EXPERT COLUMN

PRIVACY LAW

온라인 개인정보 처리 가이드라인 개정

4년 만에 바뀐 '온라인 개인정보 처리 가이드라인' 무엇이 달라졌나?

방송통신위원회가 2018년 9월 18일 '온라인 개인정보 처리 가이드라인'을 개정했다. '온라인 개인정보 처리 가이드라인'은 온라인 서비스 회원을 대상으로 한 개인정보의 처리 기준을 제시하기 위한 목적으로 2014년 11월에 제정되었다. 이번 개정에서는 이용자가 열람·제공을 요구할 수 있는 사항을 사업자가 가진 회원가입 정보, 사업자의 이용 현황, 제3자에게 제공한 현황 등으로 구체화했다.

이 글에서는 4년 만에 개정된 '온라인 개인정보 처리 가이드라인'이 어떻게 바뀌었는지 소개한다.

이번 '온라인 개인정보 처리 가이드라인'의 주요 개정 사항은 크게 6가지로 구분되는데, 3가지는 신규로 추가되었고 3가지는 기존 기준을 현행화하여 정보주체의 권리를 신장시키게끔 하였다. 중요도가 높은 '신규' 사항부터 알아보도록 하자.

1. 개인정보 열람 제공 운영 기준 (신규)

- 개인정보 열람/제공 등 대상 항목 및 방법 구체화
- 개인정보 열람/제공 등 요구 관련 별도 메뉴 운영 가능
- 자료 제공 시 실비 범위에서 수수료와 우송료 청구 가능
- 열람 제공 제한/거절 사유 명시 및 이용자에게 제한 사유 통지

정보주체가 개인정보 열람 제공을 요구할 수 있는 항목을 구체적으로 공개해야 한다. 개인정보처리방침에는 필수적으로 열람 제공 항목을 기재해야 하고 추가

적으로 홈페이지에 별도 메뉴를 만들어 열람 기능을 제공해도 된다(개인정보처리방침은 필수 조치, 홈페이지 별도 메뉴 생성은 선택 조치).

개인정보와 자동 생성된 개인정보는 기존에도 개인정보처리방침에 공개해야 했지만 이번 가이드에선 사업자가 분석 등을 통해 생성해낸 개인정보도 포함시키도록 명시하였다. 요즘 각광받는 빅데이터 분석이나 이용자 프로파일링을 이용한 구매 성향 같은 2차 개인정보가 그 예다.

최초 수집하는 경우나 제공받는 경우는 케이스를 식별하기가 비교적 용이하지만 내부 업무에 의해 2차 생성되는 정보를 파악하는 일은 상당한 애로가 있을 것으로 예상된다. 개인정보 보호 업무는 통상 보안팀이나 준법관리팀에서 담당하는데, 현업 부서에서 신규로 발생하는 분석 데이터까지 지속적으로 파악하기는 쉽지 않기 때문이다. 개인정보 보호 업무를 특정팀에서 전담하기보다 전사적인 거버넌스로 대응해야 하는 까닭이기도 하다.

개인정보의 이용현황 및 제3자 제공 현황 공개도 비슷한 부담이 있다. 제3자 제공의 경우 많은 기업이 개인정보처리방침에 '제3자 제공은 정보주체의 동의가 있거나 법령에 근거한 경우가 아니면 제공하지 않는다'와 같이 원칙만 간략히 기술한 경우가 많다. 그러나 이번 가이드를 준수하려면 모든 조직에서 실제 발생한 제3자 제공 내역(제공 업체, 제공 목적, 제공 항목, 정보주체의 동의 또는 법적 예외 등 제공 근거)을 기록해 놓아야만 열람 요구 대응이 가능하다. 이 역시 쉽지 않다. 앞서 언급했듯이 상시적인 제3자 제공 사항은 개인정보처리방침에 공개를 했어야 한다. 여기서 말하는 제3자 제공은 일시적 또는 일회적으로 발생하는 경우를 지칭한다.

2. 개인정보처리방침 공개 운영 (신규)

■ 개인정보 보호 업무 처리 부서, 연락처 등 권리행사에 필요한 항목을 상단에 명시하는 등 처리방침 공개 순서 변경

개인정보처리방침의 공개 항목 순서가 이용자의 권리 중심으로 변경되었다.

[기존 공개 순서]

1) 개인정보 수집/이용 목적, 수집하는 개인정보의 항목 및 수집 방법
2) 제3자 제공 현황
3) 보유 및 이용기간, 파기 절차 및 파기 방법
4) 처리 위탁 현황
5) 이용자 및 법정대리인의 권리 및 행사 방법
6) 개인정보의 자동 수집 장치 설치, 운영, 거부 사항
7) 개인정보 보호 책임자, 성명 및 부서, 연락처

[변경 공개 순서]

1) 이용자 및 법정 대리인의 권리 및 행사 방법
2) 개인정보 보호 책임자 성명 및 부서, 연락처
3) 개인정보의 자동 수집 장치 설치, 운영, 거부 사항
4) 개인정보 수집, 이용 목적, 수집하는 개인정보 항목 및 수집 방법
5) 제3자 제공 현황
6) 보유 및 이용 기간, 파기 절차 및 파기 방법
7) 처리 위탁 현황

3. 이용 내역 통지 운영 기준(신규)

■ 개인정보 이용 내역의 개별적/구체적 통지

정보주체의 개인정보 이용내역을 연 1회 이상 주기적으로 통보해야 할 의무는 전년도 말 기준 직전 3개월 간 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 100만 명 이상이거나 전년도 정보통신서비스 부문 매출액이 100억 원 이상인 사업자에게 해당된다. 통지 항목은 1)'개인정보의 수집·이용 목적 및 수집한 개인정보의 항목' 2)'개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목' 3)'개인정보 처리 위탁을 받은 자 및 그 처리 위탁을 하는 업무의 내용'이다.

기존에는 개인정보 수집이용 동의 고지사항이나 개인정보처리방침의 내용을 복사해서 붙여넣기하는 수준의 사항만 통보하는 것이 일반적이었다. 이번 가이드에서는 제3자 제공의 경우 개인정보처리방침에 없거나 동의 수집 시 없던 사항이라 할지라도 실제 발생한 제공 내역을 각 이용자에게 통지하도록 노력할 것을 명시하고 있다. 이 항목에서 '통지해야 한다'고 서술하지 않고 '노력해야 한다'고 쓴 것은 이를 구현하는데 상당한 부담이 따르는 일임을 이해한다는 방증이기도 하다.

예시: 개인정보 이용 내역 통지

■ 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목

- 회원 가입 성명, 휴대전화 번호, 이메일 주소
- 서비스 이용 및 상담: 성명, 휴대전화 번호, 이메일 주소
- 결제: 신용카드사명, 카드번호, 유효기간, CVC
- 취소·환불: 은행명, 계좌번호
- 배송: 수취인 성명, 휴대전화 번호, 주소

■ 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목

연번	1	2
서비스명	oo페이 이용 회원	OO 예약
제공받는 자	(계좌 결제) OO은행, (신용카드 결제) OO카드, (휴대폰 결제) COO텔레콤 ※제공한 업체 목록 모두 기재	O사, O사, O사 ※제공한 업체 목록 모두 기재
목적	상품 구매 및 배송 서비스 제공	원활한 예약 진행, 본인 의사 확인, 고객상담 및 불만처리
항목	아이디, 성명, 이메일 주소, 전화번호, 휴대전화 번호, 상품구매정보, 수취인 정보 (성명, 주소, 전화번호)	아이디, 성명, 전화번호, 상품구매정보

4. 최소한의 개인정보 수집 기준(현행화)

■ 본인 확인이 서비스 제공에 반드시 필요한 경우가 아닌 경우에도 개인정보를 수집한 경우는 최소 수집 원칙에 반(反)함

개인정보 수집 최소화의 원칙은 개인정보보호 법령의 최상위 원칙이다. '최소화'라는 용어는 주관적으로 판단될 여지가 많아 개인정보처리자가 생각하는 최소한의 범위와 정보주체가 느끼는 최소한의 범위가 다를 가능성이 높았다. 이번 가이드에서 제시한 기준은 어떤 개인정보를 선택했을 때 그 정보가 없어도 정보주체가 서비스를 이용하는데 문제가 없다면 최소 수집 원칙을 반한 것으로 판단한다는 것이다. 예컨대 정적인 콘텐츠로만 구성된 홈페이지에서 회원가입을 강제하는 경우가 그러하다. 개인정보보호 법령이 강화된 이후로 이런 경우는 사실 찾기 힘들다.

휴대전화나 아이핀, 공인인증서 등을 통한 이용자 본인 확인은 법률상 의무이행이나 서비스 제공에 반드시 필요한 경우가 아니라면 이용자에게 강제해서는 안된다고 밝히고 있다. 이용자 본인확인이 꼭 필요한 경우라도 회원 가입 시점이 아니라 실제 서비스를 이용할 시점에 본인확인을 하도록 법에 규정되어 있다는 점도 잊어서는 안될 것이다.

14세 미만 아동의 개인정보 수집에 관련해서도 유의할 내용이 있다. 인터넷 회원 가입 단계에서 만 14세 미만 아동 여부 확인을 위한 구체적인 조치를 취해야한다. 법정 생년월일을 입력하도록 하거나 '만 14세 이상'이라는 항목에 체크하는 등의 방법으로 14세 미만 아동 해당 여부에 대해 명확히 식별할 것을 가이드는 권고한다.

정보통신망법이 온라인 회원에 대한 규제를 주로 담고 있는 것이긴 하나 회원 가입이나 개인정보 수집 이용 동의가 온라인에서만 이루어지는 것은 아니다. 온라인 서비스의 경우, 애초에 총괄적인 기획을 통해 만들어지고 설계 단계에서 법적 준거성을 확인하고 사전조치를 잘 하는 편이다. 그러나 오프라인은 각 현업에서 제작한 양식을 통해 업무가 처리되는 경우가 많다. IT부서나 보안부서에서 알지도 못하고 통제도 못하기 때문에 법 기준을 위반하는 일이 빈번하게 발생하곤 한다.

개정 가이드에서는 이러한 오프라인 상의 개인정보 수집에 대해 여러 상황 예시를 통해 적절한 조치를 제시하고 있다. 필자의 설명보다 예시가 이해에 도움이 될 듯 싶어 이 부분은 가이드 내용을 그대로 옮겨 적는다.

예시① 본인확인과 가족할인 등 혜택 제공을 위한 증빙을 위해 신분증(주민등록증, 운전면허증, 가족관계증명서 등)을 요구하는 경우
– 단순 확인만으로 목적 달성이 가능하다면 별도의 사본을 저장해서는 안 되며, 수집 · 저장(예: 사본 저장)이 필요한 경우에도 수집 동의를 받지 않은 정보(예: 신분증 뒷면 지문, 주민등록번호 뒷자리 등)는 마스킹 처리한 후 수집 · 저장하여야 한다.

예시② 요금감면 대상자인지 여부 확인을 위해 장애인 등록증, 국가유공자 증빙서류 등을 수집하는 경우 확인 목적과 무관한 정보는 마스킹 처리한 후 보관한다.

예시③ 이용약관 상의 위약금 면제사유(예: 이사 등) 확인을 위해 사업자가 요구하는 인사명령서, 주민등록등본 등의 서류는 담당자 확인으로 갈음하는 방안 등을 강구하는 것이 바람직하다.

5. 단계별 개인정보 파기 기준(현행화)

- 위탁자가 영세업자이고 수탁자가 대규모 사업자인 경우 위탁자의 능력을 고려하여 관리/감독할 수 있도록 노력
- 개인정보 파기에 준하여 별도 분리 저장/보관 추가

컨설턴트인 필자의 주 사업 영역은 개인정보 수탁자 점검이다. 법에서는 개인정보 처리자가 본연의 개인정보 처리 업무를 타 사업자에게 위탁하여 처리하는 경우 위탁자한테 수탁자를 관리 감독할 책임을 부여하고 있는데 관리 감독의 대표적인 행위가 교육과 점검이다. 그런데 현실에서는 이 수탁자가 위탁자보다 훨씬 덩치가 커서 감히 교육과 점검을 직접 수행하기가 불가능에 가까운 상황이 흔

하다. 예를 들어 직원 10명인 작은 온라인 쇼핑사이트가 배송을 위해 우체국을 상시 이용한다고 하면 쇼핑사이트가 위탁자, 우체국이 수탁자이다. 직원 건강진료를 위해 S병원을 이용한다고 하면 S병원이 수탁자이고 DM 문자서비스를 위해 통신사를 이용한다고 하면 통신사가 수탁자가 될 터이다. 10명 규모의 이 쇼핑사이트가 우체국과 S병원, 통신사의 개인정보 보호 실태를 점검하고 수탁자에게 위탁자의 개인정보보호 교육을 받도록 요구하는 일이 수월할까? 어쩌면 '수월한가'보다는 '가능한가'라고 묻는 것이 맞을 것이다.

이런 애로사항을 감안했는지 이번 가이드에서는 "위탁자가 영세사업자이고 수탁자가 대규모 사업자인 경우와 같이 위탁자의 관리·감독이 현실적으로 어려운 사정이 있는 경우, 위탁자는 자신의 능력을 고려하여 합리적인 범위 내에서 최대한 관리·감독할 수 있도록 노력하여야 한다"라는 내용이 수록되어 있다. 이는, 경우에 따라 위탁자가 수탁자를 엄격하게 관리 감독하지 못할 상황이 있더라도 규모의 차이에 따른 현실적인 장애가 큰 경우라면 '노력'의 정도만으로 정상을 참작하겠다는 배려가 느껴진다.

더불어 위탁과 관련하여 현장에서 많이 듣는 질문에 대한 답이 가이드에 있어 함께 싣는다.

- 개인정보 위탁계약서에는 위탁된 개인정보의 안전한 관리와 파기 및 확인 사항을 포함하여 작성해야 한다. (계약서 반영 내용: 개인정보 파기·보호조치 관련 사항 외에 '주기적 확인 사항'과 관련한 사항 등)
- 수탁자가 독자적인 사업을 영위하고 있다고 할 지라도 위탁자로부터 제공받은 개인정보에 대해서는 위탁자의 관리·감독 아래 위탁 받은 범위 내에서만 개인정보를 처리해야 한다.
(대법원 2017.4.7. 선고 2016도13263판결 참고)
- 개인정보의 처리위탁은 위탁자 본인의 업무처리와 이익을 위한 것인 점을 고려할 때 수탁자에는 재수탁자가 포함된다고 보는 것이 타당하며, 따라서 위탁자 역시 재수탁자에 대해서 관리·감독의 책임을 다하기 위해 노력해야 하고 수탁자 또한 재수탁자에 대한 관리·감독 의무를 이행해야 한다.

6. 이해하기 쉬운 동의서 작성 기준(현행화)

■ 사업자의 동의 획득 방법으로 기존 이메일, 우편 외에도 문자메시지, SNS 등도 추가

개인정보 동의 확인 방법으로 문자메시지와 소셜 네트워크 서비스(SNS)가 추가되었다고 하는데 문자메시지는 기존에도 이미 많이 쓰이고 있었다. 페이스북, 트위터와 같은 SNS를 이용해도 된다는 점은 특기할 만하다.

■ 국외 재이전 시 국외 이전과 동일하게 이용자 동의 필요

개인정보를 국외로 이전하는 경우에는 정보주체의 동의를 받는 것이 법에서 정한 원칙이다. 한국의 B라는 온라인서비스 업체가 미국의 A라는 클라우드 서비스업체를 통해 IT서비스를 운영하고 개인정보를 이전했다. 물론 국외 이전에 대한 회원 동의를 받고 진행했다. 그런데 미국 A업체가 다시 다른 나라 C라는 업체의 IDC(Internet Data Center)를 이용해서 개인정보를 이전하는 상황이 생긴다면 이에 대해서도 한국 기업 B는 회원의 동의를 받아야 한다.

구분	법정 고지사항 내용
국외 이전 · 재이전 동의	1. 이전 · 재이전되는 개인정보 항목 2. 개인정보가 이전 · 재이전 되는 국가, 이전 일시 및 이전 방법 3. 개인정보를 이전 · 재이전 받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다) 4. 개인정보를 이전 · 재이전 받는 자의 개인정보 이용목적 및 보유·이용 기간

■ 마케팅 활용 동의(망법 제22조)와 영리목적 광고성 정보 수신동의(망법 제50조)는 별도 동의

※ 단, 마케팅 활용 동의 옆에 광고성 정보 수신동의 여부를 선택 동의 사항으로 구성 가능

정보통신망법 제22조의 동의는 수집한 개인정보를 마케팅 목적으로 이용하겠다는 의사에 대한 동의이고, 같은 법 제50조의 영리목적 광고성 정보 수신 동의는 구체적으로 광고성 정보를 수신하는 것에 대한 동의이므로 별도의 동의가 필요하다는 내용이다.

■ 개인정보 제3자 제공을 받는 자가 서비스 가입단계에서 특정되지 않은 경우 실제 구매 결제 시점에 고지 및 동의 획득 가능

제3자 제공 동의를 회원 가입 시에 받지 않은 경우일지라도 실제 구매 결제 시점에 고지하고 동의를 받는 것이 허용됨을 밝히고 있다.

구매(결제) 단계: 제공받는 제3자 고지 및 동의

제공받는 자	㈜ ooo
목적	상품 배송
항목	배송지 주소, 연락처
보유 기간	배송 완료 후 0일까지
동의 여부	☐ 동의함 ☐ 동의안함

■ 필수 동의 항목만으로 구성된 경우에만 일괄 동의 가능

개인정보 수집 이용 동의 과정에서 정보주체가 읽어야 할 많은 고지 사항과 체크해야 할 동의 항목은 사업자에게나 이용자에게나 피로한 일이었다. 다행히 온라인에서는 일괄 동의 체크라는 편리한 기능을 구현할 수가 있어 '전체 동의'라는 체크 박스를 흔히 볼 수 있다. 그러나 이번 개정 가이드에서는 이렇게 '전체 동의'를 통해 일괄 동의가 가능한 경우는 서비스 이용에 필수적인 개인정보 수집 이용 동의만 가능하며 선택사항까지 전체 동의로 일괄 처리하는 것은 원칙적으로 허용되지 않음을 밝히고 있다. 이는 이용자가 동의 처리의 편리함에 이끌려 선택적 동의 사항에 대한 판단을 제대로 하지 않을 수 있다는 점을 고려한 것으로 보인다. 선택 사항은 다소 불편하더라도 개별 동의를 할 수 있도록 구현할 것을 권고한다.

개정된 '온라인 개인정보 취급 가이드라인'에 대해 중요한 변경 사항들을 짚어 보았다. 4년 만에 개정되었지만, 그간 법령과 고시가 워낙 상세하게 강화되어 가이드라인에서 굳이 더 자세히 제시할 만한 내용은 많지 않은 듯하다. 온라인 서비스를 구현하고 운영하는 사업자 입장에서는 정보주체의 법적 권리를 보호해야 할 책임과 동시에 이용의 편리성을 보장해야 하는 과제를 매끄럽게 풀기가 쉽지 않다는데 애로가 있다. 법 배경을 모르는 이용자는 동의 처리 과정의 많은 고지 내용을 읽고 체크를 하는 일에 불편함을 호소하곤 한다. 실제로는 호소가 아니라 항의에 가깝다. 지난 5월에 발효된 GDPR(유럽 일반 개인정보보호법)에 비견해도 한국의 개인정보보호 법령은 그 디테일함과 엄격함에서 한참 앞서 있다는 것이 필자 생각이다. 이제는 법이 처벌은 더 엄정하되 세부적인 시행 기준의 적용은 좀 더 유연해지기를 기대한다.