be effective only when based on the data subject's free decision. When assessing whether consent was freely given, the circumstances in which it was given must be taken into account. The data subject shall be informed of the intended purpose of the processing. If necessary in the individual case or on request, the data subject shall also be informed of the consequences of withholding consent.	4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
(5) If special categories of personal data are to be processed, the consent must explicitly refer to these data.	

다. 미국 캘리포니아주 소비자프라이버시법(CCPA)

미국에서는 캘리포니아주에서 2018년 '캘리포니아주 소비자프라이버시법(California Consumer Privacy Act, 이하 'CCPA')이 제정되어 2020년 1월 1일부터 시행될 예정인데, 이는 미국 연방의 모든 주를 통틀어 최초로 제정된 포괄적 형태의 일반 데이터 보호법이

라는 데 의미가 있다.[29]

CCPA의 적용 대상 사업자[30]는 수집, 공유 및 판매된 개인정보를 추적하고, 이를 개인정보취급방침에 명시하며, 소비자의 요구에 따라 개인정보처리내역을 통지해야 한다. 또한 소비자의 본인 개인정보에 대한 접근권한을 보장해야 하며, 소비자가 개인정보 삭제 요청 시 일정한 예외적인 경우를 제외하고 반드시 해당 정보를 삭제해야 한다. 특히 데이터의 판매 및 재판매와 관련하여 소비자가 본인의 개인정보 판매행위를 금지할 수 있도록 "나의 개인정보를 판매하지 마십시오(Do Not Sell My Personal Information)"란 웹기반 옵트아웃 도구와 프로그램을 마련해야 한다.[31][32] 그리고 소비자가 이러한 권리를 갖

---

29) 최창수, 미국의 빅데이터 이용 활성화와 개인정보 보호, 법조 제68권 제3호, 2019, 481면.

30) 캘리포니아 주 민법 1798. 140. 참조.

① 미국 캘리포니아 주에서 사업을 영위하면서 다음 (A),(B),(C) 중 하나 이상의 한도를 충족하는 자로서, 주주나 기타 소유자의 이익이나 재정적 혜택을 위해서 구성 또는 운영되고, 소비자의 개인정보를 수집하거나 그러한 정보가 대신해서 수집되고, 단독 또는 타인과 공동으로, 소비자의 개인정보처리 목적과 방법을 결정하는 개인 소유 회사, 조합, 유한책임회사, 법인, 협회 또는 기타 법적 실체

(A) 연간 총 매출이 미화 2천5백만 달러를 초과하는 자

(B) 단독으로 또는 결합해서, 50,000건 이상의 소비자, 가구 또는 장치의 개인정보를 매년 구매하거나, 사업자의 상업적 목적으로 수령하거나, 판매하거나 상업적 목적으로 공유하는 자.

(C) 연간 총 매출의 50% 이상을 소비자의 개인정보 판매에서 얻는 자

② 위의 ①에서 정의된 사업자를 지배(control)하거나 이러한 사업자에 의해서 지배를 받고, 그러한 사업자와 공동으로 브랜드 사용(Common branding)을 공유하는 여하한 실체

((1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.)

해당 내용에 대해 더 자세한 사항은 한국인터넷진흥원, 2018년 해외 개인정보보호 동향 분석, 161면 참조.

31) 최창수, 앞의 논문, 485~488면.

32) 17989. 135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

는다는 내용을 소비자에게 고지할 의무가 있다.

요컨대 CCPA에서는 개인정보 수집 · 이용 · 제공 시 정보주체의 동의를 요하기보다는 삭제 요구권과 판매 금지권을 통해 정보주체, 즉 소비자가 '옵트아웃(opt-out)'을 할 수 있는 방식으로 구성되어 있다.[33] 다만, 사업자가 16세 미만으로부터 수집한 개인정보를 판매하고자 하는 경우에는 옵트인 동의(opt-in consent)가 필요한데, 13세 미만의 경우 부모나 후견인의 동의가, 13세 이상 16세 미만의 경우 본인의 동의가 필요하다.[34]

라. 일본 개인정보의 보호에 관한 법률

(1) 일본 개인정보보호 법제에서의 동의 제도

일본의 개인정보의 보호에 관한 법률(이하 '개인정보보호법')은 2003년 제정 이후 별다른 개정이 없다가, 2015년에 대대적으로 개정되었다. 일본은 ① 본인 동의가 없어도 데이터를 활용 가능하도록 하는 구도를 도입, ② 기본적인 제도 틀과 이것을 보완하는 민간의 자주적인 조직 활용, ③ 제3자 기관의 체제정비 등에 의한 실효성 있는 제도 집행 확보를 세 가지 포인트로 삼아 개정 작업에 착수했고[35] 그 결과 '익명가공정보' 개념의 도입, '요배려 개인정보(우리 법의 민감정보와 유사)'의 옵트아웃(opt-out) 대상 완전 제외, 개인정보보호위원회의 강화 등을 골자로 하는 개정 개인정보보호법이 통과되었다.

그 중 동의 제도에 한하여 소개하면, 일본의 개인정보보호법은 우리 법과 달리 개인정보취급사업자[36]가 개인정보를 수집 · 이용할 경우 원칙적으로 정보주체의 동의를 필요로 하지 않는다. 즉, 일본 개인정보보호법은 허위 기타 부정한 수단에 의한 취득을 금지하고 있을 뿐이므로 수집 · 이용은 원칙적으로 허용된다고 볼 수 있다. 다만 2015년 개정으로 '요배려 개인정보(우리 법의 민감정보와 유사)'에 한하여 취득 시 정보주체의 사전

---

33) 1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

34) 1798.120. (c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

35) 손형섭, 일본 개정 개인정보보호법과 우리법의 나아갈 방향, 공법연구 제46집 제2호, 한국공법학회, 2017, 300면.

36) 일본의 법률에서는 개인정보 "취급"에 대한 정의가 없다. 일반적으로 여기서 말하는 "취급"은 개인정보의 수집부터 처리(편집·가공) 제공 등까지 모두를 포함하는 것으로 이해되고 있으며, 일본의 개인정보취급사업자는 GDPR의 컨트롤러와 프로세서를 모두 포함하는 개념으로 이해되고 있다. 일본의 개인정보취급사업자는 개인정보를 데이터베이스 등을 사업용으로 사용하기만 하면 인정된다. 손형섭 · 최성락 · 박은지 · 최지수, 일본의 개인정보보호 법제 · 정책 분석에 관한 연구, 개인정보보호위원회 연구보고서, 2017, 38면

동의를 받게 되었다.

요컨대 일본 개인정보보호법은 정보주체의 동의가 없이도 개인정보를 일반적으로 수집 · 이용할 수 있는 것이 원칙이라는 해석이 가능하다.[37] 다만 일본 개인정보보호법에서는 본인에게 이용목적을 특정하여 취득하고(제15조), 미리 본인의 동의를 얻어야만 제15조의 규정에 의해 특정된 이용목적의 달성의 범위를 넘어 개인정보를 취급할 수 있으며(제16조), 제17조 제1항에서는 개인정보취급사업자는 허위 기타 부정한 수단에 의해 개인정보를 취득하여서는 아니된다고 규정하고 있다는 이유에서, 위와 같은 해석은 부적절하며 오해를 유발할 수 있다는 견해도 있다.[38]

즉, 일본 개인정보보호법은 개인정보 처리에 관한 전 과정('취급')에서 특정된 이용목적을 준수해야 하고, 이용목적을 넘어서 개인정보를 처리하려는 경우에는 정보주체의 동의를 받도록 하고 있다. 우리 법과 비교하자면, 개인정보 수집 · 이용 동의는 규정되어 있지 않으나 목적 외 이용 동의는 규정되어 있는 것이다.

한편, 일본 개인정보보호법상 '동의'는 "해당 본인임을 확인할 수 있는 것을 전제"로 하여 "본인의 개인정보를 개인정보취급사업자의 취급방법으로 취급될 것을 승낙하는 취지의 해당 본인의 의사표시"를 의미하고, 이는 "본인의 승낙하는 취지의 의사표시를 해당 개인정보취급사업자가 인식하는 것, 즉 사업의 성격 및 개인정보취급 상황에 따라 본인이 동의에 관한 판단을 위해 필요하다고 생각되는 합리적이고 적절한 방법에 의하여야" 한다고 해석된다.[39] 이에 따라 ① 구두에 의한 의사표시, ② 서면(전자적 기록 포함) 수령, ③ 메일 수신, ④ 확인 란 체크, ⑤ 홈페이지에서의 버튼 클릭, ⑥ 음성 입력, 터치 패널 터치 버튼, 스위치 등에 의한 입력 등이 모두 '본인의 동의를 얻은 경우'에 해당한다고 해석된다.[40]

<일본 개인정보보호법 번역문[41]>

제15조(이용목적의 특정) ① 개인정보취급사업자는 개인정보를 취급함에 있어서 그 이용의 목적(이하 "이용목적"이라 한다)을 가능한 한 특정하여야 한다.
② 개인정보취급사업자는 이용목적을 변경하는 경우에는 변경전의 이용목적과 상당한 연관성

37) 김은수 · 정종구, 2015년 일본 개인정보보호법의 개정 - 개정된 주요 내용과 시사점, YGBL 제8권 제1호, 2016, 125면.
38) 손형섭, 앞의 논문, 305면.
39) 個人情報保護委員会, 個人情報の保護に関する法律についてのガイドライン（通則編）, 平成31年, p. 24. "「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提となる。）。また、「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。(중략)"
40) 위 가이드라인, p. 24.

이 있다고 합리적으로 인정되는 범위를 초과해서 변경하여서는 아니된다.

제16조(이용목적에 의한 제한) ① 개인정보취급사업자는, 미리 본인의 동의를 얻지 않고서는, 전조의 규정에 의해 특정된 이용목적의 달성에 필요한 범위를 넘어서 개인정보를 취급하여서는 아니된다.
② 개인정보취급사업자는, 합병 기타의 사유에 의해 다른 개인정보취급사업자로부터 사업을 승계함에 따라 개인정보를 취득한 경우에는, 미리 본인의 동의를 얻지 않고서는, 승계 이전의 당해 개인정보의 이용목적의 달성에 필요한 범위를 넘어서 당해 개인정보를 취급하여서는 아니된다.
③ 전 2항의 규정은 다음 각호의 1에 해당하는 경우에는 적용하지 아니한다.
1. 법령에 근거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우
4. 국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 줄 우려가 있는 경우.

제17조(적정한 취득) ① 개인정보취급사업자는 허위 기타 부정한 수단에 의해 개인정보를 취득하여서는 아니된다.
② 개인정보취급사업자는, 다음에 열거하는 경우를 제외하고는, 사전에 본인의 동의를 얻지 않으면 '배려를 요하는 개인정보'(要配慮개인정보)를 취득하여서는 아니된다.
1. 법령에 의거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
4. 국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 法令이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻게 되면 당해 사무의 수행에 지장을 초래할 우려가 있는 때
5. 당해 요배려개인정보가 본인, 국가기관, 지방자치단체, 제76조 제1항 각 호에 열거된 자 및 그밖에 개인정보보호위원회규칙으로 정하는 자에 의해 공개되고 있는 경우
6. 그밖에 전 각 호에 열거된 경우에 준하는 것으로서 政令으로 정하는 경우

(2) 개인정보 제3자 제공의 제한

일본 개인정보보호법은 개인정보 제3자 제공의 경우 정보주체의 사전 동의를 원칙으

41) 이인호, 일본 개인정보보호법 번역, 개인정보보호위원회의 번역문을 참조하였음. 이하 동일함.

로 하고 있다. 그러나 일정한 요건을 갖춘 경우 사전 동의를 받지 않는, 옵트아웃 방식의 제3자 제공이 가능하다는 점에서 우리 법과 차이가 있다. 즉, 개인정보취급사업자는 제3자에게 제공되는 개인정보(요배려 개인정보를 제외)에 대하여 본인의 요청이 있는 때에 해당 본인의 식별이 가능한 개인정보의 제3자 제공을 정지하는 것으로 하고 있는 경우에, ① 제3자 제공을 이용목적으로 한다는 점, ② 제3자에게 제공되는 개인정보의 항목, ③ 제3자 제공의 방법, ④ 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인정보의 제3자 제공을 정지한다는 점, ⑤ 본인의 요청을 접수하는 방법 등에 대하여 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있으면서 개인정보보호위원회에 신고한 때에는 해당 개인정보를 제3자에게 제공할 수 있다(제23조 제2항).

<일본 개인정보보호법 번역문>

제23조(제3자제공의 제한) ① 개인정보취급사업자는, 다음 각 호의 어느 하나에 해당하는 경우를 제외하고, 미리 본인의 동의를 얻지 않고서는 개인데이터를 제3자에게 제공하여서는 아니 된다.
1. 법령에 근거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
4. 국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 줄 우려가 있는 때

② 개인정보취급사업자는 제3자에게 제공되는 개인데이터(요배려개인정보를 제외한다. 이하 이 항에서 동일하다)에 대하여, 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지하는 것으로 하고 있는 경우에, 다음에 열거하는 사항에 대하여, 개인정보보호위원회규칙에서 정하는 바에 따라 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있으면서 개인정보보호위원회에 신고한 때에는, 전항의 규정에 불구하고, 당해 개인데이터를 제3자에게 제공할 수 있다.
1. 제3자 제공을 이용목적으로 한다는 점
2. 제3자에게 제공되는 개인데이터의 항목
3. 제3자 제공의 방법
4. 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지한다는 점
5. 본인의 요청을 접수하는 방법

③ 개인정보취급사업자는, 전항 제2호, 제3호 또는 제5호에 열거한 사항을 변경하는 경우에는, 변경하는 내용에 대해 개인정보보호위원회규칙에서 정하는 바에 따라 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있으면서 개인정보보호위원회에 신고하여야 한다.

④ 개인정보보호위원회는, 제2항의 규정에 의한 신고가 있는 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 당해 신고에 관한 사항을 공개하여야 한다. 전항의 규정에 의한 신고가 있는 때에도 동일하다.

⑤ 다음에 열거하는 경우에는, 당해 개인데이터의 제공을 받는 자는 앞의 각 항의 규정의 적용에 있어서 제3자에 해당하지 않는 것으로 한다.
1. 개인정보취급사업자가 이용목적의 달성에 필요한 범위 내에서 개인데이터의 취급의 전부 또는 일부를 위탁하는 경우에 그에 수반하여 당해 개인데이터가 제공되는 경우
2. 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인데이터가 제공되는 경우
3. 특정한 자와의 사이에서 공동으로 이용하는 개인데이터가 당해 특정한 자에게 제공되는 경우로서, 그 취지 및 공동으로 이용되는 개인데이터의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인데이터의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때

⑥ 개인정보취급사업자는, 전항 제3호에서 규정하는 이용하는 자의 이용목적 또는 개인데이터의 관리에 대해 책임을 지는 자의 성명 혹은 명칭을 변경하는 경우에, 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다.

또한, 일본 개인정보보호법은 우리 법과는 달리 개인정보 제3자 제공 시 정보주체에게 고지해야 하는 사항에 대해 구체적으로 규정하고 있지 않고, 단지 “미리 본인의 동의를 받을 것”만을 요건으로 하고 있다. 대신, 2015년 개정으로 제3자 제공에 관한 기록 및 확인 의무가 도입되었다. 즉, 개인정보취급사업자는 개인정보 제3자 제공을 한 경우 원칙적으로 제공 연월일, 제공받는 자의 이름 또는 명칭 등에 관한 기록을 작성해야 하며, 제공받는 개인정보취급사업자 역시 원칙적으로 제공하는 자의 이름 또는 명칭, 주소, 대표자 및 그 경위를 확인하고 이에 관한 기록을 작성해야 한다.

<일본 개인정보보호법 번역문>

제25조(제3자 제공에 관한 기록의 작성 등) 개인정보취급사업자는, 개인데이터를 제3자(제2조 제5항 각 호에 열거된 자를 제외한다. 이하 이 조 및 다음 조에서 동일하다)에게 제공한 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 당해 개인데이터를 제공한 연월일, 당해 제3자의 이름 또는 명칭 및 그밖에 개인정보보호위원회규칙에서 정하는 사항에 관한 기록을 작

성하여야 한다. 다만, 당해 개인데이터의 제공이 제23조 제1항 각 호 또는 제5항 각 호의 어느 하나(前條의 규정에 의한 개인데이터의 제공에 있어서는, 제23조 제1항 각 호의 어느 하나)에 해당하는 경우에는, 그러하지 아니하다.

제26조(제3자 제공을 받는 시점에서의 확인 등) ① 개인정보취급사업자는, 제3자로부터 개인데이터의 제공을 받을 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 다음에 열거하는 사항을 확인하여야 한다. 다만, 당해 개인데이터의 제공이 제23조 제1항 각 호 또는 제5항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 당해 제3자의 이름 또는 명칭 및 주소 그리고 법인에 있어서는 그 대표자(법인이 아닌 단체에서 대표자 또는 관리인이 있는 경우 그 대표자 또는 관리인)의 이름
2. 당해 제3자에 의한 당해 개인데이터의 취득의 경위
② 前項의 제3자는, 개인정보취급사업자가 同項의 규정에 의한 확인을 하려고 하는 경우에, 그 개인정보취급사업자에 대해 당해 확인에 관한 사항을 속여서는 아니된다.
③ 개인정보취급사업자는, 제1항의 규정에 의한 확인을 한 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 당해 개인데이터의 제공을 받은 연월일, 당해 확인에 관한 사항 및 그밖에 개인정보보호위원회규칙으로 정하는 사항에 관한 기록을 작성하여야 한다.
④ 개인정보취급사업자는, 前項의 기록을, 당해 기록을 작성한 날부터 개인정보보호위원회 규칙으로 정하는 기간 동안 보존하여야 한다.

(3) 형사처벌 조항

종래 일본의 개인정보보호법에는 개인정보의 침해행위를 직접 처벌하는 규정은 존재하지 않았다. 2015년 개정으로 개인정보취급사업자 등이 자기 또는 제3자의 부정한 이익을 취할 목적으로 개인정보 데이터베이스 등을 제공 또는 도용하는 행위를 직접 처벌하는 '데이터베이스 제공죄'가 신설되었을 뿐이다.[42] 후술하는 바와 같이 정보주체의 동의 없이 개인정보를 처리하는 경우 형사처벌까지 가능한 경우가 많은 우리 법과는 큰 차이가 있다.

(4) 정보은행 산업

일본에서 제공되고 있는 '정보은행' 서비스란, 개인과 데이터 활용에 관한 계약 등에 기반하여 PDS 등의 시스템을 활용하여 개인 데이터를 관리하고, 개인의 지시 또는 미리 지정한 조건에 따라 개인을 대신하여 타당성을 판단한 후, 데이터를 제3자(다른 사업자)에게 제공하는 사업[43]이다. 정보주체는 정보은행 사업자에게 정보제공의 기준을 제시하

42) 박강우, 일본에서 개인정보의 형법적 보호, 강원법학 제55권, 강원대학교 비교법학연구소, 2018, 34면.
43) 한국인터넷진흥원, 해외 개인정보보호 동향 보고서(2018년 6월 2주), 2면

고 정보은행 사업자가 제3자에게 정보주체의 정보를 제공할 것을 결정하는 구조라고 할 수 있다. 일본은 2018. 5. 12. 총무성과 경제산업성에서 '정보 신탁 기능의 인정에 관한 지침 초안'을 발표하는 등 정보은행 산업을 장려하고 있는데, 정보은행 산업은 마이데이터 산업과 유사하면서도 일본의 사회 및 법제도의 특징이 반영된 것이라고 할 수 있다.

2. 국내 법제도 현황 분석

가. 국내 개인정보처리에 대한 동의 제도의 현황

국내 정보보호 법체계에서 동의 제도는 개인정보자기결정권을 가장 직접적이고 구체적으로 구현해주는 제도이다. 개인정보처리자는 원칙적으로 정보주체의 동의가 있어야 개인정보를 처리(수집 · 이용 · 제공 등)할 수 있으며, 정보주체의 동의를 위해 정보주체에게 관련 내용을 충실히 알려야 하고, 정보주체의 동의는 사전에 명시적, 개별적으로 받아야 한다.[44]

나. 동의 원칙

정보통신망법은 개인정보 수집 · 이용 · 제공 및 위탁에 관하여 정보주체의 동의를 받을 것을 원칙으로 하고 있으며 몇 가지 예외를 두고 있다. 가령 개인정보의 수집 이용 동의에 관한 정보통신망법 제22조는 제1항에서 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우에는 법정 고지사항을 알리고 동의를 받아야 한다고 규정하고, 제2항에서 동의 예외사유를 정하고 있다. 한편 개인정보보호법은 개인정보 수집 · 이용 · 제공이 가능한 경우로 정보주체의 동의를 포함하여 다른 법률의 특별한 규정 등 여러 사항[45]을 두고 있으나 원칙적으로 정보주체의 동의를 받아야 하는 점은 동일하다고 해석된다. 그리고 동의가 원칙이기 때문에 동의 예외사유는 엄격하게 해석된다.

법제처 역시 개인정보보호법 제17조 제1항 등의 '다른 법률에 특별한 규정이 있는 경

---

44) 권영준, 앞의 논문, 696~698면.

45) 개인정보보호법 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

우'에 해당하는지 여부는 엄격하게 해석해야 하므로 "'다른 법률에 특별한 규정이 있는 경우'란 다른 법률에서 개인정보의 목적 외 용도로의 이용 또는 제3자 제공 등에 관하여 구체적으로 허용하고 있는 경우를 의미한다고 보아야 한다."라며 '다른 법률의 특별한 규정'이 되기 위해서는 "해당 규정이 개인정보보호법에서 정한 내용과 다른 사항을 구체적으로 명시하고 있어야 할 것"[46]이라고 일관되게 엄격하게 해석하고 있다.

또한, 개인정보 동의를 받지 않아도 되는 경우에 관하여 개인정보보호법과 정보통신망법의 규정이 통일되어 있지 않으며 각각의 법에서도 수집 · 이용과 제3자 제공 등 처리 유형에 따라 예외 사항이 다르다. 예를 들면, 개인정보보호법 제15조 제1항 제4호에 따라 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우는 개인정보 수집 · 이용 시 동의를 받지 않아도 되는 예외 사유에 해당하지만 동법 제17조 제1항 제2호에는 포함되어 있지 않아 제3자 제공 시에는 동의를 받아야 한다. 또한 위 사유는 정보통신망법에서는 동의 예외사유로 규정되어 있지 않다.

다. 법정 고지사항

우리 법은 개인정보처리자로 하여금 정보주체로부터 동의 받을 때 고지 의무를 규정하고 있다. 가령, 개인정보보호법 제15조 제2항에 따르면 개인정보 수집 · 이용 시에는 (i) 개인정보 수집 · 이용 목적, (ii) 수집하려는 개인정보의 항목, (iii) 개인정보의 보유 및 이용 기간, (iv) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 고지하여야 한다.

또한 고지하는 방법도 법령에 정해져 있다. 개인정보보호법 제22조 제2항에 따르면, 개인정보처리자가 정보주체로부터 동의를 받을 때 중요한 내용은 명확하게 표시하여 알아보기 쉽게 하여 동의를 받아야 한다. 개인정보보호법 시행령 제17조 제2항에 따르면 위 '중요한 내용'이란, 개인정보의 수집 · 이용 목적, 수집 · 이용하려는 개인정보의 항목, 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실, 처리하려는 개인정보의 항목 중 민감정보 및 고유식별정보의 사항, 개인정보의 보유 및 이용 기간, 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적을 말한다. 동 시행규칙에서는 글씨 크기에 관한 의무까지 규율하고 있다.[47]

정보통신망법에는 위와 같은 내용이 구체적으로 규정되어 있지 않으나, 법정 고지사항

46) 법제처 2014. 10. 14. 회신 14-0621, 법제처 2019. 9. 6. 회신 19-0018 해석례, 법제처 2018. 4. 16. 회신 18-0124 해석례, 법제처 2017. 12. 4. 회신 17-0506 해석례 등

47) 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하고 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시하며 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시하도록 함(개인정보보호법 시행규칙 제4조).

은 쉽고 명확하게 이해가 될 수 있도록 기재되어야 하는 점은 동일하다. 특히 방송통신위원회는 온라인 개인정보처리 가이드라인을 발표하여 "'법정 고지사항'만을 간결하게 고지하고, 일반인이 이해할 수 있을 정도의 '쉬운 용어'를 사용하도록 하며, '중요내용은 부호, 색채, 굵고 큰 문자 등'을 활용하여 명확하게 표시해야 하고, 불가피하게 전문용어를 사용하는 경우에는 별도의 용어 설명을 제공"[48]하여야 한다고 안내하고 있다.

한편, 개인정보 제3자 제공의 경우 '정보를 제공받는 자'에 대해 고지할 의무가 있는데, 이른바 '유형고지'는 허용되지 않는 것으로 해석된다. 즉, 행정안전부는 '정보를 제공받는 자'란, 제공받는 자의 이름 또는 상호를 의미하며 '금융기관', '정부기관' 등과 같이 제공받는 자를 알기 어렵도록 포괄적으로 알려서는 안 되고 제공받는 자가 여러 명일 경우에는 각각의 이름 또는 상호를 알려야 한다는 입장이다.[49] 표준 개인정보 보호지침 제7조 제3항[50] 역시 같은 내용을 규정하고 있다. 정보통신망법도 마찬가지로 해석되며 실무상 제공받는 자가 너무 많은 경우에는 링크를 누르면 별도 화면에 제공받는 자가 열거되는 방식으로 구현되고 있다. 개인정보 처리업무 위탁 시 정보통신망법 제25조 제1항에 따라 정보주체의 동의를 받으면서 '수탁자'를 고지하는 경우에도 위와 같다.

라. 사전 · 명시 · 구분 동의

(1) 사전 동의

우리 법의 동의 제도가 사전 동의를 전제로 하고 있다는 점에는 이론이 없다. 개인정보보호법은 제15조 제1항 제1호, 제17조 제1항 제1호 등에서 정보주체의 동의를 '받은' 경우 개인정보를 수집 · 이용 · 제공할 수 있다고 규정하고 있고, 이를 구체화한 표준 개인정보 보호지침 제6조 제2항 제1호는 '정보주체로부터 사전에 동의를 받은 경우'라고 규정하고 있다.

또한 동법 제15조 제1항 제5호는 동의 예외 사유로 '(전략) 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우'를 규정하고 있다. 정보통신망법의 경우 명확하게 사전 동의를 규정하고 있는 것은 아니지만, 달리 볼 근거는 없다. 즉, 동법 제22조 제1항은'이용하려고 수집하는 경우', 제24조의2 제1항은 '제공하려면' 이용자의 동의를 받으라고 규정하고 있다. 실제로 인터넷상에서 회원가입 등 정보처리 시 이용자의 동의는 모두 사전에 이루어

48) 방송통신위원회, 온라인 개인정보처리 가이드라인, 2018, 22면.
49) 행정안전부, 앞의 해설서, 92면.
50) 제7조(개인정보의 제공) ③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

지고 있다. 후술하는 바와 같이 방송통신위원회 및 한국인터넷진흥원의 입장도 같다.

(2) 명시적 동의

일반적으로 우리 법상 개인정보처리에 대한 동의는 묵시적 동의가 아닌 명시적 사전 동의를 요구하는 것으로 인식되고 있다.[51] 특히 개인정보보호법[52]이나 정보통신망법 시행령[53]에서 규정한 방식으로 명시적 동의를 요구하고 있다.

행정안전부 역시 해설서를 통해 "(개인정보보호법) 제22조에서 규정한 방식에 따라 동의를 받아야 하기 때문에 이 법에서 정보주체의 동의는 명시적 동의를 의미한다."[54]라고 설명하고 있으며 방송통신위원회와 한국인터넷진흥원 역시 "이용자로부터 개인정보를 수집할 때에는 수집 시점(회원 가입, 서비스 가입 등) 이전에 이용자가 ① 수집 · 이용 목적, ② 수집하는 개인정보의 항목, ③ 개인정보의 보유 및 이용기간 등 3가지 사항을 명확히 인지하고 명시적으로 동의할 수 있는 절차를 마련해야"[55] 한다는 입장을 밝히고 있다.[56]

(3) 구분 동의

또한 우리 법의 동의 제도는 구분 동의를 원칙으로 하고 있다.

개인정보보호법 제22조 제1항은 동법에 따른 개인정보의 처리에 대하여 정보주체 또는 그 법정대리인의 동의를 받을 때에는 각각의 동의 사항을 구분하여 동의받을 것을 규정하고 있다. 정보통신망법 역시 제24조의2 제3항에서 개인정보 수집 · 이용 동의와 제공 동의 및 위탁 동의는 구분하여 받도록 규정하고 있다. 원치 않는 제3자 제공 및 취급위탁에 동의해야만 서비스 가입이 가능한 경우가 빈번하게 발생하여 이용자의 개인정보 자기결정권이 사실상 제한되는 문제점을 해결하기 위한 것이 그 입법 취지이다.[57] 즉, 개인정보처리자는 정보주체에 대하여 동의 사항을 구분하여 알리고 각각의 동의를 받아야

51) 이창범, 개인정보보호법, 법문사, 2012, 122면.
52) 개인정보보호법 제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.
53) 정보통신망법 시행령 제12조(동의획득방법) ① 정보통신서비스 제공자 등이 법 제26조의2에 따라 동의를 얻는 방법은 다음 각 호의 어느 하나와 같다. 이 경우 정보통신서비스 제공자 등은 동의를 얻어야 할 사항(이하 '동의 내용'이라 한다)을 이용자가 명확하게 인지하고 확인할 수 있도록 표시하여야 한다.
54) 행정안전부, 개인정보보호 법령 및 지침 고시 해설, 2016, 72면.
55) 방송통신위원회 · 한국인터넷진흥원, 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서, 2012, 26면.
56) 다만 대법원은 스스로 공개한 개인정보에 대하여는 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 묵시적 동의를 인정하고 있다. 대법원 2016. 8. 17. 선고 2014다235080 판결.
57) 위 해설서, 62면.

한다는 것이다. 이에 대해 방송통신위원회는 선택동의 사항 없이 필수동의로만 구성되어 있는 경우에는 일괄동의 기능을 운영하는 것이 가능하다는 입장이나[58] 선택동의는 개별적으로 선택할 수 있게 하여야 한다고 설명하고 있다. 또한 일괄동의 기능을 운영하는 경우에도 개인정보 수집 및 이용에 대한 동의란과 개인정보 제3자 제공 동의란은 별도로 만들어 두는 것으로 운영되는 것이 보다 일반적인 것으로 보인다.

그 뿐 아니라, 개인정보보호법은 특히 정보주체가 좀 더 신중한 의사결정을 해야 할 필요가 있는 사항에 대해서는 동의의 내용과 의미를 명확하게 인지한 상태에서 동의 여부를 결정할 수 있도록 통상의 동의와 구분해서 별도의 동의를 받도록 하고 있다. 이때에도 개인정보처리자는 정보주체가 다른 개인정보처리의 목적과 별도로 동의여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다. 예컨대, 고유식별정보를 수집할 때에는 '고유식별정보 수집·이용·제공에 대한 동의'를, 건강에 관한 정보를 수집할 때에는 '민감정보 수집·이용·제공에 대한 동의'를 별도로 분리해서 목적 등을 고지하고 동의를 받아야 한다.[59]

참고로 신용정보법 제32조 제1항 본문은 개인신용정보 제공 동의에 대하여 "신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다"고 규정하고 있다. 동조 단서에서 "다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다"는 예외를 규정하고 있기는 하지만, 원칙적으로는 제공할 때마다 미리 개별 동의를 받아야 한다는 매우 엄격한 입법태도를 취하고 있는 것이다.

마. 변경 시 동의와 필수적 · 선택적 동의 사항

개인정보처리자는 정보주체의 동의를 받았을 때 정보주체에게 고지했던 법정 고지사항이 변경되는 경우에도 다시 동의 받을 의무가 있다.[60] 변경하는 사항이 처리되는 개인정보의 항목에 해당하고 변경 항목이 다수에 해당하는 경우라면 변경보다는 신규 처리에 가까우므로 재동의를 받을 필요가 있다고 볼 여지도 있지만, 처리하는 개인정보 항목이 조금만 변경되거나 처리 목적이나 보유 기간 등이 사소하게 변경되는 경우에도 다시 동의를 받아야 하는 것으로 해석되는 경우가 많다는 점에서 실무적으로 상당한 부담이 된

58) 방송통신위원회, 온라인 개인정보처리 가이드라인, 2018, 25면.
59) 행정안전부, 앞의 해설서, 129~130면.
60) 개인정보보호법 제15조 제2항 후단, 제17조 제2항 후단, 정보통신망법 제22조 제1항 후단, 제24조의2 제1항 후단 등.

다. 이와 관련하여 행정안전부는 “정보주체의 동의가 필요한 개인정보는 장래에 변경이 가능하다는 점에서 정부주체가 동의할 시점에서 확정한 동의를 받아야 할 항목을 모두 열거하고 그 외 이에 준하거나 유사한 항목을 포섭하는 의미로 ‘등’의 용어를 사용하는 것이 허용되는지”에 대해 “「개인정보보호법」은 개인정보 수집시 필요 최소한의 개인정보만을 수집하도록 하고 있으며, ‘등’의 용어를 써서 추가적인 개인정보를 받을 수 있도록 한다면 무분별한 개인정보 수집으로 이어질 소지가 있으므로 정보주체 동의시 수집할 구체적인 개인정보 항목을 나열하면서 ‘등’을 써서는 안 되며, 추후 업무상 새로운 개인정보가 필요한 경우 별도로 동의를 얻어야 한다.”고 보고 있어 매우 엄격한 입장을 취하고 있다.[61]

또한 우리 법은 필수적 · 선택적 동의 사항을 구별하고 있다. 개인정보보호법 제22조 제5항은 정보주체가 선택적 동의 사항에 동의를 하지 않는다는 이유로 개인정보처리자가 정보주체에게 재화 또는 서비스 제공을 거부할 수는 없다고 한다.[62] 특히 신용정보법은 개인정보의 제3자 제공에 관한 제32조에서 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다고 규정하면서, 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다고 규정하고 있다(제4항). 아울러 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 안 된다고 규정하고 있다(제5항).[63]

바. 정보통신망법의 개인정보 처리위탁 동의

개인정보보호법상 개인정보의 처리위탁은 정보주체의 동의를 요하지 않는다. 그러나 정보통신서비스 분야의 경우는 다르다. 정보통신망법은 일정한 예외(정보통신서비스의 제

61) 행정안전부, 앞의 해설서, 84면.

62) 정보통신서비스 분야에도 위 내용이 적용될 것으로 보인다. 정보통신망법 제23조 제3항은 “정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다.”고 규정하고 있다. 방송통신위원회 · 한국인터넷진흥원, 앞의 해설서, 71~72면 참조. 또한 정보통신망법 제50조에 따라 영리목적 광고성 정보 전송, 이른바 ‘스팸’에 대한 수신 역시 선택적 동의 사항이다.

63) 신용정보법 시행령은 신용정보회사등이 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하는 경우에는 “1. 신용정보주체가 그 동의사항에 대하여 동의하지 아니하면 그 신용정보주체와의 금융거래 등 상거래관계를 설정·유지할 수 없는지 여부, 2. 해당 신용정보주체가 그 동의사항에 대하여 동의함으로써 제공·활용되는 개인신용정보가 신용정보회사등과의 상거래관계에 따라 신용정보주체에게 제공되는 재화 또는 서비스(신용정보주체가 그 신용정보회사등에 신청한 상거래관계에서 제공하기로 한 재화 또는 서비스를 그 신용정보회사등과 별도의 계약 또는 약정 등을 체결한 제3자가 신용정보주체에게 제공하는 경우를 포함한다)와 직접적으로 관련되어 있는지 여부, 3. 신용정보주체가 그 동의사항에 대하여 동의하지 아니하면 법 또는 다른 법령에 따른 의무를 이행할 수 없는지 여부” 등을 고려하여야 한다고 규정한다(제28조 제8항).

공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 수탁자와 위탁업무 내용을 공개하거나 이용자에게 알린 경우)를 두고는 있으나, 원칙적으로 개인정보 처리위탁의 경우에도 이용자, 즉 정보주체의 동의를 받도록 규정하고 있다.[64]

사. 형사처벌

개인정보보호법령의 동의 규정을 위반하였을 경우, 과태료뿐만이 아니라 형사처벌도 가능하다. 개인정보보호법의 경우 정보주체의 동의 없이 개인정보를 제3자에게 제공한 경우는 형사처벌 대상(제71조 제1호)이고 동의 없이 개인정보를 수집 · 이용한 경우는 과태료 부과 대상(제75조 제1항 제1호)이지만, 정보통신망법의 경우 정보주체의 동의 없이 개인정보를 수집 · 이용 · 제공 · 위탁한 경우 모두 형사처벌을 할 수 있도록 규정하고 있다(제71조). 형사처벌의 수위는 개인정보보호법과 정보통신망법 모두 5년 이하의 징역 또는 5천만원 이하의 벌금으로 규정되어 있다. 또한 위 형사처벌 규정과 관련하여서는 양벌규정도 마련되어 있다(정보통신망법 제75조, 개인정보보호법 제74조).

아울러 정보통신망법에 따르면 동법 제22조 제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우, 제24조의2를 위반하여 개인정보를 제3자에게 제공한 경우, 제25조 제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 경우 방송통신위원회가 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다(제64조의3 제1항 제1호, 제4호, 제5호).

3. 국내법상 동의 제도의 문제

국내법상 동의 제도에 대한 비판은, 크게 ① 복잡한 규제로 인해 정보의 활용범위를 지나치게 제한한다는 점과 ② 오히려 정보주체의 개인정보자기결정권을 효과적으로 보호

---

64) 정보통신망법 제25조(개인정보의 처리위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 있도록 업무를 위탁(이하 "개인정보 처리위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보 처리위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 처리위탁을 하는 업무의 내용

② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

하지 못하고 있다는 점으로 나뉜다. 이러한 비판은 특히 유럽연합의 GDPR이 제정되면서 비교법적인 관점에서 활발해 졌다고 볼 수 있다.

가. 정보 활용범위의 제한 관련

(1) 지나치게 엄격하고 복잡한 동의 제도

전술한 바와 같이 우리 법에서는 수집 · 이용 · 제공 · 위탁(정보통신망법의 경우) 각각의 경우에 동의를 받을 것을 요구하고 있을 뿐 아니라, 원칙적으로 수집 및 이용에 대한 동의와 제공 동의, 위탁 동의를 구분해서 개별적으로 동의를 받아야 하는데다 필수 동의사항에 대해서도 사전 동의를 받을 것을 강제하고 있다. 즉, 사전 · 명시 · 구분 동의를 모두 요구하고 있다. 예외적으로 특별한 사정이 없는 한 원칙적으로 동의를 요구하고 있어 이른바 '동의만능주의'를 채택하고 있다고 평가될 만하다. 이는 비교법적으로도 매우 지나친 규제라는 비판이 있다.

특히 관련 법률의 규정 뿐 아니라 실무상 해석도 지나치게 엄격하게 이루어지고 있다. 개인정보 제3자 제공 시 제공받는 자를 일일이 모두 고지해야 하는, 유형고지를 금지하는 것이 그 예다. 법원의 판결도 마찬가지이다. 즉, 대법원은 "법정 고지사항을 게재하는 부분과 이용자의 동의 여부를 표시할 수 있는 부분을 밀접하게 배치하여 이용자가 법정 고지사항을 인지하여 확인할 수 있는 상태에서 개인정보의 수집·제공에 대한 동의 여부를 판단할 수 있어야" 한다[65]며, 동의 시 법정 고지사항의 정보주체의 인지가능성에 대하여 매우 엄격한 입장을 취한바 있고, 정보통신망법은 정보통신서비스 제공자가 수집한 개인정보를 이용자로부터 동의받은 목적과 다른 목적으로 이용하는 것을 금지하고(제24조), 그 위반행위를 형사처벌 대상(제71조 제3호)로 규정하고 있다는 이유에서 동의서의 문구 역시 매우 엄격하게 해석[66]하고 있다.

이러한 법원의 판단은 데이터산업의 활성화와 정보주체에 대한 다양한 서비스 제공의 측면은 물론, 후술하는 바와 같이 정보주체의 실질적 이익, 특히 개인정보자기결정권의 실질적 보장 측면에서 형식적인 동의 규제에 지나치게 얽매여 있는 것은 아닌지 근본적인 의문을 가지게 하는데, 마이데이터 산업과 연계하여 그 내용 및 타당성을 살펴볼 필요

65) 대법원 2016. 6. 28. 선고 2014두2638 판결. "이벤트 화면에 스크롤바를 설치한 것만으로는 개인정보 수집 · 이용 및 제3자 제공에 관한 동의를 구하고 있고 화면 하단에 법정 고지사항이 존재한다는 점을 쉽게 인지하여 확인할 수 있는 형태라고 볼 수" 없다고 판단함으로써, 정보통신망법 제26조의2 및 동법 시행령 제12조 제1항 및 제2항에서 규정하는 법정 고지사항의 인지가능성에 대하여 매우 엄격한 입장을 취하였다.

66) 대법원 2018. 7. 11. 선고 2016도10102 판결. 선불폰 이용계약 체결 시 동의한 개인정보 수집·이용의 목적범위에 이동통신사가 임의로 이용자의 선불요금을 충전해 계약기간을 연장하는 것이 포함되지 않는다고 보았다. 이외에도 대법원 2018. 7. 12. 선고 2016두55117 판결, 2017. 4. 7. 선고 2016도13263 판결 등 참조.

가 있다.[67]

엄격할 뿐 아니라 복잡하다는 것 또한 문제인데, 개인정보보호법과 정보통신망법은 물론, 신용정보법에 나아가 위치정보의 보호 및 이용 등에 관한 법률(이하 '위치정보법')까지 정보보호에 관한 법률이 지나치게 다양하고 규정도 상이하여 수범자로 하여금 혼란스럽게 한다. 가령 위치정보법은 다른 법률들과 달리 위치정보사업자가 개인위치정보를 수집하고자 하는 경우에는 미리 일정한 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 받도록 하고 있다(제18조 제1항). 게다가 전술한 바와 같이 GDPR이 동의의 요건을 상세하게 규정하고 있으나 대부분의 정보처리에 대해 동일하게 적용되는 것과는 달리 우리 법은 같은 법률 내에서도 정보처리의 유형에 따라 상이한 규제를 하고 있다. 특히, 적용 법률 및 정보처리 유형에 따라 법정고지사항도 달라지기 때문에 일괄적인 고지가 허용된다면 개인정보처리자 입장에서 정보활용이 매우 용이하겠으나, GDPR과 달리[68] 법정고지사항 고지의무는 별도로 규정된 개인정보처리방침 공개의무와 구별되는, 정보주체의 동의 시 명시적으로 이루어져야 하는 의무사항이라는 점에서, 정보활용의 폭을 더욱 제한하고 있다. 즉, 어떤 단계의 정보처리가 이루어지는지, 어느 법률이 적용되느냐에 따라 의무사항은 물론 제재 수준도 다르기 때문에 개인정보처리자의 예측 가능성이 크게 떨어지는 것이다.

(2) 변경 동의의 문제

전술한 바와 같이 우리 법에서는 개인정보처리에 대한 동의 시 고지한 법정 고지사항이 변경되는 경우에도 다시 동의를 받도록 하고 있다. 문제는, 변경하는 사항이 사소한 경우라고 하더라도 마찬가지라는 점이다. 이는 전술한 바와 같이 법정 고지사항에 대해 엄격하게 규정하고 있는 현행법 및 이를 더 엄격하게 해석하는 실무의 태도와 맞물려 정보 활용범위를 크게 제한하는 문제로 기능하고 있다.

가령, 개인정보 제3자 제공에서 정보를 제공받는 자의 경우 유형고지가 금지되는데다 계열사, 회원사 등도 별개의 법인격을 갖고 있다면 제3자에 해당[69]하기 때문에 프랜차이즈와 같이 회원사가 수시로 변하는 경우에는 매번 새롭게 동의를 받아야 하는 문제가 발생한다.[70] 그 외에도 개인정보 보유기간 등을 변경하는 경우도 마찬가지인데, 개인정보처리자가 더 나은 서비스를 제공하기 위한 경우까지 불필요한 동의를 받도록 하고 있다.

이는 개인정보 이용 목적과 관련해서도 부각되는 문제이다. 대법원은 전술한 바와 같

67) 고환경 · 손경민 · 주성환, 앞의 논문, 31~32면.
68) GDPR의 경우 제13조 및 제14조에서 고지해야 하는 '사항'만을 규정하고 있을 뿐이므로 privacy policy를 통한 일괄 고지가 허용된다고 해석된다.
69) 행정안전부, 앞의 해설서, 99면 질의응답 참조.
70) 정찬모, 개인정보보호에 있어 정보주체의 동의, 인하대학교 법학연구 제18집 제1호, 2015, 84면.

이 정보주체에게 고지한 정보 수집 목적을 사전 동의서의 문언에 따라 엄격하게 해석하는 경향을 보이는데, 이는 정보 활용의 범위를 지나치게 제한하는 것이므로 GDPR과 같이 당초 수집 목적과 양립하는 목적(compatible purpose), 즉 합리적으로 관련된 범위 내인 경우에는 정보주체 동의 없이 추가 처리를 허용해야 한다는 비판이 제기된다. 예컨대 기존에 적법하게 수집한 개인정보를 제품 개발을 위한 목적으로 이용 및 제공하는 것은 당초 수집 목적과 합리적으로 관련된 범위 내의 처리라고 볼 수 있는 것이다.[71] 다만 현행법상으로는 최초 수집 및 이용 목적 고지 시 '제품 개발을 위한 목적'으로 개인정보를 이용한다는 점을 알리지 않았다면 위 목적 이용을 위해서는 변경 동의를 다시 받아야 하는 결론에 이르게 된다.

(3) 형사처벌 중심의 제재

우리 법은 매우 복잡하게 규제를 하고 있어 개인정보처리자가 그 내용을 모두 알기 어려움에도 불구하고 동의 없이 개인정보를 처리하였을 경우 형사처벌까지 가능한, 강력한 제재 수단을 동원하고 있다. 그러나 앞서 살펴본 바와 같이, 정보주체의 권리를 강력하게 보호하고 있다는 평가를 받는 GDPR도 적법 처리 조건 없이 개인정보를 처리한 경우 형사처벌을 하고 있지 않다. 우리 법체계와 유사한 면이 많다고 할 수 있는 일본의 개인정보보호법 역시 마찬가지다.

그 처벌 수위 또한 문제인데, 개인정보보호법 제71조 제1호나 정보통신망법 제71조 제3호에 의하면 정보주체의 동의를 받지 않고 개인정보를 제3자에게 제공한 경우 징역 5년 이하 또는 벌금 5천만원 이하에 해당한다. 반면 형법은 '비밀장치에 의해 보존되어 있는 정보'를 그 비밀장치를 깨고 열어 보는 행위를 3년 이하의 징역 또는 금고, 500만원 이하의 벌금에(제316조 비밀침해죄), 의사나 변호사 등이 의뢰인과의 신뢰관계에서 주고받은 의뢰인의 비밀을 누설한 행위를 3년 이하의 징역 또는 금고, 700만원 이하의 벌금에(제317조 업무상비밀누설죄) 처하고 있다는 점을 고려한다면 지나치게 강한 형사처벌 조항이라고 볼 수 있는 것이다.[72]

(4) 정보통신서비스 분야의 강한 규제

마이데이터 산업을 비롯한 데이터산업 분야에서 동의 제도가 가장 크게 문제되는 부

71) 김민호 · 고환경 · 김현경, 개인정보보호법 개정안(인재근 의원 대표발의)에 대한 의견서, 개인정보보호법학회, 2019, 9~12면.
72) 성낙인 · 이인호 · 김수용 · 권건보 · 김상용 · 이지은 · 김주영 · 손형섭 · 박진우 · 김송옥, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008, 745~746면 참조.

분은 바로 정보통신망법의 규제가 개인정보보호법보다 오히려 엄격하다는 점이다.[73] 즉, 개인정보보호법, 정보통신망법, 신용정보법, 위치정보법 등 여러 법률에 개인정보보호 관련 규정이 있어 통일되지 않아 혼란을 야기한다는 점도 큰 문제이지만, 정보통신망법의 규제가 개인정보보호법보다 엄격하다는 점도 문제이다. 개인정보처리위탁의 사전동의 요건이나, 수집 · 이용 · 제공 시 동의 예외 조항이 개인정보보호법에 비해 제한적이라는 것 등이 그 예다. 물론, 이는 온라인에서의 정보유출 등 개인정보침해 문제가 오프라인에서의 그것보다 심하다는 우려에서 나온 결과이겠지만 마이데이터 산업 등 데이터산업 분야에는 큰 장애 요소가 되며, 현실적으로도 맞지 않다는 비판이 제기될 수 있다.

가령, 개인정보보호법 및 신용정보법은 '정보주체와의 계약의 체결 및 이행을 위해 불가피하게 필요한 경우'에는 사전 동의 의무를 면제하고 있으나, 정보통신망법에는 그러한 규정이 없고 동의 예외요건이 강화되어 있다.[74] 또한 개인정보보호법은 동의 없이 정보를 수집 · 이용한 경우에는 제3자 제공한 경우와 달리 형사처벌이 아닌 과태료 처분만을 제재수단으로 하고 있으나 정보통신망법은 형사처벌도 가능하도록 규정하고 있다. 따라서 정보통신서비스 제공자 입장에서는 서비스 이용 과정에서 발생하는 정보를 이용하여 서비스 기능을 개선하려고 하더라도 수집하는 개인정보 항목이 변경된다는 이유로 새롭게 동의를 받아야 하고, 이를 위반하면 5년 이하의 징역 또는 5천만원 이하의 형사처벌을 받을 수 있게 된다. 특히 계약의 체결 및 이행을 위해 필요한 정보의 수집이라면 정보주체의 입장에서도 충분히 예견 가능성이 있다는 점에서 정보통신망법에서만 이를 동의 예외사유로 정하고 있지 않은 것은 그 부당성은 더 크다고 할 수 있다. 이러한 점은 더욱이 앱 개발사업 등을 영위하는 스타트업 기업의 경우 법률 전문지식이 부족한 경우가 많은데 이들을 모두 잠재적 범죄자로 만들 수 있다는 점에서 심각성을 보인다.[75]

게다가 정보통신 분야에서의 동의 제도는 오히려 오프라인에서의 동의 제도에 비해 비현실적인 측면이 있다. 즉, 정보통신망법이 당초 동의 요건을 절대적인 합법성 기준으로 설정한 것은 회원가입시 이용자가 직접 제공해주는 정보를 수집하는 경우만을 상정했기 때문으로 보이는바, 실제로는 인터넷 이용과정에서 무수히 많은 개인정보가 자동으로 수집된다. 그리고 그렇게 수집된 개인정보는 다른 제3자가 온라인 또는 오프라인에서 수집한 이용자의 다른 개인정보와 결합되어 더욱 세밀하게 분석될 수 있다. 그리고 그 일련

---

73) 한편, 연혁적으로 개인정보보호법이 온라인상의 개인정보보호를 규율하고 있던 정보통신망법을 그대로 반영하여 개인정보보호법이 정보통신망법의 문제를 거의 답습하고 있다는 평가도 있다. 이러한 견해에 대하여는 위의 책, 739~746면 참조.

74) 정보통신망법 제22조(개인정보의 수집·이용 동의 등) ② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

75) 고환경, 개인정보 동의 및 파기 규정의 적정성에 관하여, 네이버 개인정보 칼럼, 2015.

의 과정은 이용자의 동의가 없거나 인식이 없는 상태에서 이루어지는 경우가 많을 수밖에 없는 것이다.[76] 특히 사물인터넷 기술이 적용되는 스마트카 또는 자율주행차의 경우, 사람이 개입하지 않고 정보가 수집, 이용되는 사물인터넷 체제 하에서는 사전에 정보주체로부터 일일이 개인정보 수집과 이용에 대한 동의를 받는 것이 거의 불가능하다. 그러한 동의를 아주 엄격하게 받도록 법적으로 강제하는 동의 제도는 사물인터넷과 관련된 기술의 발전에 장애가 될 수 있다. 또한 엄격한 동의 제도는 정보의 효율적 교환과 이에 기초한 자동적인 처리를 전제로 하는 사물인터넷 체제를 붕괴시킬 우려가 있다.[77]

(5) 소결론

요컨대 우리 법은 동의 제도를 지나치게 절대화하고 있으며 엄격한 동의 요건을 모든 개인정보 처리에 요구하고 있다는 점에서 비판을 받기에 충분하다. 이는 개인정보보호법 및 그 근거가 된 정보통신망법이 수집·이용·제공되는 개인정보를 모두 '비밀'과 같은 수준으로 이해하고 있는 데에서부터 시작된 것으로, 현행 개인정보보호법 및 정보통신망법의 개인정보보호규정은 '개인정보보호법'이 아니라 '비밀보호법'으로 기능하고 있다는 평가 내지 비판을 받고 있다.[78] 결국 이는 정보주체의 보호와 사업자의 이익 사이에서 적절한 균형을 상실한 입법으로 생각된다. 나아가 향후 본격화될 것으로 보이는 마이데이터 산업 발전을 저해할 가능성 역시 매우 큰 것으로 보인다.

나. 개인정보자기결정권 보호 관련

(1) 동의규제의 역설

문제는, 위와 같이 정보활용의 범위를 크게 제한하면서까지 우리 법이 보호하려고 했던 개인정보자기결정권을 현행 동의 제도가 오히려 제대로 보호하지 못하고 있다는 점이다. 이러한 현상은 이른바 '동의규제의 역설(paradox)'이라고 불리는데, '동의규제의 역설'이란 동의서가 길고 복잡해질수록 정보주체는 고지사항을 제대로 읽지 않아 정보를 제공하는지도 모른 채 개인정보를 제공하고 사업자들은 면죄부를 받게 된다는 것을 말한다.[79] 즉, 동의가 형식화되어 제 기능을 하지 못하고 있다는 뜻이다.

정보주체는 대체로 개인정보 보호의 중요성에 대해서는 알고 있지만, 개인정보에 관한

76) 성낙인 · 이인호 · 김수용 · 권건보 · 김상용 · 이지은 · 김주영 · 손형섭 · 박진우 · 김송옥, 앞의 책, 740~743면.
77) 권영준, 앞의 논문, 709면.
78) 성낙인 · 이인호 · 김수용 · 권건보 · 김상용 · 이지은 · 김주영 · 손형섭 · 박진우 · 김송옥, 앞의 책, 745~746면.
79) 고환경, 앞의 칼럼.

동의의 내용과 범위, 의미에 대해 충분히 알지 못하고, 또한 알려고 시도하지 않는 경향을 보인다. 알고 하는 동의(informed consent)가 되려면 정보가 충분히 제공되고 이를 충분히 인지한 가운데 동의가 이루어져야 하지만 실제로는 알고 하는 동의가 이루어지지 않고 있는 것이 현실이다. 이는 동의가 형식화되고 있음을 의미한다. 정보주체는 개인정보 보호의 중요성에 대해 추상적으로만 인식하고 있고, 동의 내용에 대해 숙려할 합리적 인센티브가 부족하기 때문에 이런 현상이 발생하는 것이다.[80]

현행법은 정보주체로부터 더 확실하고 강력한 동의를 받는 데에 초점이 맞추어져 있으나 역설적으로 이는 동의를 더욱 형식적으로 만드는 원인이 된다. 충분한 정보를 제공하고자 할수록 개인정보처리방침이나 관련 약관은 복잡하고 길어지고 개별 사항들에 대해 사전에 명시적이고 개별적인 동의를 받고자 할수록 동의를 위해 거쳐야할 절차는 늘어난다. 이러한 복잡한 절차 속에서 정보주체는 번잡함을 느낄 뿐 개인정보 보호는 실질적으로 구현될 수 없다.[81]

오히려 동의가 기업의 면죄부로 기능하며 오히려 정보주체의 소외를 심화시키기도 한다.[82] 유효한 동의의 요건을 매우 까다롭게 정하고 대신 다른 적법 처리 요건을 제시하고 있는 GDPR과는 달리, 동의 제도를 절대적으로 놓고 다른 예외를 매우 엄격하고 협소하게 해석하고 있는 우리 법제에서는 반대로 정보주체의 동의를 받기만 하면 되기 때문이다. 즉, 현실적으로 동의 제도는 정보의 최소수집 원칙, 목적 명확성 원칙, 민감정보 처리 금지원칙 등을 우회하는 수단으로 남용되고 있다.[83]

또한, 현재 행해지고 있는 개인정보 처리 동의는 형식상으로는 자유로운 상태에서 행해지지만, 서비스 제공받기를 포기하지 않는 이상에는 정보처리에 동의하지 않을 수 없으므로 실질적으로 자유가 제약된 상태에서 행해진다. 또한 필수 동의사항 이외의 선택적 동의사항에 대한 동의거부가 서비스 제공거절사유가 되지는 못하지만 서비스 차별사유는 될 수 있기 때문에 필수정보와 선택정보의 구별이 큰 의의를 가지지 못하고 있다.[84]

요컨대 동의규제의 역설은 모든 종류의 개인정보처리에 일괄적으로 동의를 요구할 뿐 그 동의가 알고 하는 동의(informed consent)인지, 자유로운 상태에서의 동의인지 실질적인 판단이 이루어지지 않기 때문에 일어나는 현상이라고 할 수 있다. 개인정보처리자의 입장에서는 동의를 받지 않으면 사업을 할 수 없고, 정보주체의 입장에서는 동의를 하지 않으면 서비스를 받을 수 없기 때문에 GDPR을 넘어서는 강력한 개인정보자기결정권 보호수단인 동의 제도가 제 기능을 하지 못하는 역설적인 상황이 벌어지고 있는 것이다.

80) 권영준, 앞의 논문, 703면.
81) 위의 논문, 705면.
82) 고환경 · 손경민 · 주성환, 앞의 논문, 31면.
83) 정찬모, 앞의 논문, 2015, 86면.
84) 위의 논문, 83면.

(2) 동의 형식화의 현실

개인정보처리에 대한 동의규제의 역설은 동의의 형식화의 형태로 나타난다. 익히 알려진 바와 같이 정보주체는 제대로 동의서를 읽어보지도 않고 개인정보처리에 동의하게 되는데, 이하에서는 구체적인 현실에 대해 소개하고자 한다.

㈎ 행정안전부와 개인정보보호위원회의 2018년 조사

행정안전부와 개인정보보호위원회는 2013년부터 개인정보보호 실태조사를 하여 연구보고서를 발간하고 있다. 2019년 2월, 행정안전부와 개인정보보호위원회는 2018년의 개인정보보호 실태조사에 대해 발표하였다.[85]

<표 4-1> 개인정보 동의서 확인

구 분		(1) 전혀 확인하지 않는다	(2) 대부분 확인하지 않는다	(3) 대부분 잘 확인한다	(4) 매우 잘 확인한다	(1)+(2) 확인하지 않음	(3)+(4) 확인함
전 체		9.5	60.1	27.6	2.8	69.6	30.4
성별	남성	8.9	57.2	30.7	3.2	66.1	33.9
	여성	10.1	63.3	24.3	2.4	73.4	26.7
연령	20대	10.7	61.4	24.4	3.5	72.1	27.9
	30대	9.8	57.8	30.1	2.2	67.6	32.3
	40대	6.9	62.8	28.0	2.3	69.7	30.3
	50대	10.3	58.4	28.6	2.7	68.7	31.3
	60대 이상	10.0	60.3	26.3	3.4	70.3	29.7

정보주체가 개인정보를 개인정보처리자에게 제공할 때 정보주체의 30.4%만이 동의서를 확인하는 것으로 나타났으며 9.5%는 동의서를 전혀 확인하지 않는 것으로 나타났다. 정보주체 성별로는 남성(33.9%)이 여성(26.7%)보다 동의서를 더 확인하며, 연령별로는 30대(32.3%)에서 동의서 확인 비율이 높게 나타났다.

특히 위 (1) “전혀 확인하지 않는다”와 (2) “대부분 확인하지 않는다”를 합하면 69.6%의 비율을 차지하는 것으로 확인된다.

85) 이하에서 인용한 조사는, <행정안전부 · 개인정보보호위원회, 2018 개인정보보호 실태조사, 2019, 113~125면>을 참조한 것이다. 이 조사는 2018년 8월 9일부터 같은 해 10월 22일까지, 국내 12세 이상 69세 이하 2,500명을 대상으로 설계 · 진행된 조사이다. 자세한 사항은 위의 조사, 10면 참조.

<표 4-2> 동의서 미확인 이유

구 분		확인하는 것이 귀찮고, 번거로워서	동의서 내용에 상관없이 서비스를 반드시 이용해야 해서	내용이 많고 이해하기 어려워서	확인해도 개인정보보호에 도움이 되지 않을 것 같아서
전 체		38.4	30.7	24.4	6.5
성별	남성	41.8	29.6	22.1	6.5
	여성	35.2	31.8	26.7	6.4
연령	20대	39.0	26.8	28.7	5.5
	30대	40.6	25.1	28.1	6.3
	40대	40.4	33.2	21.0	5.4
	50대	36.1	34.6	21.7	7.6
	60대 이상	35.1	34.2	22.7	8.0

※ Base = 동의서를 확인하지 않는 응답자

동의서를 확인하지 않는 이유에 관하여는, '확인하는 것이 귀찮고, 번거로워서'가 38.4%로 가장 많았으며, 그 다음으로는 '동의서 내용에 상관없이 서비스를 반드시 이용해야 해서'가 30.7%로 뒤를 이었다.

<표 4-3> 개인정보처리방침 인지 여부

구 분		미인지	인지
전 체		42.9	57.1
성별	남성	42.3	57.7
	여성	43.5	56.5
연령	20대	39.3	60.7
	30대	43.5	56.5
	40대	43.4	56.6
	50대	43.9	56.1
	60대 이상	44.7	55.3

한편, 개인정보처리자가 공개해야 하는 개인정보처리방침에 대해 인지하고 있는 경우는 57.1%로 나타났으며, 저연령층일수록 근소하게 높은 값을 보였다.

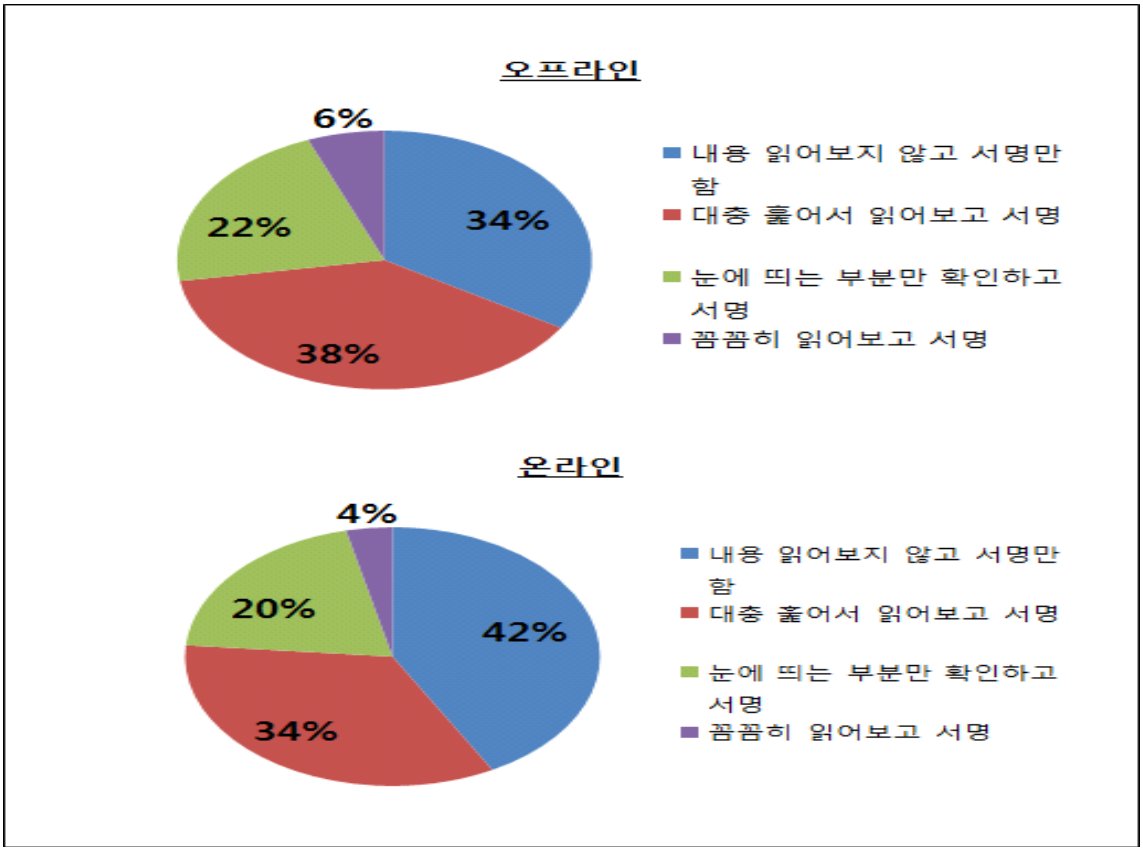
㈏ 나종연 교수의 2013년 조사

나종연 교수[86]는 개인정보보호위원회 연구용역 보고서에서 정보주체가 개인정보처리 동의서와 관련하여 보이는 행태를 면밀하게 조사 · 분석한 바 있다.[87]

86) 서울대학교 소비자학과 교수(2004~)

87) 이하에서 인용한 조사는, <나종연, 정보주체 동의권의 실질적 보장을 위한 연구(개인정보보호위원회 연구용역 보고서), 서울대학교 산학협력단, 2013, 75~118면>을 참조한 것이다. 이 조사는 2013년 8월 8일부터 같은 달 13일까지, 국내 성인 소비자 500명을 남녀 성별 50%씩 할당하여 설계 · 진행된 조사이다. 자세한 사항은 위의 연구, 99~100면

<그림 4-1> 개인정보 수집 · 이용 동의에 대한 소비자의 행동



개인정보 수집 · 이용 시 동의서에 서명하는 경우, 소비자들이 ① 내용 읽어보지 않고 서명만, ② 대충 훑어서 읽어보고 서명, ③ 눈에 띄는 부분만 확인하고 서명, ④ 꼼꼼히 읽어보고 서명하는지 여부에 대해 조사한 결과, 오프라인에서는 가장 많은 조사 대상자가 개인정보 수집·이용 동의서에 동의할 때 동의서의 내용을 대충 훑어서 읽어보고 서명하는 것(38.6%)으로 나타났다. 온라인에서는 조사 대상자가 개인정보 수집·이용 동의서에 동의할 때 내용을 읽어보지 않고 서명만 하는 행동(42%)이 가장 많이 나타났다.

반면에, 동의서의 내용을 꼼꼼히 읽어보고 서명하는 행동은 오프라인(6%), 온라인(3.6%)로 가장 낮게 나타났다. 오프라인과 온라인에서의 개인정보 수집·이용 동의서에 대한 소비자의 동의 행태를 확인한 결과, 온라인과 오프라인 간에 큰 차이 없이 내용을 읽어보지 않고 서명만 하는 경우가 가장 높은 비율을 차지하고 있었으나, 오프라인 상에서 조금 더 주의 깊게 동의 행동을 하고 있는 것으로 볼 수 있다.

참조.

88) 5점 만점, 이하 동일함.

<표 4-4> 동의서를 읽어보지 않는 이유

세부 내용	평균점수[88]
내용이 너무 길어서/양이 많아서 (창의 크기가 커서 스크롤바를 많이내려야 함 등)	4.34
읽든 안 읽든 어차피 동의해야 하니까 읽을 필요가 없어서	4.26
읽기가 불편해서 (글자크기 작음, 한 화면에서 읽기가 쉽지 않음 등)	4.15
개인정보 동의서가 대부분 비슷하기 때문에, 사업자별로 따로 읽을 필요가 없다고 생각해서	3.89
읽기가 귀찮아서	3.89
내용이나 용어가 너무 어려워서 읽고 싶지 않음 (예 : 제3자 제공, 업무위탁 등)	3.85
시간이 없어서 또는 내용을 읽을 시간을 주지 않아서 (예 : 카드발급, 휴대폰 개통시 사업자가 체크할 부분만 제시)	3.57
대기업이나 이름이 알려진 신뢰할 만한 사이트의 경우 회사를 믿고 상세히 읽지 않음	3.56
개인정보에 관심이 없어서	2.25

한편, 해당 조사에서 동의서를 다 읽어보지 않는 이유에 관하여는, 동의서의 내용이 너무 길거나 양이 많아서, 동의서의 내용을 읽든 안 읽든 상관없이 동의해야 하기에 읽을 필요가 없어서, 글자 크기가 작거나 동의서를 화면에서 읽기가 쉽지 않아서의 순서대로 조사되었다.

또한, 개인정보 수집 · 이용 동의서의 내용에 대한 이해도와 관련하여서는 전반적으로 개인정보 수집·이용에 대한 이해도가 낮은 편으로 보이며, 제대로 이해한다고 응답한 사람은 38.6%에 불과한 것으로 나타났다.

<표 4-5> 업종별 개인정보 수집 · 이용 동의관련 행태

업종	원하지 않은 채 동의한 경험		동의 후, 마케팅 및 홍보성 정보 습득 경험	
	평균점수	Top 2%	평균점수	Top 2%
통신사	4.23	82.0	4.22	81
신용카드사	4.21	80.2	4.20	80.2

포털사이트 가입	4.18	79.4	3.38	47.2
온라인 마켓	4.17	79.6	3.65	57.4
온라인 소셜커머스사	3.96	71.6	3.45	49.8

업종별로는 통신사와 신용카드사의 서비스 이용을 위하여 개인정보 제공을 원하지 않는 경우라도 동의하는 경우가 많은 것으로 나타났으며, 온라인 소셜커머스사의 경우 원하지 않은 채 동의한 경험이 상대적으로 적은 것으로 확인되었다. 이는 통신사나 신용카드사가 제공하는 서비스가 소비자의 삶에 있어 매우 중요한 영역이기 때문에, 소비자가 통신사나 신용카드사와 거래하게 되는 경우 사업자가 더욱 우월적 지위를 가지는 상황이라는 점이 영향을 미쳤을 것으로 예상되고 있다.

<표 4-6> 필수/선택적 동의사항에 관한 동의 행태

내용	평균점수
동의하지 않을 경우, 서비스를 이용할 수 없거나 다른 불이익이 있을까봐 동의하는 편이다.	3.87
필수적 동의사항과 선택적 동의사항이 구분되어 있지 않으면 그냥 동의하는 편이다.	3.76
자세히 읽기가 귀찮아서 그냥 일괄 동의하는 편이다.	3.55
선택적 사항이 있는 것을 몰랐거나, 전부 필수적으로 동의해야 한다고 생각했다.	3.38
선택적 사항에 대해서도 대부분 동의하는 편이다.	3.02
선택적 사항에 대해 주의 깊게 보는 편이다.	2.89
경험 상 필수적 사항과 선택적 사항으로 구분하여 동의하도록 되어 있었다.	2.81
필수적 사항에 대해 주의 깊게 보는 편이다.	2.81

필수적 동의사항과 선택적 동의사항과 관련하여서도 필수사항과 선택사항이 구분되어 있다고 보는 소비자의 비중이 낮은 것으로 나타났으며, 선택사항에 대해 주의 깊게 보지 않고 선택사항에 대해 대부분 동의하고 있는 것으로 나타났다.

위의 조사 결과는, 전술한 국내 법제도의 비판점이 여실히 현실적으로 드러난 것이라고 볼 수 있다. 정보주체는 동의서를 제대로 읽지 않고 필수적 · 선택적 동의사항을 구별하지 않고 동의를 하고 있었으며 그 이유는 동의서가 지나치게 어렵고 복잡하고 길 뿐만 아니라, 어차피 동의를 하지 않으면 서비스를 받지 못한다는 점에 있었다.

다. 동의제도 문제에 대한 설문조사

앞서 언급한 동의제도 문제에 대하여 실제 마이데이터 사업자는 어떻게 생각하고 있는지 살펴보기 위해 본 연구과제를 수행하며 일부 마이데이터 사업자들을 대상으로 설문조사를 실시하였다. 설문 내용은 마이데이터 서비스를 위한 개인정보처리 동의 과정의 어려움 및 사업자 입장에서 선호하는 동의 방식, 마이데이터 서비스의 원활한 시행을 위한 방안 등이었다. 설문조사 중 동의 제도에 관한 부분은 아래와 같다.

4. MyData 서비스를 위해 개인정보 처리 동의(이하 “개인동의”)를 받는 과정에서 느끼는 어려움을 모두 선택해 주십시오. (복수선택, 3개까지 선택 가능)

□ 동의와 관련된 법령이 지나치게 복잡하여 이를 이해하고 준수하기 어렵다.
□ 동의와 관련된 법령이 자주 개정되는데 이에 대한 파악이 어렵다.
□ 개인동의 획득을 위한 프로그램을 개발하거나 이를 이용하는 것이 어렵다.
□ 어떤 것이 개인정보이고 어떤 것이 개인정보가 아닌지 판단하기 어렵다.
□ 동의를 받아야 하는 개인정보의 범위를 판단하기 어렵다.
□ 수집하는 개인정보 항목을 모두 파악하기 어렵다.
□ 개인정보를 사용하는 목적을 모두 파악하기 어렵다.
□ 개인정보 보유기간을 설정하는 것이 어렵다.
□ 개인정보를 제공하는 제3자를 모두 파악하기 어렵다.
□ 제3자에게 제공하는 개인정보 항목을 파악하기 어렵다.
□ 개인정보를 제공받는 제3자가 이를 이용하는 목적을 판단하기 어렵다.
□ 개인정보를 제공받는 자의 개인정보 보유기간을 판단하기 어렵다.
□ 필수적·선택적 동의 항목을 구분하는 것이 어렵다.
□ 선택적 동의 항목에 대하여는 정보주체가 동의를 거부하는 경우가 많아 필요한 개인정보를 취득하는 것에 어려움이 있다.
□ 동의서에 체크박스를 하나만 만들어 일괄동의를 받아도 되는지 아니면 동의사항마다 체크박스를 만들어야 하는지 판단하기 어렵다.
□ 고지사항에 변경이 발생하는 경우 추가 개인동의를 받아야 하는지 여부를 판단하기 어렵다.
□ 고지사항에 변경이 발생하는 경우 추가 개인동의를 받기가 어렵다.
□ 기타 어려움이 있다면 적어주십시오.

5. 다음 중 MyData 서비스를 수행하는 데 있어서 개인동의 제도의 가장 큰 문제점은 무엇이라고 생각하나요?

□ 복잡한 개인정보 동의 취득 방식 - 법정 고지사항 파악, 필수적 선택적 동의사항 구분, 개인정보 수집이용 동의/ 제3자 제공 동의/ 마케팅 활용 동의/ 영리목적 광고성 정보 수신 동의 등 구성의 어려움 등

□ 엄격한 개인정보 동의 취득 방식 - 일부 예외사유가 있는 경우를 제외하면 법정 고지사항을 모두 알리고 사전에 명시적인 동의를 받도록 하고, 일부 고지사항의 변경이 있는 경우 재차 변경 동의를 받도록 하는 것 등

□ 형식적인 개인정보 동의 취득 방식 - 사업자는 법정 고지사항에 있는 내용을 형식적으로 열거, 동의서 분량이 방대해지는 경우 이용자가 실질적으로 동의내용을 인지하기 어려운 상황 등

□ 적법한 개인정보 동의를 획득하지 않는 경우의 제재(형사처벌, 과징금 등)

□ 기타 문제라고 생각하는 점이 있다면 적어주십시오.

6. 다음 중 가장 선호하는 개인동의 방식이 무엇인지 선택하여 주십시오.

□ 현행 개인동의 방식

□ 개인정보 처리방침에 대한 동의 취득 방식

□ 이용약관에 개인동의 관련 내용을 모두 포함한 후 이용약관에 대한 동의 취득 방식

□ 서비스를 위하여 필요한 개인정보 이용을 위하여는 동의를 받지 않아도 되고, 마케팅과 같이 서비스를 위하여 필요하지 않은 개인정보 이용을 위하여만 동의를 취득하는 방식

□ 서비스 이용 시 개인정보 처리에 대한 동의 의제 방식

□ 기타 선호하는 방식이 있다면 적어주시기 바랍니다

7. 다음 중 가장 선호하는 개인동의 구성이 무엇인지 선택하여 주십시오.

□ 현행 개인동의 구성

□ 개인정보 수집이용 동의, 제3자 제공 동의 등을 구별하지 않고 필수적 개인정보에 대하여는 하나의 동의 항목만을 이용하는 개인동의 구성

□ 필수적 개인동의, 선택적 개인동의를 구별하지 않고 전체적으로 하나의 동의 항목만을 이용하는 개인동의 구성

□ 개인정보 처리에 동의하지 않는 항목에 대하여만 의사표시하는 opt-out형 개인동의 구성

□ 기타 선호하는 방식이 있다면 적어주시기 바랍니다.

8. 다음 중 가장 선호하는 개인동의 절차가 무엇인지 선택하여 주십시오.

□ 현행 개인동의 절차

□ 개별 개인정보를 실제로 이용할 때 동의를 받는 개인동의 절차

□ 서비스 개시 후 개인정보 처리에 반대할 때 의사표시 하도록 하는 opt-out형 개인동의 절차

□ 기타 선호하는 방식이 있다면 적어주시기 바랍니다.

9. MyData 서비스를 원활하게 시행하기 위하여 가장 필요하다고 생각하는 것을 선택해 주십

시오.
□ 개인동의 제도 등에 관한 데이터 3법 내용의 개정
□ MyData 서비스 사업자를 위한 표준 개인동의 양식
□ MyData 서비스 사업자를 위한 개인정보 처리 가이드라인
□ MyData 서비스만을 위한 특별법의 제정
□ 기타 필요하다고 생각하는 것이 있다면 적어주시기 바랍니다.

이에 대해 사업자들은 동의 제도 관련 법규정이 지나치게 복잡하여 이해하거나 준수하기 어렵고(50%), 자주 개정되어 파악하기도 어렵다(33%)는 응답을 하였다. 무엇보다, 법정 고지사항을 파악하고, 필수적 동의사항과 선택적 동의사항을 구분하며 개인정보 수집 · 이용 동의, 제3자 제공 동의, 마케팅 활용 동의, 영리목적 광고성 정보수신 동의 등 각각의 동의를 따로 받아야 하는 등 복잡한 동의 취득 방식이 마이데이터 서비스 수행에 있어서 가장 큰 문제점이라고 꼽았다(50%).

사업자들은 선호하는 개인정보처리 동의 방식으로 '이용약관에 개인동의 관련 내용을 모두 포함한 후 이용약관에 대한 동의 취득 방식'(50%)을, 선호하는 개인정보처리 동의서 구성 방식으로는 '개인정보 수집이용 동의, 제3자 제공 동의 등을 구별하지 않고 필수적 개인정보에 대하여는 하나의 동의 항목만을 이용하는 개인동의 구성'(50%)을 선택하였는 바, 전술한 바와 같이 GDPR처럼 개인정보처리방침을 통한 일괄 고지와 포괄적 동의가 허용될 필요성을 느낄 수 있는 대목이었다.

4. 시사점

우리 법의 동의 제도의 현황과 비판점에서 주목할 점은 우리 법의 동의 제도가 지나치게 엄격하고 복잡하여 정보의 활용 범위를 제한한다는 것뿐만이 아니라, 실제로 정보주체의 보호, 즉 개인정보자기결정권을 제대로 보장하지도 못하고 있다는 부분이다. 그렇기 때문에 동의 제도를 개선함에 있어서는 사업자의 영업의 자유 및 정보의 활용 범위를 넓히는 것만큼이나 정보주체의 개인정보자기결정권을 실질적으로 보장할 수 있도록 하는 것도 중요하다.

즉, 동의 제도가 지나치게 엄격하다고 해서, 개인정보자기결정권 보장을 후퇴시키는 방향으로 입법 또는 정책이 이루어져는 안 될 것이고, 오히려 개인정보자기결정권을 보다 현실적으로 보장하는 방향으로 개선이 이루어져야 할 것이다.

또한, 개인정보 유출, 오남용 등의 위험이 적절히 통제될 필요가 있다. 개인정보 분야

외에도 정보보안 분야에 있어서 규제가 강화되고 있는 이유는 개인정보 유출로 인한 피해가 자주, 광범위하게 일어나고 있기 때문이다. 2019년 국정감사에서 제기된 지적에 의하면, 2012년 8월 이후 2019년 8월에 이르기까지 340차례에 걸쳐 총 7,428만 건의 개인정보가 유출되었다고 한다.[89] 개인정보 유출 뿐 아니라 개인정보처리자에 의한 개인정보 오남용의 위험도 상존하는 상황에서, 이러한 위험성이 적절히 통제되지 않으면 마이데이터 산업의 근간이 흔들릴 수도 있다.

마지막으로, 대량의 데이터를 보유하고 있는 기존의 개인정보처리자와 새롭게 사업을 시도하는 개인정보처리자 간의 이익 균형을 고려할 필요성이 있다. 이미 대량의 데이터를 합법적으로 수집하여 이를 이용 및 보유하고 있는 기존의 개인정보처리자는 복잡한 동의 절차를 추가적으로 거치지 않아도 개인정보를 이용할 수 있으며, 이와 같이 기존 사업자가 이미 적법하게 처리하고 있는 개인정보는 기존 사업자가 시간 및 비용을 투자하여 획득한 영업의 결과물이라는 점 또한 고려될 필요가 있는 것이다.

5. 산업 분야별 마이데이터 관련 법제도 현황 분석

지금까지는 현행 개인정보보호 관련 법령상 동의 제도의 문제점 및 시사점을 전반적으로 살펴보았다면, 본 항에서는 구체적 산업 분야별로 마이데이터 관련 법제도 현황에 대해 살펴본다. 앞서 살펴 본 바와 같이 정보주체 중심의 마이데이터 서비스는 의료, 교육, 금융, 통신, 에너지 등 다양한 분야에서 그 수요가 꾸준히 증가하고 있는바, 이하에서는 특히 통신, 금융, 의료 분야에서 현행법 하에서 인정되는 정보주체의 권리를 바탕으로 마이데이터 서비스를 제공할 수 있는지 살펴본다.

가. 통신분야

정보통신망법은 이용자가 정보통신서비스 제공자등에 대하여 본인의 개인정보 열람 및 제공을 청구할 수 있도록 규정하고 있다(제30조 제2항[90]). 따라서 이용자가 직접 자신의 개인정보를 정보통신서비스 제공자로부터 제공받아 마이데이터 사업자에게 해당 정보를 관리하고 제3자에게 제공하도록 하는 방식으로 마이데이터 사업자가 서비스를 제공하는

89) 서울경제 2019. 10. 4.자, “개인정보 7천만건 탈탈 털렸지만…과태료는 건당 131원 불과” 참조. (https://www.sedaily.com/NewsView/1VPE35TOV3)

90) 정보통신망법 제30조 ② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.
1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

방법이 가능할 것이다.

마이데이터 사업자가 이용자로부터 위임을 받아 상기 이용자의 권리를 대리하여 행사하는 방법으로 서비스를 제공하는 것도 가능하다고 보인다. 정보통신망법은 위와 같은 이용자의 권리를 대리행사 할 수 있는지에 대하여 명시적으로 규정하고 있지 않으나, 이를 대리에 친하지 않은 행위로 단정하기 어렵다. 또한 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보보호법이 적용되는데[91] 개인정보보호법 제38조는 정보주체가 그 권리를 대리인에게 행사하도록 할 수 있다는 명시적인 규정을 두고 있다.

나아가, 이러한 이용자 직접 수령 후 제공 방식, 대리 방식을 취하지 않더라도, 이용자의 개인정보를 기존에 보유하고 있는 타 사업자와 협의가 가능한 경우라면, 마이데이터 사업자가 (이용자의 정보를 기존에 보유하고 있는 타 사업자의 마이데이터 사업자에 대한) 정보통신망법 제24조의2[92]에 따른 제3자 제공 동의를 받는 방안을 고려할 수도 있다. 이 경우 제3자 제공 동의는 (타 사업자 대신에) 마이데이터 사업자가 받는 것도 가능할 것이다.[93]

결국 현행 정보통신망법 하에서는 이용자가 직접 자신의 개인정보를 정보통신서비스 제공자로부터 제공받아 마이데이터 사업자에게 해당 정보를 관리하고 제3자에게 제공하도록 하는 방식, 마이데이터 사업자가 이용자(정보주체)의 위임을 받아 그를 대행/대리하여 정보통신서비스 제공자로부터 개인정보를 제공받는 방식, 마이데이터 사업자가 (마이데이터 사업자에 대한) 제3자 제공 동의를 받아 서비스를 제공하는 방식이 가능할 것으로 보인다.

참고로, 전기통신사업법은 번호이동성제에 대해 규율하고 있다. 번호이동성제란, 이용자가 자신이 가입한 통신서비스의 제공사업자를 변경하는 경우에도 이용자가 사용하던 기존의 전기통신번호를 유지할 수 있도록 해주는 제도이다. 개인이나 가정, 회사에서는 오랫동안 이용한 전화번호를 한 번 사용하기 시작하면 잘 바꾸려 하지 않는 경향이 있었다.[94] 번호이동성제도는, 번호를 유지한 채로 사업자를 변경한다는 점에서, 전술한 바와 같이 GDPR의 정보이동권과 유사한 면이 있다.

전기통신번호이동성의 시행에 관한 사항과 번호이동성관리기관의 지정 및 그 업무 처

91) 개인정보보호법 제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

92) 정보통신망법 제24조의2 ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다.(이하생략)

93) 금융위원회, 금융분야 개인정보보호 가이드라인, 2017 90면은 '개인정보를 제공받고자 하는 자가 정보주체의 동의를 받아 해당 정보주체의 개인정보를 보유하고 있는 자에게 제공 요청을 할 수 있는지 여부'에 대해 '해당 개인정보를 제공하는 자와 제공받고자 하는 자가 상호 협의한 경우에는 개인정보를 제공받고자 하는 자가 개인정보를 제공하는 자에게 정보주체의 동의 의사를 대신 제출한 후 개인정보를 제공받는 것은 가능'하다고 설명하고 있는데 이를 참고할 수 있겠다.

94) 신종철, 통신법해설, 진한엠앤비, 2019, 168면.

리 등에 필요한 사항은 과학기술정보통신부장관이 정하여 고시하고 있는데(전기통신사업법 제58조 제5항), 이를 위하여 이동전화서비스 번호이동성 시행 등에 관한 기준과 시내전화서비스 등 번호이동성 시행에 관한 기준 등의 고시가 제정되어 시행되고 있다. 또한, 번호이동성관리기관(동법 제58조 제4항)으로는 사단법인 한국통신사업자연합회가 지정되어 있다.[95]

나. 금융분야

신용정보/금융정보와 관련하여서는 신용정보법, 금융실명거래 및 비밀보장에 관한 법률(이하 '금융실명법') 등이 규율하고 있다.[96]

신용정보법은 정보주체가 자신의 신용정보를 신용정보회사등으로부터 제공받을 수 있도록 규정하고 있다(제38조 제1항[97]). 따라서 정보주체가 직접 자신의 신용정보를 신용정보회사등으로부터 제공받아 마이데이터 사업자에게 해당 정보를 관리하고 제3자에게 제공하도록 하는 방식으로 마이데이터 사업자가 서비스를 제공하는 방법이 가능할 것이다.

마이데이터 사업자가 정보주체로부터 위임을 받아 상기 권리를 대리하여 행사하는 방법으로 서비스를 제공하는 것도 가능하다고 보인다는 점은 통신분야에서 설명한 바와 동일하다.

나아가, 이러한 정보주체 직접 수령 후 제공 방식, 대리 방식을 취하지 않더라도, 신용정보를 제공하는 자와 협의가 된 경우라면 마이데이터 사업자가 (신용정보를 기존에 보유하고 있는 타 사업자의 마이데이터 사업자에 대한) 신용정보법 제32조[98]에 따른 제3자 제공 동의를 받는 방안을 고려할 수도 있겠다. 앞서 본 바와 같이 이 경우에도 제3자 제공 동의는 (타 사업자 대신에) 마이데이터 사업자가 받는 것도 가능할 것이다.

참고로 금융실명법은 금융회사등에 종사하는 자는 명의인의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등")를 타인에게 제공하거나 누설하여서는 안 된다고 규정하고 있는바(제4조 제1항), 마이데이터 사업자가 금융회사로부터 거래정보등을 제공받으려는 경우 상기 규정도 유의하여 살펴볼 필요가 있을 것이다. 정보주체 직접 수령 후 제공 방식, 대리 방식에서는 금융회사가 '타인'에게

95) 위의 책, 168~169면.

96) 또한 현행법 해석상으로는 금융회사가 정보통신서비스를 제공하는 경우 정보통신망법의 적용도 받을 수 있다.

97) 신용정보법 제38조 ① 신용정보주체는 신용정보회사등에 본인의 신분을 나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법으로 본인임을 확인받아 신용정보회사등이 가지고 있는 본인정보의 제공 또는 열람을 청구할 수 있으며, 본인정보가 사실과 다른 경우에는 금융위원회가 정하여 고시하는 바에 따라 정정을 청구할 수 있다.

98) 신용정보법 제32조 ① 신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다. (이하생략)

제공하는 것이 아니므로 위 규정이 특별히 문제되지 않을 것으로 보이고, 마이데이터 사업자에게 제공하는 경우라면 위 규정에 따른 동의를 받는 경우 마이데이터 사업자가 제공받는 것이 가능할 것이다.

다. 의료분야

의료정보에 대해서도 정보주체가 열람 청구권을 행사하고 이를 마이데이터 사업자에게 제공하는 방식, 마이데이터 사업자가 정보주체의 위임을 받아 대리/대행의 방식으로 개인정보를 제공받는 방안을 적용 가능할 것으로 보인다.

정보주체의 열람 청구권 등을 규정한 개인정보보호법 제35조 제1항[99] 등은 민감정보(의료정보는 건강에 관한 정보로서 개인정보보호법 제23조[100]의 민감정보에 해당할 가능성이 높다)에 대해서도 동일하게 적용될 것이며, 개인정보보호법 제23조 제1항 제1호는 정보주체의 별도 동의를 받은 경우에는 민감정보의 처리가 허용되는 것으로 명시하고 있다. 그리고 앞서 본 바와 같이 개인정보보호법 제38조는 정보주체가 제35조에 따른 열람 등의 요구를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다고 규정하고 있는 점을 고려하면 위와 같은 해석이 가능하다.

나아가 (의료정보 제공자가 의료인, 의료기관의 장, 의료기관 종사자가 아닌 경우라면) 이러한 정보주체 직접 수령 후 제공 방식, 대리 방식을 취하지 않더라도, 의료정보를 제공하는 자와 협의가 된 경우라면 마이데이터 사업자가 (의료정보 제공자의 마이데이터 사업자에 대한) 개인정보보호법 제17조[101]에 따른 제3자 제공 동의를 받는 방안을 고려할 수도 있겠다. 이 경우 제3자 제공 동의는 (타 사업자 대신에) 마이데이터 사업자가 받는 것도 가능할 것이다.

다만 의료법상 의료인, 의료기관의 장 및 의료기관 종사자가 의료정보를 제공하는 경우라면 의료법 규정을 준수하여야 할 것이다. 그런데 의료법 규정에 따르면 의료정보 제공자가 직접 마이데이터 사업자에게 제3자 제공을 하는 방안은 불가능해 보이고, 대리/대행

---

99) 개인정보보호법 제35조 ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

100) 개인정보보호법 제23조 ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

101) 개인정보보호법 제17조 제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.
1. 정보주체의 동의를 받은 경우 (이하생략)

방안에 있어서도 일정 요건을 갖추어야 할 것으로 보인다.

즉, 의료법 제21조 제2항은 의료인, 의료기관의 장 및 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하는 행위를 원칙적으로 하여서는 안 되는 것으로 규정하고 있다. 예외적으로 의료법 제21조 제3항은 환자가 지정하는 대리인이 환자 본인의 동의서와 대리권이 있음을 증명하는 서류를 첨부하는 등 보건복지부령으로 정하는 요건을 갖추어 요청한 경우 환자 본인이 아니더라도 기록을 열람할 수 있도록 그 예외사유를 정하고 있다. 다만, 의료법 시행규칙 제13조의3 제2항 제4호는 이러한 열람권을 행사하기 위해서는 "환자의 신분증 사본"을 확인하여야 하는 것으로 규정하고 있는 등 위 규정에 따른 요건 및 절차를 준수하여야 한다는 점에서 고려할 사항이 보다 많다고 할 것이다.[102)]

참고로 최근 보건복지부는 2019. 10. 16. "진료기록 열람 및 사본발급 업무 지침"을 배포하였다. 위 지침은 의료법 제21조에 따른 진료기록 열람 및 사본 등의 제공 방식에 대하여,"환자의 편의 및 의료기관 행정 효율 제고를 위해 각 의료기관 여건에 맞는 온라인 본인인증 시스템 구축 및 온라인 신청 접수 시행을 권고함"으로 안내하고 있다. 위 지침에 따라 향후 의료분야에서 마이데이터 서비스가 보다 활성화 될 수 있을지를 지켜볼 필요가 있을 것이다.

제5장 개선 방안

제1절 개인정보 보호 관련 법률 개정안 검토

1. 개인정보보호법 개정안(인재근 의원안[103)])

가. 주요 내용

2018. 11. 15. 인재근 등 14인의 국회의원은 개인정보보호법 일부개정법률안(이하 "인재근 의원안")을 발의하였다. 인재근 의원안은 "4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있으며" 이를 달성하

102) 참고로 이에 대하여 최근 보건복지부는 다소 완화된 유권해석을 한 바 있다(보건복지부 의료기관정책과, '17.12. 22.). 즉, 환자의 본인확인 방법 등과 관련하여 의료기관이 자신의 책임으로 별도의 절차를 거쳐 진료기록 사본을 발급하는 것이 일률적으로 금지된다 하기는 어려우므로, 의료기관이 관련 시스템을 갖추고 무선 통신 등을 이용한 본인인증 방법 등을 거쳐 사본 발급 신청을 접수하고 진료기록 사본을 전송하는 등 '온라인 신청 또는 발급'의 방법을 이용할 수 있다고 하고 있다. 다만 의료법 시행규칙 제13조의3에 따른 요건 및 절차를 준수하지 않아서 발생하는 환자정보 유출 등의 사고에 대하여 의료기관에 법적 책임이 있음을 양지하고 신중하게 판단하여야 한다는 입장이다.

103) 개인정보보호법 일부개정법률안(인재근의원 대표발의), 의안번호 16621, 2018. 11. 15.

기 위해 개인정보보호법을 개정한다는 목적을 갖고 있다.

개정안의 내용 중 마이데이터 서비스와 특히 관련성이 있는 부분은 “당초 수집 목적과 합리적으로 관련된 범위 내에서 추가 처리를 허용”하는 인재근 의원안 제15조 제3항과 제17조 제4항일 것이다. 그 구체적인 내용은 다음과 같다.

제15조에 제3항을 다음과 같이 신설한다. ③ 개인정보처리자는 **당초 수집 목적과 합리적으로 관련된 범위 내**에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령이 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.
제17조... (중략) ... 제4항을 다음과 같이 신설한다. ④ 개인정보처리자는 **당초 수집 목적과 합리적으로 관련된 범위 내**에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령이 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

즉, 애초에 개인정보를 수집한 목적 등의 범위를 초과하여 개인정보를 이용하거나, 당초 수집 목적 등의 범위를 초과하여 개인정보를 제3자에게 제공하는 것을 금지[104]하는 현행 개인정보보호법과 달리, 수집 목적과 양립하는 목적(compatible purpose)의 경우 추가 처리를 허용한 GDPR 제6조 제4항[105]과 유사한 취지의 규정을 신설하고자 한다.

이외에도 인재근 의원안은 개인정보보호 법령을 일원화하고자 하며, 그 과정에서 정보통신망법 중 개인정보 보호에 대한 규정을 그대로 개인정보보호법으로 옮겼다. 특히, 정보통신서비스 제공자는 개인정보를 처리위탁할 때 원칙적으로 이용자의 동의를 받아야 한다는 규정을 그대로 두었다. 그 구체적인 내용은 아래와 같다. 다만, 현재 국회에서는 아래와 같이 정보통신서비스 제공자에 대해서만 개인정보 처리위탁 동의 특례를 유지하

104) 개인정보보호법 제18조 제1항 참고

105) GDPR 전문 50은 “The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected”라고 하여, 당초 수집 목적과 양립 가능한 목적을 위해서는 개인정보의 추가 처리가 가능하며, GDPR 제6조 제4항은 이러한 양립 가능성을 판단하기 위하여 “(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation”등을 고려하여야 한다고 규정하고 있다.

는 것은 부당하다는 논의가 계속되고 있으므로, 실제 입법 과정에서 아래와 같이 동의를 요구하는 규정이 개정될지 여부를 지켜볼 필요가 있겠다.

> 제39조의4(개인정보의 처리위탁에 대한 특례) ① 제26조제2항 및 제3항에도 불구하고 정보통신서비스 제공자와 그로부터 제17조제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁(이하 "개인정보 처리위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
> 1. 개인정보 처리위탁을 받는 자(이하 "특례 수탁자"라 한다)
> 2. 개인정보 처리위탁을 하는 업무의 내용

한편, 인재근 의원안은 개인정보 처리에 대하여 정보주체의 동의를 받는 방법에 대하여 규정하고 있는 개인정보보호법 제22조를 개정하는 내용은 두고 있지 않다.

나. 개정안에 대한 평가

우선, 합리적으로 관련된 범위 내에서 정보주체의 동의 없이 개인정보를 이용하고 제3자에게 제공할 수 있도록 하는 부분은 마이데이터 산업에 긍정적인 영향을 끼칠 것으로 보인다.

마이데이터 서비스는 정보주체의 요청에 따라 많은 양의 개인정보를 능동적으로 활용·이전하기 때문에, 개인정보의 유동적인 처리가 여타 서비스에 비하여 중요하다. 즉, 기존 개인정보를 이용하는 서비스는 정해진 목적(예를 들어, 물건의 배송, 청구서 발행, 맞춤형 서비스 제공 등)을 위하여 개인정보를 처리하고, 이를 달성한 후에는 개인정보를 삭제하여야 하므로, 개인정보의 활용이 제한적인 편이었다. 반면, 마이데이터 서비스는 정보주체뿐만이 아니라 제3자로부터도 개인정보를 받고, 이러한 개인정보를 다양한 방식으로 처리한 다음, 이를 정보주체에게 제공하거나 다시 제3자에게 이전하기도 하고, 그 제3자가 또 다시 처리한 개인정보를 다시 받아 처리하는 등, 개인정보 처리가 역동적이고 그 활용도가 광범위하다. 그리고 마이데이터 서비스는 다양한 근원으로부터 수집한 개인정보를 활용하여 정보주체에게 유익한 새로운 정보를 창출하기 때문에, 개인정보 수집 단계에서부터 개인정보 이용 목적을 구체적으로 특정하는 것이 쉽지 않다. 따라서 마이데이터 서비스의 성공적 정착을 위해서는 개인정보 활용 범위를 합리적인 수준에서 최대한 넓힐 필요가 있다.

그런데 현행 개인정보보호법과 정보통신망법에 의하면 당초 수집 목적 외로 개인정보를 이용하거나 제3자에게 제공하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처할 수 있고[106], 대법원은 이른바 “부활충전” 사건을 통해[107] 이용자로부터 동의받은 목

적'을 엄격하게 해석하는 입장을 취하고 있어서, 대한민국에서 마이데이터 서비스를 제공하는 것에는 많은 제약이 있다. 특히, 앞서 본 바와 같이 현행 개인정보보호법령은 개인정보 처리 목적이 변할 때마다 다시 개별적인 동의를 받을 것을 요구하고 있으므로[108], 마이데이터 서비스 사업자가 새로운 서비스를 개발하거나, 정보주체에게 유익한 가공된 정보를 마련하기 위해서는 다시 정보주체에게 동의를 받아야 하는 번거로움이 있다. 이는 단순히 사업자의 서비스 개발 비용을 증가시킬 뿐만 아니라 정보주체마저도 계속적인 동의 요구로 인해 피로감을 느끼게 한다. 인재근 의원안이 입법되면 이러한 현황을 개선할 수 있을 것으로 예상된다.

그러나 현행 개인정보보호법 개정안(인재근 의원안)만으로는 마이데이터 산업의 성공을 장담할 수 없다. 가장 큰 문제는 개인정보 처리를 위한 동의를 받는 방법을 수정하지 않고 있기 때문이다. 앞서 살펴봤듯이, 현행 법제도는 사전, 명시, 개별, 선택, 변경 동의 등 여러 엄격한 원칙을 고수하며, 역동적이고 능동적인 개인정보 처리가 핵심인 마이데이터 산업과 조화를 이루기 힘든 구조를 가지고 있다. 이러한 동의 제도 경직화의 가장 큰 원인 중 하나는 동의를 받는 방법을 규정하고 있는 개인정보보호법 제22조인데, 인재근 의원안은 이를 변경하는 내용을 담고 있지 않다. 추후 개인정보보호법을 실제로 입법하는 과정에서 추가로 개정할 필요가 있는 부분이다. 이러한 한계를 극복할 수 있는 대안인 유형 고지 방안과 구분 동의의 폐지에 대하여는 아래 "제2절 개인정보 보호 관련 제도 개선방안 검토"에서 보다 자세히 다루도록 하겠다.

2. 정보통신망법 개정안(노웅래 의원안[109])

106) 개인정보보호법 제71조 제2호, 정보통신망법 제71조 제1항 제3호

107) 대법원 2018. 7. 12. 선고 2016두55117 판결: 법원은 "번호유지기간 내에 있는 선불폰 서비스 이용자들을 대상으로 개인정보를 이용하여 임의로 일정 금액을 충전하는 이른바 '부활충전'"을 위하여 이용자의 개인정보를 이용하는 것은 "선불폰 서비스 제공자인 원고가 고객인 이용자들을 위하여 일정한 금액을 충전하여 주는 것도 이용자들의 의사에 합치할 때에만 허용된다고 보아야 하는 점, 선불폰 서비스를 계속 이용할 의사가 확인되지 아니한 이용자에게 원고가 임의로 일정 금액을 충전한 것은 선불폰 서비스 이용계약을 체결한 이용자들이 당연히 예상할 수 있는 범위 내의 서비스라고 보기 어려운 점, 선불폰 서비스 이용계약에서 정한 일정 기간이 경과하면 당연히 계약이 해지될 것을 기대하고 있던 이용자의 경우에는 더 이상 자신의 명의로 사용할 의사가 없는 선불폰 가입번호가 계속 사용할 수 있는 상태로 유지됨으로 인하여 불측의 손해를 입게 될 염려도 배제할 수 없는 점 등의 사정" 등을 이유로, 목적 외 개인정보 이용이라고 판단하였다. 한편 동일한 사건에 대한 형사재판(대법원 2018. 7. 11. 선고 2016도10102 판결)에서도 대법원은 통신사업자에게 5000만원의 벌금을, 관련 임원에게 징역 2년에 집행유예 3년 선고를 확정하였다.
이에 대하여는 요금 충전의 주체가 따로 정해져 있는 것이 아니고 이용자에게 무상으로 서비스를 제공한 것으로서, 넓게 보아 서비스의 범주에 모두 해당되기 때문에, 본래 수집한 이용목적에 벗어나지 않는다는 주장도 가능할 것이다. 그러나 대법원은 엄격하게 해석하는 태도를 고수하며 이러한 주장을 인정하지 않았다.

108) 개인정보보호법 제15조 제2항 단서, 제17조 제2항 단서, 정보통신망법 제22조 제1항 단서, 제24조의2 제1항 단서 등

109) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안 (김병욱의원 대표발의), 의안번호 16636, 2018. 11. 15.

노웅래 등 10인의 국회의원은 2018. 11. 15. 정보통신망법 일부개정법률안을 발의하였다. 위 개정안은 인재근 의원안과 함께 발의되어 같이 통과되는 것을 전제로 마련된 것으로, 그 목표는 개인정보보호와 관련된 정보통신망법 조항을 모두 개인정보 보호법으로 옮겨 개인정보보호 법령을 개인정보 보호법으로 일원화하는 것에 있다. 따라서 개인정보 동의제도에 대한 내용은 실질적으로 인재근 의원안과 동일하다.

특히 일반 개인정보처리자와 달리 정보통신서비스 제공자등이 개인정보 처리에 대해 지나치게 강화된 규제를 할 필요성에 대해서는 근본적인 재검토가 불가피한 것으로 생각된다.

3. 신용정보법 개정안(김병욱 의원안[110])

가. 주요 내용

김병욱 등 13인의 국회의원은 2018. 11. 15. 신용정보법 일부개정법률안(이하 "김병욱 의원안")을 발의하였다. 개인정보보호법령의 전반적인 개정을 목적으로 한 인재근 의원안과 달리, 김병욱 의원안은 본인신용정보관리업(마이데이터), 전문개인신용평가업 및 개인사업자신용평가업과 같은 구체적인 업무를 신용정보법에 도입하거나, 빅데이터 분석 및 이용을 위한 법적 근거를 추가하는 등 데이터 경제로의 전환을 위하여 필요한 제도를 마련하는, 보다 구체적인 목적을 갖고 있다.

김병욱 의원안은 본인신용정보관리업을 영위하기 위해서는 금융위원회로부터 허가를 받도록 하는 등(안 제2조 제9호의2, 제4조 제1항) 마이데이터 산업과 관련된 여러 내용을 담고 있다. 그 중 개인정보 처리를 위한 동의 제도에 관하여는, 개인신용정보 활용 동의를 받을 때 중요사항을 우선적으로 고지할 수 있다는 취지의 제34조의2 제3항 및 제4항이 가장 연관성이 크다. 구체적인 내용은 다음과 같다.

제34조의2(개인신용정보 등의 활용에 관한 동의의 원칙) ③ 대통령령으로 정하는 신용정보제공·이용자는 제1항에도 불구하고 **고지사항 중 그 일부를 생략하거나 중요한 사항만을 발췌하여 그 신용정보주체에게 알리고 정보활용 동의를 받을 수 있다.** 다만, 개인인 신용정보주체가 고지사항 전부를 알려줄 것을 요청한 경우에는 그러하지 아니하다. ④ 제3항 본문에 따라 고지사항 중 그 일부를 생략하거나 중요한 사항만을 발췌하여 정보활용 동의를 받는 경우에는 같은 항 단서에 따라 신용정보주체에게 고지사항 전부를 별도로 요청할

110) 신용정보의 이용 및 보호에 관한 법률 일부개정법률안 (김병욱의원 대표발의), 의안번호 16636, 2018. 11. 15.

수 있음을 알려야 한다.

이외에도 김병욱 의원안은 정보활용의 위험도, 이로 인하여 신용정보주체가 받는 이익 등을 고려하여 등급을 부여한 후 정보활용 동의를 받을 때 이러한 등급을 같이 고지하도록 하는 이른바 동의 등급제를 도입하고자 한다.

제34조의3(정보활용 동의등급) ① 대통령령으로 정하는 신용정보제공·이용자는 정보활용 동의 사항에 대하여 **금융위원회가 평가한 등급(이하 이 조에서 "정보활용 동의등급"이라 한다)을 신용정보주체에게 알리고 정보활용 동의**를 받아야 한다. 정보활용 동의 사항 중 대통령령으로 정하는 중요사항을 변경한 경우에도 같다.
② 금융위원회는 제1항에 따른 평가를 할 때 다음 각 호의 사항을 고려하여 **정보활용 동의등급을 부여하여야 한다.**
1. 정보활용에 따른 사생활의 비밀과 자유를 침해할 위험에 관한 사항(활용되는 개인신용정보가 「개인정보보호법」 제23조에 따른 민감정보인지 여부를 포함한다)
2. 정보활용에 따라 신용정보주체가 받게 되는 이익이나 혜택
3. 제34조의2제2항제1호 및 제2호의 사항
4. 그 밖에 대통령령으로 정하는 사항

또한, 김병욱 의원안은 정보주체의 열람권, 정정권 등 각종 권리행사를 대리인에게 하게 할 수 있다는 점을 명문화하였다(안 제39조의3). 대리 가능한 권리행사로는 열람권, 정정권 외에도 동의 철회권 뿐 아니라, 후술하는 개인신용정보 전송요구권도 포함되어 있다.

제39조의3(신용정보주체의 권리행사 방법 및 절차) ① 신용정보주체는 다음 각 호의 권리행사(이하 "열람등요구"라 한다)를 서면 등 대통령령으로 정하는 방법·절차에 따라 **대리인에게 하게 할 수 있다.**
1. 제33조의2제1항에 따른 전송요구
2. 제36조제1항에 따른 고지요구
3. 제36조의2제1항에 따른 설명요구 및 제2항 각 호의 어느 하나에 해당하는 행위
4. 제36조의3제1항에 따른 설명요구
5. 제37조제1항에 따른 동의 철회 및 제2항에 따른 연락중지 청구
6. 제38조제1항 및 제2항에 따른 열람 및 정정청구
7. 제38조의2제1항에 따른 통지 요청
8. 제39조에 따른 무료열람
9. 제39조의2제2항에 따른 교부 또는 열람
② 만 14세 미만 아동의 법정대리인은 신용정보회사등에게 그 아동의 개인신용정보에 대하여 열람등요구를 할 수 있다.

이와 관련하여 주목할 만한 점은, 마이데이터 사업자가 위와 같은 정보주체의 권리행사 대리업무를 수행할 수 있도록 하였다는 것이다. 즉, 김병욱 의원안은 본인신용정보관리회사의 부수업무로 안 제39조의3 제1항 각호의 권리를 대리 행사하는 업무를 포함시켰다. 이에 의하면 마이데이터 사업자는 개인신용정보주체의 위임을 받아 개인신용정보 전송요구권을 대리행사 하는 것이 명시적으로 허용되는 것이다.

> 제11조의2(부수업무) ⑤ 본인신용정보관리회사의 부수업무는 다음 각 호와 같다.
> 1. 해당 신용정보주체에게 제공된 본인의 개인신용정보를 기초로 그 본인에게 하는 데이터 분석 및 컨설팅 업무
> 2. 신용정보주체 본인에게 자신의 개인신용정보를 관리·사용할 수 있는 계좌를 제공하는 업무
> **3. 제39조의3제1항 각 호의 권리를 대리 행사하는 업무**
> 4. 그 밖에 대통령령으로 정하는 업무

참고로 전술한 바와 같이 GDPR은 정보주체가 자신이 지정한 정보처리자에게 정보를 이전하여 줄 것을 요구하는 권리인 정보이동권을 도입하였는데, 김병욱 의원안은 이러한 정보이동권을 "개인신용정보의 전송 요구"라는 명칭으로 금융분야에 도입하였다. 즉, 김병욱 의원안에 따르면 개인신용정보주체는 일정한 정보처리자에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 정보주체 본인[111]이나 본인신용정보관리회사 등에게 전송하여줄 것을 요구할 수 있다(안 제33조의2 제1항).

개인신용정보의 전송 요구는 정보주체가 능동적으로 정보이동을 요구한다는 측면에서 기업의 정보활용 요청에 대한 수동적인 동의와는 구분되지만[112], 여전히 정보주체의 의사를 확인하는 것은 필요하다. 이에 따라 김병욱 의원안은 정보주체가 개인신용정보의 전송을 요구할 때 중요 사항을 특정하여 전자문서 등 안전성과 신뢰성이 확보된 방법으로 하도록 하고, 정보주체의 철회권을 보장하였으며, 정보처리자 역시 정보주체의 본인확인이 안 되는 경우에는 전송요구를 거부할 수 있도록 하였다(안 제33조의2 제5, 7, 8항).

> 제33조의2(개인신용정보의 전송 요구) ⑤ 개인인 신용정보주체가 제1항 각 호의 어느 하나에 해당하는 자에게 제1항에 따른 전송요구를 할 때에는 다음 각 호의 사항을 모두 특정하여 전자문서나 그 밖에 안전성과 신뢰성이 확보된 방법으로 하여야 한다.
> 1. 신용정보제공·이용자등으로서 전송요구를 받는 자
> 2. 전송을 요구하는 개인신용정보
> 3. 전송요구에 따라 개인신용정보를 제공받는 자
> 4. 정기적인 전송을 요구하는지 여부 및 요구하는 경우 그 주기

111) 김병욱 의원안이 정보주체 본인에 대한 전송을 요청할 수 있도록 한 것은, GDPR 제20조 개인정보 이동권에서 개인정보를 수령할 권리를 규정한 것이 대응한 것으로 보이나, 이 경우 현행 신용정보법에서 이미 인정되고 있는 열람청구권과의 관계를 명확하게 정리할 필요가 있다는 지적에 관하여는, 고환경 · 손경민 · 주성환, 앞의 논문, 31면 참조.

112) 금융위원회, 금융분야 마이데이터산업 도입방안, 2018, 16면.

5. 그 밖에 대통령령으로 정하는 사항
⑦ 개인인 신용정보주체는 제1항에 따른 전송요구를 철회할 수 있다.
⑧ 제1항에 따라 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다.

나. 개정안에 대한 평가

마이데이터 서비스는 여러 창의적인 방법으로 개인정보를 처리하기 때문에 개인정보를 수집할 당시 어떠한 개인정보를 어떠한 목적으로 활용할지 예측하는 것이 어려울뿐더러, 이를 모두 적시하는 것은 동의서 양을 과도하게 방대해지도록 하는 효과를 가져 온다. 이는 마이데이터 사업자 입장에서 동의서 작성 업무에 상당한 시간을 소모해야 한다는 부담으로 작용한다.

그러나 더 큰 문제는 이렇게 복잡하고 긴 동의서가 동의 규제의 역설의 주요 원인이 된다는 것이다. 즉, 앞서 살펴봤듯이 충분한 정보를 제공하고자 할수록 동의서는 길어지고, 이로 인하여 정보주체는 고지사항을 제대로 읽지 않아 자신이 어떠한 정보를 제공하는지도 모른 채 개인정보를 제공하게 되며, 사업자들은 면죄부를 얻게 되는 "동의규제의 역설[113]"이 발생한다. 개인정보자기결정권을 보장하기 위하여 설계된 엄격한 동의 제도가 오히려 위 권리의 실현을 방해하는 것이다.

따라서 김병욱 의원안처럼 고지사항 중 일부를 생략하거나 중요한 사항만을 알리도록 하는 것은 이러한 동의규제의 역설을 해결할 수 있는 하나의 좋은 방안이 될 것이다. 정보주체가 읽고 이해할 수 있는 양의 동의서가 마련되면, 정보주체는 자신의 개인정보가 어떻게 이용되는지 보다 명확하게 파악할 수 있을 것이고, 이러한 이해를 기초로 하여 적극적으로 개인정보자기결정권을 행사할 수 있을 것으로 기대된다. 특히, 정보제공의 단순화는 정보제공의 실질화를 유도하여 알고 하는 동의가 구현되는 것에 도움이 될 것[114]이다. 사업자의 입장에서는 동의서 작성에 소요되는 시간과 비용을 절약할 수 있다는 점에서 모두에게 이로운 개정안이라고 평가할 수 있다.

실제로 정무위원회는 김병욱 의원안에 대하여 "개정안은 신용정보주체가 정보활용 동의 사항을 이해할 수 있도록 정보활용 동의서를 단순화하고, (중략) 정보주체의 인지적 한계를 보완할 수 있고 해당 개인신용정보를 제공·활용하는 금융회사 역시 업무상 불필요하게 정보를 요구하는 행태가 줄어들 것으로 기대되는 바, 바람직한 입법조치로 사료

113) 고환경, [칼럼] 개인정보 동의 및 파기 규정의 적정성에 관하여 (고환경 변호사) (2015. 7. 23.), https://blog.naver.com/n_privacy/220427876061
114) 권영준, 앞의 논문 p. 713

됨"이라고 평가하였는데[115], 이는 개정안에 대한 위 평가와 일치한다.

김병욱 의원안이 정보주체의 권리행사 대리업무를 본인신용정보관리회사의 부수업무로 포함시킨 것은, 특히 대리 가능한 권리행사 중에 정보이동권(개인신용정보 전송 요구권)이 포함되어 있다는 점을 감안하면 상당히 주목할 만한 입법이라고 평가할 수 있다.

제2절 개인정보 보호 관련 제도 개선방안 검토

1. 동의 방식 개선 등 관련 법령의 개정을 통한 제도 개선 방안

가. 일괄(포괄) 동의 도입 방안

개인정보 처리 동의 제도 개선 방안과 관련하여 우선 일괄(포괄) 동의의 도입을 고려해 볼 수 있다. 현행 개인정보보호 법령은 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 각각 동의를 받아야 한다고 하여,[116] 일괄 동의를 금지하고 있으며, 하급심 판례는 과거 신용정보법 역시 일괄(정확히는 포괄) 동의를 받아 개인신용정보를 처리하는 것을 금지하고 있다고 판시[117]한 바 있다. 결국, 일괄적 동의를 위해서는 법률의 개정이 필요하다.

물론 일괄 동의는 마이데이터 사업자의 개인정보 동의 획득 부담을 경감시킨다는 점에서 긍정적인 측면이 있다. 참고로 우리나라와 같은 상세한 동의제도를 두고 있지 않은 미국에서는 아래와 같은 화면[118]을 통해서만 개인정보 처리에 대한 동의를 받고 있다. 그러나 이를 무조건적인 대안으로 받아들이기 보다는, 이에 대해 보다 면밀한 검토를 선행하는 것이 바람직해 보인다. 개인정보처리방침의 고지 및 정보처리 유형을 불문한 포괄 동의 허용 방식은 동의 절차 자체는 단순하지만 간접적으로 확인 가능한 개인정보처리방침 자체의 정보는 방대하기 때문에, 개인정보자기결정권 행사를 적정하고 실질적으로 보장하는지에 대하여 부정적인 견해가 제기될 수도 있을 것이기 때문이다. 결국 알고 하는 동의를 위해서는 정보제공의 실질화를 위한 방안을 고민할 필요가 있다는 점[119]을 유의할 필요가 있을 것이다.

115) 정무위원회, 신용정보의 이용 및 보호에 관한 법률 일부개정법률안 검토보고(<빅데이터 분석·이용의 법적 근거 명확화 등>, 김병욱의원대표발의(의안번호 제16636호)) (2018. 12.), 107~108면.

116) 개인정보보호법 제22조 제1항, 정보통신망법 제24조의2 제3항 참고

117) 서울고등법원 2010. 5. 10.자 2009라1941 결정. 구체적으로 서울고등법원은 신용정보법의 규정을 종합하면, 신용정보법에서 규정하고 있는 동의는 "일반적·포괄적 동의가 아니라 구체적·개별적 동의로 해석되고", 따라서 "판매자의 개인신용정보는 법률상 판매자가 구체적·개별적으로 동의한 경우에만 채무자가 채권자들에게 제공할 수 있는 것이지 채무자가 임의로 제공하거나 사전에 일반적·포괄적 동의를 받아 제공할 수 있는 것은 아님이 인정된다"고 하였다.

118) 미국의 대표적인 커뮤니티 웹사이트인 reddit의 회원가입 화면이다(https://www.reddit.com/)

119) 권영준, 앞의 논문 p. 713

By clicking next, you agree to our Terms and that you have read our Privacy Policy and Content Policy.

위 미국의 사례를 받아들인다면, 이미 우리 법에서 개인정보처리방침 공개 의무를 규정하고 있는 만큼, 개인정보처리방침을 공개하여 개인정보처리 관련 법정고지사항을 충실하게 고지하고, 이에 동의하는 방안을 원칙으로 하고, 민감정보 이용 등의 특별한 경우를 예외로 규정하는 방안을 고려해볼 수 있다.

나. 유형고지 도입 방안

그렇다면 개인정보의 실질화는 어떻게 실현할 수 있을까. 무엇보다도 정보제공을 단순화[120]하여야 한다는 주장을 참고할 필요가 있다. 이를 위한 대안에는 유형고지의 도입이 있다. 중요한 사항을 요약하여 고지할 수 있도록 하는 김병욱 의원안과 유사한 면이 있는 제도이다. 처리하는 모든 개인정보 항목, 개인정보 처리의 목적, 개인정보를 제공받는 제3자 등을 나열하는 것이 아니라, 이들을 일정한 유형으로 그룹화하여, 이런 유형에 대한 정보를 정보주체에 제공하여 어떤 정보들이 수집 이용 또는 제공될 지를 정보주체가 합리적으로 예측할 수 있도록 하는 것이다.

개인정보 보호의 국제적 일반규율로서 자리잡아가고 있는 유럽연합의 GDPR은 앞서 본 바와 같이 정보주체의 동의에 근거하여 개인정보를 처리하는 것을 다음과 같이 허용한다.

Article 4 Definitions
For the purposes of this Regulation:

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

제4조 정의
본 규정의 취지에 따르면

120) 권영준, 앞의 논문 p. 715

(11) 개인정보주체의 동의는 본인과 관련된 개인정보의 처리에 대해 합의한다는 개인정보주체의 희망을 진술 또는 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 의사표시를 가리킨다.
Article 6 Lawfulness of processing 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; **제6조 처리의 적법성** 1. 개인정보 처리는 적어도 다음 각 호의 하나에 해당되고 그 범위에서만 적법하다. (a) 개인정보주체가 하나 이상의 특정 목적에 대해 본인의 개인정보 처리를 동의한 경우

제4조에서 말하는 사전에 정보를 제공받은(informed) 동의가 이루어지기 위해서는 정보주체의 선택을 도울 수 있는 핵심 정보를 정보주체에게 알려주어야 하는데, 이때 개인정보 항목이 아닌 유형을 알리는 것도 가능하다는 것이 EU 규제기관의 입장[121]이다.

현행 데이터 3법이 유형 고지를 금지하는지 여부는 불분명하다. 예를 들어, 개인정보보호법은 개인정보를 제3자에 제공하기 위해서는 (i) 개인정보를 제공받는 자 (ii 개인정보를 제공받는 자의 개인정보 이용 목적 (iii) 제공하는 개인정보의 항목 (iv) 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 (v) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 알리고 동의를 받도록 규정하고 있는데[122], 얼마나 상세하게 이러한 정보를 적어야 하는지는 구체적으로 규정[123]하고 있지는 않기 때문이다.

단, 규제기관은 이를 허용하지 않는 입장임은 분명해 보인다. 앞서 언급한 바와 같이 행정안전부는 개인정보 제3자 제공을 위한 위 법정 고지사항 중 (i) 개인정보를 제공받는 자에 대하여 "'개인정보를 제공받는 자'란 제공받는 자의 이름 또는 상호를 의미하므로, 금융기관, 정부기관 등과 같이 정보주체가 제공받는 자를 알기 어렵도록 포괄적으로 알려서는 아니" 된다고 하여 유형 고지를 금지하고 있다[124].

121) Article 29 Working Party, Guidelines on onsent under Regulation 2016/679(2017. 11. 28.), p. 13.
122) 개인정보보호법 제15조 제2항
123) 물론, "개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처)"(정보통신망법 제63조 제3항 제3호)처럼 법정 고지사항을 구체적으로 기재하는 경우도 있다.
124) 행정안전부, 개인정보보호 법령 및 지침·고시 해설서, 2016, 92면

결국 유형 고지 방안을 하나의 유효한 수단으로 인정하기 위해서는 이를 명시적으로 인정하는 입법 작업이 필요할 것으로 생각된다. 규제기관의 입장이 확고한 상황에서 불확실한 법령 해석에 의존하는 것보다는 확실한 규정 도입을 통해 사업자가 안심하고 마이데이터 산업에 참여할 수 있도록 유도하는 것이 보다 효율적이기 때문이다.

다. 동의제도 위반에 따른 형사처벌 규정의 개정

앞서 살펴봤듯이, 데이터 3법은 과징금이나 과태료와 같은 행정적 제재뿐만이 아니라 징역 또는 벌금과 같은 형사적 제재까지 동원하여 동의제도 위반을 규율한다. 이는 GDPR에서조차 발견되지 않는 한국 데이터 3법의 주요 특징 중 하나인데, 문제는 형사처벌이 법위반 예방에 효과적인지에 대해 의문이 제기되고 있다는 것이다. 여러 가지 이유가 있겠으나, 지나치게 엄격한 법령이 오히려 해당 법령의 활용도를 낮추는 효과를 가지고 온다는 지적이 제기되고 있는 것이다. 또, 기본적으로 형사 제재는 개인에게 부과되기 때문에, 기업보다 업무 담당자 개인에게 책임을 전가한다는 지적이 제기되고 있고, 기업을 규율하는 데 한계가 있다는 비판도 존재한다.

이를 해결하기 위해서는 형사제재 규정을 개정할 필요가 있다. 형벌은 최후의 수단이며, 죄질과 책임에 상응하도록 적절한 비례성을 갖춰야 한다는 점[125], 동의 방식에 관한 규제를 일부 준수하지 못하였다는 것은 실체적 위반이기 보다는 절차적 위반인데 이에 대하여도 형사처벌 하는 것은 부당하다는 점 등을 모두 고려하면, 동의제도 위반보다 불법성이 더 큰 행위에 대하여 형사적 제재를 적용하는 것이 타당하다. 예를 들어, 현행 정보통신망법처럼 단순히 이용자의 동의를 받지 아니하고 개인정보를 수집한 자를 형사처벌 할 것[126]이 아니라, 동의를 받지 않는 것에 더하여 “부정한 목적”등을 갖는 등 추가적인 사실관계가 인정되는 경우에만 형사적 수단을 활용하는 것을 생각할 수 있다.

참고로, 김병관 의원 등 11인은 2019. 10. 15. 개인정보 보호법 개정안[127]을 발의하였다. 그 내용을 살펴보면, 개인정보 유출을 방지하기 위해서는 법인을 규제하여야 하고, 이를 위해서는 형사처벌보다 과징금이 효과적이라는 생각에 기초하여, 현행 개인정보 보호법의 개인정보 유출에 따른 형사처벌 조항[128]을 삭제하고, 과징금 조항을 추가하도록 하고 있다. 이는 개인정보 유출뿐만이 아니라 동의제도에도 마찬가지고, 추후 데이터 3법의 형사처벌 조항을 검토할 때도 반드시 고려하여야 할 것이다.

---

125) 한국사법행정학회, 주석형법(2011. 11. 30.), 67면
126) 정보통신망법 제71조 제1항 제1호
127) 개인정보보호법 일부개정법률안 (김병관의원 대표발의), 의안번호 22890, 2019. 10. 15.
128) 개인정보 보호법 제73조 제1호 참고

라. 정당한 이익에 근거한 개인정보 처리의 도입

다만 앞서 언급한 수준의 동의 제도의 부분 개선만으로는 개인정보보호의 실질화와 데이터 활용 촉진이라는 두가지 정책 목적을 달성하기 부족할 것으로 생각된다. 특히 그동안의 관행 등에 비추어볼 때 근본적인 규제 패러다임이 변화되지 않으면 개인정보 수집, 이용 및 제공에 있어 동의제도에 의존하는 사업자들의 관행은 쉽게 바뀌지 않을 것으로 예상되기 때문이다. 전술했듯이 4차 산업혁명 시대에 보편화화되고 있는 초연결 사물인터넷 체제 하에서 사전에 정보주체로부터 일일이 개인정보 처리에 대한 동의를 받는 것은 실질적으로 불가능하다는 점을 고려하면, 우리는 동의 제도에 의존하는 것에서 벗어나 규제 패러다임을 근본적으로 변화시켜야 할 것으로 생각한다.

이를 위해 다시 GDPR을 살펴볼 필요가 있다. GDPR은 물론 동의에 의한 개인정보 처리를 허용하고 있으나, 이는 제한적으로만 활용되는 수단이다. 왜냐하면 앞에서도 설명한 바와 같이 적법한 동의가 되기 위해서는 다음과 같은 엄격한 조건을 충족하여야 하기 때문이다.

Article 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

제7조 동의의 조건
1. 처리가 동의를 기반으로 이루어지는 경우, 개인정보처리자는 개인정보주체가 본인의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.

2. 개인정보주체의 동의가 기타의 사안과도 관련된 서면의 진술서로 제공되는 경우, 동의 요청은 그 기타의 사안과 분명히 구별되는 방식으로, 이해하기 쉽고 입수가 용이한 형태로, 명확하고 평이한 문구를 사용한 방식으로 제시되어야 한다. 진술서의 어느 부분이라도 본 규정을 위반하는 경우 그 구속력이 인정되지 않는다.

3. 개인정보주체는 언제든지 본인의 동의를 철회할 권리를 가진다. 동의의 철회는 철회이전에 동의를 기반으로 한 처리의 적법성에 영향을 미치지 않는다. 개인정보주체는 동의를 제공하기 전에 이 사실에 대해 고지 받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.

4. 동의가 자유롭게 제공되는지 여부를 평가할 때, 무엇보다 서비스 제공 등의 계약의 이행이 해당 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 한다.

특히 제7조 제3항은 정보주체가 언제든지 동의를 철회하는 것을 허용하기에, 동의만을 적법한 개인정보 처리의 근거로 삼는 것은 중장기적인 관점에서 바람직하지 않다. 오히려 많은 EU 내의 사업자는 아래의 정당한 이익(legitimate interest) 조항에 기초하여 개인정보를 처리한다.

Article 6 Lawfulness of processing
1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

제6조 처리의 적법성
1. 개인정보 처리는 적어도 다음 각 호의 하나에 해당되고 그 범위에서만 적법하다.

(f) 개인정보처리자 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우로서, 개인정보가 보호되어야 할 개인정보주체의 이익 또는 기본적 권리와 자유가 우선되는 경우는 제외한다.

개인정보주체가 어린이인 경우에는 특히 그러하다.

우리나라는 이와 유사한 규정을 개인정보보호법 제15조 제1항 제6호[129]에 두고 있지만, 매우 한정적인 경우에만 그 적용을 허용한다. 개인정보처리자의 정당한 이익을 위해서 뿐만이 아니라, 이러한 이익이 "명백하게" 정보주체의 권리보다 우선하여야 하기 때문에, GDPR과 같이 일반적인 개인정보 수집 및 이용의 근거가 되기는 어렵다. 행정안전부 역시 "EU에서는 이익형량의 원칙에 따라 정보주체의 이익과 개인정보처리자의 이익을 비교 형량하도록 하고 있으나 우리나라에서는 개인정보처리자의 이익이 명백히 우선하는 경우에만 개인정보 수집이 허용된다"고 하여(행정안전부, 전게 해설 81면) 정당한 이익에 따른 개인정보 처리를 제한적으로만 인정하는 태도를 취하고 있는 것이다. 심지어 정보통신망법은 이러한 취지의 규정조차 두고 있지 않다. 그러므로 추후 입법 작업을 통하여 개인정보처리자의 정당한 이익에 근거한 개인정보 처리를 허용하는 것이 필요하다.

참고로 대통령직속 4차 산업혁명위원회는 2019. 10. "4차 산업혁명 대정부 권고안"을 발표하였는데, 여기에는 경직된 개인정보보호 법제 등을 개선하여야 할 필요성과 "개인정보에 관한 권리는 헌법상 비례의 원칙에 따라 다른 이익과의 형량을 통해 보호 수준이 합리적으로 재설정되어야 한다. 보다 근본적으로는 개인의 사생활·인격권 보호 및 개인정보자기결정권의 실질적 보장이라는 목적을 위하여 법제가 구성되는 것이 바람직하다"는 선언이 포함되어 있다[130]. 비례의 원칙에 따른 개인정보자기결정권 보호를 요구한 것은 GDPR에서의 정당한 이익에 따른 개인정보 처리를 염두에 두고 이루어진 것으로 판단된다.

2. 현행 법령 내에서의 동의 제도 개선 방안

앞선 방안은 모두 데이터 3법의 추가적인 개정을 전제로 한 논의다. 그렇다면 현행 법령의 개정 없이 동의 제도를 개선하는 새로운 방법은 없을지, 특히 개인정보 처리 동의권의 포괄적인 대리행사를 위임하는 것이 가능한지, 스마트 컨트랙트의 도입이 가능한지에 대하여 살펴보겠다.

가. 현행 법률 하에서 개인정보 처리 동의권의 포괄적인 대리행사를 위임하는

129) 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

130) 대통령직속 4차 산업혁명위원회, 4차 산업혁명 대정부 권고안(2019. 10.), 69~70면

것이 가능한지 여부

마이데이터 서비스 제공자들이 현행 데이터 3법에서 겪는 어려움을 극복할 수 있는 방법에는 정보주체가 개인정보 처리에 관한 동의권 행사를 마이데이터 서비스 제공자들에게 포괄적으로 대리행사 하도록 하는 방안이 있다. 이것이 가능하다면 사업자들은 하나의 계약서를 통해 필요한 모든 개인정보 처리를 할 수 있어서, 앞서 살펴본 동의 제도의 문제를 극복하면서 마이데이터 서비스를 제공할 가능성이 열릴 것이다.

개인정보보호법은 개인정보 처리에 대한 동의권 행사를 대리할 수 있다는 취지의 규정을 두고 있지 않다. 참고로 동법 제38조 제1항[131]은 대리를 허용하고 있으나, 이는 개인정보 열람 등 요구에 대한 것이지, 개인정보 처리에 대한 것이 아니다. 그렇다면 개인정보 처리에 대한 동의는 대리(특히 법정 고지사항이 구체적으로 고지되지 않은 상황에서 이루어지는 포괄적인 대리)가 불가능하다는 주장이 가능할 수 있다. 즉, 개인정보보호법은 대리가 가능한 경우를 구체적으로 정하고 있으므로, 별도로 정하지 않은 경우에 대하여는 해석상 대리가 허용되지 않는다는 것이다. 그러나 이 주장의 타당성을 판단하기 위해서는 대리에 대한 논의를 좀 더 구체적으로 살펴볼 필요가 있다.

일반적으로 대리는 법률행위를 대리하는 것이기 때문에 법률행위 내지 의사표시에 한하여 허용된다. 하지만 구체적으로 법률에서 대리를 금지하거나 그 성질이 대리행위와 적합하지 않은 때에는 대리가 허용되지 않는다. 후자를 “대리에 친하지 않은 법률행위”라고 하는데, 이는 특히 민법에 규정된 친족법이나 상속법상의 이른바 일신전속적 행위 또는 일신전속적 권리에 의한 행위에 많다[132].

단, 일신전속적 권리에 의한 법률행위라고 하여 모두 대리에 친하지 않은 법률행위가 되는 것은 아니다. 일신전속적 권리에는 행사상 일신전속권과 귀속상 일신전속권이 있다. 전자는 권리를 행사할지 말지가 그 시점에서 권리자의 의사에만 맡겨져 있는 권리로서 권리자의 의사에 반해 그 행사를 강제할 수 없는 권리를 지칭하고, 후자는 어느 특정인에게만 귀속되어야 하고 타인에게 이전되는 경우에는 아무런 의미가 없게 되는 권리를 의미한다. 즉, 행사상 일신전속성은 권리의 행사를 권리자의 의사에 절대적으로 맡기는지의 문제인 반면, 귀속상 일신전속성은 권리의 양도 및 상속에 의한 승계를 인정할 수 있는지의 문제다[133]. 그렇다면 권리의 행사를 타인의 의사에 맡기는 것을 본질적인 내용으로 하

131) 제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.

132) 이영준, 민법총칙, 박영사, 2007, 487면

133) 정구태, 유류분반환청구권의 일신전속성, 679면. 참고로, 행사상 일신전속권과 귀속상 일신전속권은 이렇게 별개의 문제에 대한 개념이기 때문에 서로 일치하기도 하지만 일치하지 않는 경우도 다수 존재한다. 예를 들어, 판례는 위자료청구권은 행사상의 일신전속권에는 속하지만 귀속상의 일신전속권은 아니라고 한다(대법원 1993. 5. 27 선고 92므143 판결).

는 대리는 행사상 일신전속권에는 허용될 수 없고, 따라서 행사상 일신전속권에 기초한 법률행위는 “대리에 친하지 않은 법률행위”라고 할 것이다. 반면 권리의 양도성 여부는 대리의 가능성과는 별개의 문제이기 때문에 귀속상 일신전속권에 기초한 법률행위는 대리에 친하지 않은 법률행위라고 단정할 수 없을 것이다.

한편, 판례는 인격권의 일종인 저작인격권[134]과 관련하여, 저작인격권은 양도하거나 이전할 수는 없는 귀속상의 일신전속권이지만 대리하거나 위임하는 것은 가능하기에 행사상의 일신전속권은 아니라는 취지로 판시하였다. 단, 저작인격권을 포괄적으로 대리하는 것은 실질적으로 이를 양도하는 것이기 때문에 가능하지 않다고 하였다[135].

개인정보의 처리에 대한 동의권은 개인정보의 처리에 대한 최초의 결정권을 부여하는 것이기 때문에, 개인정보자기결정권에 근거한 권리다[136]. 개인정보의 재산적 가치를 이유로 개인정보자기결정권을 일종의 재산권으로 파악하는 입장이 없는 것은 아니다. 하지만 헌법재판소는 개인정보자기결정권의 근거 중 하나로 헌법 제10조 제1문의 일반적 인격권을 제시하고 있다는 점[137], 개인정보자기결정권을 물권/채권의 재산권 체계 속에 위치시키는 것은 이론적으로도 적절하지 않은 점, 개인정보가 재산적 가치를 지니고 있다고 하여 개인정보자기결정권이 재산권이라고 하는 것은 논리적 비약인 점을 고려하면[138], 개인정보자기결정권과 이에 근거한 개인정보 처리에 대한 동의권은 인격권에 해당한다는 견해 또한 유력하다.

그렇다면 인격권인 개인정보 처리에 대한 동의권은, 앞서 본 판례에 따라 대리가 허용된다는 결론을 도출할 수 있다. 이에 더하여 실무상 개인정보 수집 행위는 위탁도 가능하고, 이 경우 동의를 대신해서 받게 된다는 점을 고려하면, 개인정보 처리에 대한 동의를 대리하는 것은 금지되지 않는다고 보는 것이 타당하다.

그러나 저작인격권에 대한 대법원 판례가 명시하듯이 귀속상 일신전속권의 포괄적 대리는 허용된다고 보기 어려운 점, 명시적으로 대리를 허용하고 있는 개인정보 열람 등과 달리 개인정보의 처리에 대한 동의에 대하여는 대리와 관련된 규정이 없기에 포괄적인 대리는 개인정보보호법 해석과 충돌될 수 있다는 점을 고려하면, 개인정보 처리에 대한

---

134) 저작권법 제14조(저작인격권의 일신전속성) ①저작인격권은 저작자 일신에 전속한다.
② 저작자의 사망 후에 그의 저작물을 이용하는 자는 저작자가 생존하였더라면 그 저작인격권의 침해가 될 행위를 하여서는 아니 된다. 다만, 그 행위의 성질 및 정도에 비추어 사회통념상 그 저작자의 명예를 훼손하는 것이 아니라고 인정되는 경우에는 그러하지 아니하다

135) 대법원 1995. 10. 2 자 94마2217 결정: “저작인격권은 저작재산권과는 달리 일신전속적인 권리로서 이를 양도하거나 이전할 수 없는 것이라 할 것이므로 비록 그 권한행사에 있어서는 이를 대리하거나 위임하는 것이 가능하다 할지라도 이는 어디까지나 저작인격권의 본질을 해하지 아니하는 한도 내에서만 가능하다 할 것 (중략) 포괄적으로 위임되었다는 것을 전제로 피신청인들에 의한 이 사건 저작물의 저작자표시 변경이 신청인의 저작인격권의 침해로 되지 않는다고 판단하고 있는바, 이는 실질상 저작인격권의 양도를 인정하는 결과로 되어 저작인격권의 본질을 벗어나는 것이 되므로 허용되어서는 아니된다.”

136) 권영준, 앞의 논문 685면

137) 헌법재판소 2005. 5. 26. 자 99헌마513, 2004헌마190(병합) 결정

138) 권영준, 앞의 논문 682면

동의권의 포괄적인 대리행사를 위임하는 것이 가능한지에 대해서는 반론의 여지 또한 있고, 결국 이는 입법적 해결 내지 법원의 판결을 통한 해석이 이루어질 필요가 있는 사안이라고 볼 수 있다. 앞서 설명한 바와 같이 개인정보 동의 규제 위반의 경우 형사처벌 등 다양한 법적 리스크가 발생하기 때문에, 법리적으로 명확하게 정리되지 않은 사항에 대하여 사업자로 하여금 법적 리스크를 부담할 것을 강요하기는 어려울 것이기 때문이다.

요컨대 이와 같은 해석상의 논란 가능성을 극복하고 마이데이터 사업자에게 포괄적으로 대리권을 부여하고자 한다면, 이를 적극적으로 허용하는 법률 개정을 하는 방안을 고려하여 볼 필요가 있겠다. 전술한 바와 같이 일본의 정보은행 서비스는 GDPR의 정보이동권 도입 없이도 마이데이터 서비스와 유사하면서도 폭넓은 정보활용을 가능하게 하였는데, 정보주체의 개인정보처리에 관한 동의에 대한 권리의 마이데이터 사업자에 의한 포괄적 대리권 수여가 가능해 진다면, 이미 법적 · 제도적 연구가 상당 부분 진척된 일본의 정보은행 산업과 연계하여 마이데이터 산업을 진흥케 할 방안을 모색할 수 있을 것이다.

지금까지의 논의를 종합하면, 결국 개인정보 처리에 대한 동의권이 양도되었다고 볼 만한 수준으로 판단되지 않는 범위에서는 그 행사를 마이데이터 사업자가 대리하도록 하는 것이 가능하다는 해석은 법리적 근거가 있다는 주장이 가능할 것으로 보인다. 다만 어느 정도의 범위에서 동의권의 행사를 위임해야 하는지(특히 개인정보보호법에 따른 법정 고지사항을 고지하지 않은 상황에서 동의권에 대한 포괄적인 대리행사 위임이 가능한지 여부), 마이데이터 사업자가 제공하는 서비스를 정보주체가 이용하기 위해 필요한 범위에서 동의권을 위임하는 것으로 정하면 충분할지, 수집 및 이용, 제공, 위탁, 변경 동의 또는 필수적, 선택적 동의 등 동의권의 종류를 한정하여 위임하면 가능할지 등에 대해서는 보다 면밀한 추가 검토가 필요할 것이다.

나. 스마트 컨트랙트를 통한 개인정보 동의절차 도입 가능 여부

근래 블록체인 기술의 활용도가 증가하면서 블록체인을 통해 실현할 수 있는 스마트 컨트랙트에 대한 관심이 높아지고 있다. 여기서 스마트 컨트랙트란 인간의 개입 없이 계약 조건이 자동적으로 이행 및 집행되는, 디지털화되고 컴퓨터 입력이 가능한 계약서다[139]. 물론, 이러한 스마트 컨트랙트를 코딩 지식 등이 없는 일반인도 읽을 수 있는 형태로 작성하고, 디지털로 서명하여 암호화하는 것 역시 가능하다.

이러한 스마트 컨트랙트가 개인정보 처리를 위한 동의 제도에서 유용한 이유는 다음과 같다. 우선, 스마트 컨트랙트를 통해서는 역동적인 동의체계를 개발하는 것이 가능하

139) Ruben (R.W.H.G.) Schulpen, Smart contracts in the Netherlands, 2018, p. 8

다. 스마트 컨트랙트는 컴퓨터가 읽을 수 있는 디지털화된 문서로 작성되기 때문에 서류 계약서처럼 조건이 고정되지 않는다. 원한다면 개인정보처리자는 정보주체가 수집·이용 또는 제3자에게 제공할 개인정보의 범위를 선택할 수 있는 동의서를 생성할 수도 있다.

또, 스마트 컨트랙트는 컴퓨터나 프로그램이 인식할 수 있는 형태로 작성되기 때문에 자동적인 계약의 이행 및 집행이 가능하다는 견해도 제기되고 있다.

마지막으로 스마트 컨트랙트는 컴퓨터가 읽을 수 있기 때문에 블록체인과의 연동이 가능하다.

단, 스마트 컨트랙트를 곧바로 마이데이터 서비스에 도입하는 것은 보다 깊은 추가 검토가 필요할 것으로 보인다. 아직까지 스마트 컨트랙트는 널리 도입되지 않았으며, 따라서 그 효용 또는 부작용에 대해서 알려진 것이 상대적으로 적고, 따라서 예측하지 못한 문제가 발생할 가능성을 배제할 수 없기 때문이다.

따라서 스마트 컨트랙트 기술의 발전을 유심히 살펴보면서 그 장단점에 대한 연구가 충분히 이루어진 후에 이를 마이데이터 서비스에 도입하는 것이 보다 적절할 것이다.

제6장 결론

이상에서 현재 이루어지고 있는 마이데이터 서비스의 다양한 사례, 이와 관련된 개인정보보호 관련 법령, 특히 동의 제도의 국내외 현황, 국내법에 대한 비판점, 개선 방안에 대하여 검토하였다. 유럽연합의 GDPR에 있는 정보이동권이 도입된다면 마이데이터 산업을 강화시킬 좋은 방안은 되겠으나 현재에도 우리나라에서 마이데이터 서비스가 이루어지고 있고, 그러므로 더욱 중요한 것은 현재의 동의 제도를 어떻게 개선하느냐는 것이다.

국내법과 비교하기 위해 외국의 법제도 현황을 살펴본 결과 특히 유럽연합의 GDPR이 상세한 적법 처리 조건과 엄격한 동의 제도를 바탕으로 정보주체의 개인정보자기결정권을 강하게 보호하면서도 정보 활용이 산업적으로 가능하도록 하는 좋은 예시를 보여주는 것으로 평가할 수 있다. 즉, GDPR은 동의가 유효하려면 자유롭게 부여되고(Free/Freely given), 개별적으로 특정되며(Specific), 사전 정보가 제공되어 있고(Informed), 모호하지 않은 의사표시(Unambiguous indication)에 의해야 한다고 규정하였다. 그러면서도 '정보주체가 계약 당사자가 되는 계약을 이행하거나 계약 체결 전 정보주체가 요청한 조치를 취하기 위해 처리가 필요한 경우'를 적법 처리 조건의 하나로 두어 개인정보처리자로 하여금 정보주체의 동의를 받지 않고서도 정보활용을 할 수 있는 길을 열어 두었다. 또한 정보를 제3자에게 제공하는 경우, 수령인(recipient)에 대해 정보주체에게 고지하여야 하지만 전체 목록이 아닌, 그 유형을 고지하는 것도 가능하도록 하였다.

미국 캘리포니아주의 CCPA는 옵트아웃(opt-out) 기반의 데이터 보호법이라는 데 의

미가 있다. 사업자는 소비자의 요구에 따라 개인정보처리내역을 통지해야 하며 개인정보 삭제 요청 시 일정한 예외적인 경우를 제외하고 반드시 해당 정보를 삭제해야 하며, 웹기반 옵트아웃 도구와 프로그램을 마련해야 한다.

일본의 개인정보보호법의 특징은 목적이 특정된 경우라면 정보주체의 동의 없이도 개인정보를 수집 · 이용할 수 있다는 점이다. 개인정보 제3자 제공의 경우에는 우리 법과 유사한 동의 원칙을 규정하고 있지만, 일정한 범위에서 옵트아웃 방식을 허용하고 있는데다 정보주체에 대한 법정 고지사항에 대해서도 우리와 같은 엄격한 규제를 하고 있지 않다는 점에서 우리 법과 차이가 있다. 이러한 점에 근거하여 최근에는 정보은행 서비스 도입이 진행되고 있다.

이에 반하여 우리 법은 복잡한 규제로 인해 정보의 활용범위를 지나치게 제한하면서도, 오히려 정보주체의 개인정보자기결정권을 효과적으로 보호하지 못하고 있다는 비판에 직면하고 있다. 즉, 사전 · 명시 · 구분 동의를 모두 요구하고 있는데다 정보주체의 동의가 원칙이라는 점에서 '동의만능주의'를 채택하고 있다는 비판이 제기된다. 법률 규정뿐 아니라 실무상 해석도 엄격하여 개인정보 제3자 제공시 제공받는 자를 일일이 모두 고지해야 한다고 해석되고 있다. 법정 고지사항을 엄격하게 해석하는 것에 더불어 그 사항이 조금만 변경되더라도 또다시 정보주체의 동의를 받아야 하는 점도 오히려 더 나은 서비스를 제공하기 위한 경우까지 불필요한 동의를 받도록 하고 있다는 비판의 대상이다. 게다가 외국의 법제와는 전혀 달리, 형사처벌 중심의 제재를 취하고 있다. 뿐만 아니라 개인정보보호법에 비해 정보통신망에 오히려 더 엄격한 규제를 부과하고 있어 마이데이터 산업을 비롯한 데이터 산업에 큰 장애로 기능한다는 비판이 제기된다. 특히, 사물인터넷 기술이 적용되는 분야에서는 현행 동의 제도가 비현실적이라는 지적이 있다.

동의규제의 역설이란, 동의서가 길고 복잡해질수록 정보주체는 고지사항을 제대로 읽지 않아 정보를 제공하는지도 모른 채 개인정보를 제공하고 사업자들은 면죄부를 받게 된다는 것을 말하는데 '알고 하는 동의(informed consent)'가 이루어지고 있지 못하다는 국내 동의 제도의 현실에 들어맞는 비판이다. 이렇게 동의 제도가 형식화된 결과 정보주체들은 동의서의 내용을 읽어보지 않고 서명만 하거나, 대충 훑고 서명하는 경우가 대부분이었다.

이러한 국내법의 개선 방안으로 현재 발의된 개인정보보호법 개정안 및 신용정보법 개정안이 주목된다. 개인정보보호법 개정안에 따르면 합리적으로 관련된 범위 내에서 정보주체의 동의 없이 개인정보를 이용하고 제3자에게 제공할 수 있기 때문에 마이데이터 산업에 긍정적인 영향을 끼칠 수 있을 것으로 보인다. 그러나 현행 사전, 명시, 개별, 선택, 변경 동의 등 엄격한 원칙을 고수하는 현행 법제도의 중심이 되는 개인정보보호법 내용을 개정하는 내용을 담고 있지 않아 아쉬움이 남는 점이 있다

신용정보법 개정안은 신용정보주체가 정보 활용 동의사항을 이해할 수 있도록 정보활용 동의서를 단순화하고, 정보주체의 인지적 한계를 보완할 수 있다는 평가를 받아 '동의 규제의 역설'을 일정 부분 해소할 수 있을 것이라는 기대를 받는다. 또한 정보주체가 열람권 등 권리행사를 대리인을 통하여 할 수 있도록 명시하고 마이데이터 사업자도 그 대리업무를 수행할 수 있게 되었다. 또한 정보이동권(개인신용정보 전송 요구권)을 도입하고, 그 과정에서 정보주체의 의사 확인 규제를 함께 규정하였다.

동의 제도 자체의 개선 방안으로는, 포괄 동의 혹은 유형 고지를 도입하는 방안을 들 수 있다. 예를 들면, 개인정보처리방침 공개를 통해 법정 고지사항을 일괄적으로 고지하고 이어서 정보처리에 대한 포괄적 동의를 받는 방안을 고려해볼 수 있다. 그러나 동의 제도 개선은 완전한 해결책이 될 수 없다. 현재와 같이 동의 제도에 의존하는 것은 데이터 경제 시대에 부합하지 않기 때문이다. 이를 위해서는 GDPR과 같이 정당한 이익에 근거한 정보처리를 가능하도록 할 필요성이 제기된다.

법률의 개정 없이 동의 제도를 개선하는 방안에 대해서도 살펴보았다. 특히 개인정보처리 동의권의 포괄적 대리가 가능한지가 문제된다. 그러나 현행법 하에서 개인정보처리 동의의 포괄적 대리가 가능한지에 대해 의문이 제기될 여지가 있고, 사업자로 하여금 법적 리스크를 부담할 것을 강요하기는 어려움이 있다는 문제가 있다는 점에서, 이에 관한 명확한 법률 규정이 필요한 것으로 보인다.

이처럼 마이데이터 산업의 성공적인 정착을 위해서는 정보보호 관련 법제도의 정비가 관건이고, 현재 개인정보자기결정권의 실현 수단의 핵심이 되는 동의 제도를 개선하는 것이 당면 과제라고 할 수 있다. GDPR을 비롯한 외국의 법제도의 장점을 참고하여 제4차 산업혁명에 대비하여 개인정보자기결정권의 실질적 보장과 데이터 산업 진흥을 위한 정보활용이라는 두 마리 토끼를 모두 잡을 수 있는 지혜가 필요하다.

참고문헌

고연희, 「본인신용정보 관리업 도입과 해외사례」, 『NICE Credit Insight』, NICE평가정보 CB 연구소, 2018.

고환경 외, 『정보이동권과 마이데이터 산업』, BFL 제93호, 2019.

고환경, 『개인정보 동의 및 파기 규정의 적정성에 관하여』, 2015. 7. 23., https://blog.naver.com/n_privacy/220427876061

권영준, 「개인정보자기결정권과 동의 제도에 대한 고찰」, 『법학논총 제36권 제1호』, 전남대학교 법학연구소, 2016.

금융위원회, 『금융분야 개인정보보호 가이드라인』, 2017.

금융위원회, 『금융분야 마이데이터 산업 도입방안』, 2018.

김민호 외, 『개인정보보호법 개정안(인재근 의원 대표발의)에 대한 의견서』, 개인정보보호법학회, 2019.

김은수 외, 「2015년 일본 개인정보보호법의 개정 - 개정된 주요 내용과 시사점」, 『YGBL 제8권 제1호』, 2016.

개인정보보호위원회, 유럽 일반 개인정보보호법(GDPR) 번역문, 2017.

나종연, 『정보주체 동의권의 실질적 보장을 위한 연구』, 개인정보보호위원회, 2017.

대통령직속 4차 산업혁명위원회, 『4차 산업혁명 대정부 권고안』, 2019. 10.

보건복지부 의료기관정책과,『진료기록 열람 및 사본발급 관련 법령 해석 등 안내』, 2017. 12. 22.

박강우, 「일본에서 개인정보의 형법적 보호」,『강원법학』제55권, 강원대학교 비교법학연구소, 2018.

박훤일, 「정보이동권의 국내 도입방안 - EU GDPR의 관련 규정을 중심으로」, 『경희법학』 제52권 제3호, 경희대학교 법학연구소, 2017.

방송통신위원회, 『온라인 개인정보처리 가이드라인』, 2018.

방송통신위원회 · 한국인터넷진흥원, 『정보통신서비스 제공자를 위한 개인정보보호 법령 해설서』, 2012.

서울경제, 『개인정보 7천만건 탈탈 털렸지만…과태료는 건당 131원 불과』, 2019. 10. 4., https://www.sedaily.com/NewsView/1VPE35TOV3

성낙인 외, 『개인정보보호법제에 관한 입법평가』, 한국법제연구원, 2008.

손형섭, 「일본 개정 개인정보보호법과 우리법의 나아갈 방향」, 『공법연구』 제46집 제2호, 한국공법학회, 2017.

손형섭 외, 『일본의 개인정보보호 법제 · 정책 분석에 관한 연구』, 개인정보보호위원회, 2017.

신종철, 『통신법해설』, 진한엠앤비, 2019.

이영준, 『민법총칙』, 박영사, 2007.

이인호, 『일본 개인정보보호법』 번역, 개인정보보호위원회, 2016.
이창범, 『개인정보보호법』, 법문사, 2012.
정구태, 「유류분반환청구권의 일신전속성」, 『홍익법학』 14권2호, 홍익대학교 법학연구소,
정무위원회, 『신용정보의 이용 및 보호에 관한 법률 일부개정법률안 검토보고 - 빅데이터 분석·이용의 법적 근거 명확화 등』, 2018. 12.
정찬모, 「개인정보보호에 있어 정보주체의 동의」, 『인하 법학』 제18집 제1호, 2015.
최창수, 「미국의 빅데이터 이용 활성화와 개인정보 보호」, 『법조』 제68권 제3호, 법조협회, 2019.
한국사법행정학회, 『주석형법』, 2011.
한국인터넷진흥원, 『우리 기업을 위한 'EU일반 개인정보보호법(GDPR)』, 2018.
한국인터넷진흥원, 『해외 개인정보보호 동향 보고서』, 2018. 6.
행정안전부, 『개인정보보호 법령 및 지침 고시 해설』, 2016.
홍선기, 「일반개인정보보호규정(GDPR) 발효에 따른 독일 개인정보보호법제의 입법동향 및 시사점」, 『정보법학』 제22권 제1호, 한국정보법학회, 2018.

Article 29 DATA PROTECTION WORKING PARTY, *Guidelines on the Right to Data Portability* (2017. 4. 5.)
Article 29 DATA PROTECTION WORKING PARTY, *Guidelines on consent under Regulation* (2017. 11. 28.)
Ruben (R.W.H.G.) Schulpen, *Smart contracts in the Netherlands,* 2018.
個人情報保護委員會, 個人情報の保護に關する法律についてのガイドライン（通則編）, 2019.

1. 본 보고서는 과학기술정보통신부의 방송통신발전기금을 지원받아 수행한 결과로 과학기술정보통신부 및 한국데이터산업진흥원의 공식의견과 다를 수 있습니다.
2. 본 보고서의 내용을 발표 및 인용할 때에는 반드시 한국데이터산업진흥원 사업의 결과임을 밝혀야 합니다.
3. 본 보고서 내용과 관련한 문의는 한국데이터산업진흥원 유통기반실 (02-3708-5352)로 연락해 주시기 바랍니다.