발 간 등 록 번 호
11-1311000-000320-01

사업자를 위한
개인정보보호 질의 · 응답집

행정안전부

한국인터넷진흥원
Korea Internet & Security Agency

발 간 등 록 번 호
11-1311000-000320-01

사업자를 위한

개인정보보호 질의 · 응답집

행정안전부
MINISTRY OF PUBLIC ADMINISTRATION AND SECURITY

한국인터넷진흥원
Korea Internet & Security Agency

Contents

제1장 개인정보보호 감 잡기 5

1. 개인정보보호란 무엇인가 6
2. 우리 회사에는 어떤 법률이 적용될까 10
3. 준용사업자와 정보통신서비스 제공자 13
4. 개인정보보호의 대상은 누구인가 17

제2장 개인정보보호의 시작은 내부관리계획 수립부터 19

1. 내부관리계획 그게 뭐야 20
2. 내부관리계획 어떻게 작성해야 하나 22

제3장 개인정보 관리책임자와 개인정보 취급자 25

1. 우리 회사의 개인정보 관리책임자는 누가 되어야 할까 26
2. 나 홀로 사업인데 개인정보 관리책임자를 두어야 하나 31
3. 개인정보 취급자란 33

제4장 개인정보를 수집하고 이용하려면 37

1. 회원가입 · 이벤트 시 고객의 동의를 받자 38
2. 민감한 개인정보를 수집하고 있지는 않은가 43
3. 개인정보는 최소한으로 수집하자 46
4. 14세 미만 아동의 개인정보 수집은 이렇게 하자 49
5. 수집 · 이용목적이란 무엇일까 52
6. 목적외 이용이 되지 않게 하려면 55
7. 개인정보 활용 목적이 달라지면 무엇을 해야 하나 58

제5장 개인정보를 제3자에게 제공 · 위탁하려면 61

1. 수집한 정보를 제3자에게 제공할 때 지켜야 할 사항 62
2. 이런 경우도 제3자 제공인가 66
3. 수사기관이 개인정보를 요구할 때는 69
4. 제3자 제공과 개인정보 취급위탁 구별하기 72
5. 개인정보 업무를 외주업체에 위탁할 때 주의사항 76

6. 개인정보 취급위탁시에는 언제나 동의를 받아야 하나 79
7. 개인정보 취급위탁 계약을 체결할 때의 주의사항은 82
8. 대리점의 개인정보 유출방지를 위한 노력 85
9. 동의 받는 방법 총정리 87
10. 영업을 양도하거나 합병할 때는 91

제6장 고객의 개인정보는 철저히 관리하자 95

1. 개인정보 취급방침, 이것만은 꼭 기억하자 96
2. 개인정보 취급방침을 알리는 방법 101
3. 개인정보 취급방침을 변경할 때는 104
4. 해킹과 불법 접근을 차단하려면 108
5. 내부직원의 개인정보 유출을 방지하려면 112
6. 개인정보 암호화 꼭 해야 하나 115
7. 보안프로그램은 어떻게 설치 · 이용하면 될까 119
8. 개인정보에 대한 접근권한은 최소한으로 123
9. 물리적인 접근제한 조치를 하려면 125
10. 개인정보를 출력 · 복사할 때는 127

제7장 고객의 개인정보 권리, 언제 어디서나 당당하게 129

1. 고객이 회원탈퇴를 요구할 때는 130
2. 가입은 쉽게 탈퇴는 가입보다 더 쉽게 133
3. 이용자가 수집동의에 대한 증빙을 요구할 때는 137
4. 개인정보 이용 내역을 요구하는 고객은 139
5. 개인정보의 이용 정정 요구는 이렇게 대응하자 142
6. 지체없이 필요한 조치란 144
7. 개인정보 파기는 언제 어떻게 해야 하는가 146
8. 개인정보 파기의 예외사유는 150

제8장 법을 위반하면 과태료와 벌칙이 부과됩니다 153

1. 과태료와 벌칙을 알아보자 154
2. 개인정보 분쟁조정제도, 개인정보 침해신고센터를 활용해 보자 158

사업자를 위한 개인정보보호 질의·응답집

제1장 개인정보보호 감 잡기

1. 개인정보보호란 무엇인가

2. 우리 회사에는 어떤 법률이 적용될까

3. 준용사업자와 정보통신서비스 제공자

4. 개인정보보호의 대상은 누구인가

제1장 개인정보보호 감 잡기

1. 개인정보보호란 무엇인가

Q | 개인정보보호란 무엇을 의미하는가?

A | 개인정보보호는 정보주체(고객, 이용자)의 개인정보가 안전하게 수집 · 이용 · 취급 · 관리되도록 하고, 정보주체의 동의 없이 함부로 수집되거나 이용 · 제공되지 않도록 함으로써 정보주체의 '개인정보 자기결정권'을 보장하는 것이라고 할 수 있다.

토 막 상 식

개인정보 자기결정권

개인정보 자기결정권이란 정보주체(고객, 이용자)가 자신의 개인정보가 언제, 어디서, 어떻게, 어느 범위까지 수집 · 이용 · 제공되는지에 대해 스스로 판단 · 결정할 수 있는 권리를 말한다. 개인정보 자기결정권은 헌법재판소에서 국민의 기본권으로 인정하고 있으며, 정보통신망법 등 관련 법률에 구체적으로 반영되어 있다.

좀 더 알아 봅시다

□ 개인정보의 개념

● '개인정보'는 일반적으로 "특정 개인을 식별하거나 식별할 수 있는 정보"를 말한다. 즉, 개인과 관련된 일체의 정보는 모두 개인정보에 해당될 수 있다(예: 성명, 주소, 연락처, 직업 등). 개인정보에는 해당 개인과 직접 관련이 있는 정보

뿐만 아니라 그 개인에 대한 타인의 의견, 평가, 견해 등 제3자에 의해 생성된 간접적인 정보(예: 신용평가 정보 등)도 해당될 수 있다.

1) 개인에 관한 정보

- 법률상의 개인정보는 "자연인(自然人)에 관한 정보"만 해당된다. 법인(法人)이나 단체의 정보는 법률에 따라 보호되는 개인정보의 범위에 해당되지 않는다.

2) 생존하는 개인에 관한 정보

- 법률상의 개인정보는 "생존하는" 자연인에 관한 정보만 해당된다. 따라서 이미 사망하였거나 민법에 의한 실종신고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 법률상의 개인정보로 볼 수 없다.

3) 생존하는 특정 개인을 알아볼 수 있는 정보

- 법률상의 개인정보에 해당되기 위해서는 그 정보로 "특정 개인을 알아볼(식별할)" 수 있어야 하며, 해당 정보만으로는 특정 개인을 식별할 수 없다 하더라도 "다른 정보와 쉽게 결합"하여 식별 가능하다면 개인정보에 해당된다. 예를 들어 단순히 "성명" 정보만 있다면 특정 개인을 식별하는 것이 쉽지 않으나(동명이인 등), 개개인의 "주소 · 연락처" 등과 결합되어 특정한 개인을 식별할 수 있다면 개인정보로 볼 수 있다.

- 그러나, 만약 통계적 목적으로 변환되어 개인을 식별할 수 있는 요소가 제거된 상태라면 개인정보로 보기 어렵다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

6. "개인정보"란 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

□ 개인정보보호의 의미

● 개인정보보호란, 개인정보를 취급하는 사업자가 정보주체(고객, 이용자 등)의 개인정보를 수집 · 이용하는 과정에서 정보주체의 동의를 받는 등 정당하게 개인정보를 수집 · 이용하고, 개인정보를 보관 · 관리하는 과정에서 내부자의 고의나 관리부주의 또는 외부의 공격으로부터 유출 · 변조 · 훼손되지 않도록 하며, 정보주체의 개인정보 자기결정권이 제대로 행사될 수 있도록 보장하는 일련의 행위 · 조치를 의미한다.

□ 정보사회의 발전과 개인정보보호의 필요성

● 오늘날에는 정보통신 기술의 발전에 따라 정보의 수집 · 저장 · 유통이 손쉬워지면서, 상업적인 서비스는 물론이고 공공행정 · 교육 등 다방면에 걸쳐 정보주체의 개인정보를 수집하고 이를 활용하는 행위가 널리 이루어지고 있다. 또한 동호회 등 비영리단체들도 회원의 개인정보를 이용하는 경우가 증가하는 추세이다.

● 이렇듯 개인정보의 수집 · 저장 · 유통이 간편하고 손쉽게 이루어짐에 따라 민간 · 공공부문을 막론하고 매우 방대한 분량의 개인정보가 축적 · 활용되고 있다. 그러나 이에 비해 개인정보에 대한 보호조치 및 정보주체의 권리보장은 충분하게 이루어지지 않고 있다. 최근 외부의 공격이나 내부직원의 부주의 등으로 1~2천만 건에 달하는 대량의 개인정보가 연이어 유출된 사건들은 개인정보보호의 중요성을 상기시켜주고 있다.

최근의 주요 개인정보 유출 · 침해 사례

○ 백화점, 인터넷쇼핑몰 등 6,950만건 연쇄 유출 ('10.3~5)
○ 통신사 콜센터, 연예인 등 2만건 유출 ('09.9)
○ 정유사 멤버십정보 1,100만건 유출 ('08.9)
○ 인터넷 오픈마켓 회원정보 1,800만건 해킹 유출 ('08.2)

● 특히 기업에서 개인정보 유출사고가 발생한 경우에는 집단 손해배상 소송으로 이어져 법적 · 경제적 피해와 함께 기업의 이미지와 신뢰도 하락과 같은 무형의 피해까지 입을 수 있다. 이에 따라 사업자들은 관련 법령의 준수 및 기술적 관리적 보호조치 이행 등 개인정보보호 활동에 보다 적극적으로 나설 필요가 있다.

관련 Q&A

Q | 협력사의 사업자등록번호에 대해서도 개인정보보호 조치를 취해야 하는가?

A | 개인정보는 생존하는 개인에 관한 정보이므로, 협력사의 사업자 등록번호와 같은 법인 · 단체의 정보는 개인정보에 해당하지 않는다.

Q | 사망한 회원의 유족이 상속 문제로 개인정보 열람을 청구해 왔다. 돌아가신 분의 정보도 개인정보에 포함되는가?

A | 원칙적으로 개인정보는 생존하는 자연인에 관한 정보만 해당되며 이미 사망한 자에 관한 정보는 법률상의 개인정보로 볼 수 없다. 다만 사자(死者)에 관한 정보가 현재 생존하고 있는 유족 등과 관련이 있는 경우(예, 상속 등)에는 유족의 프라이버시를 보호하는 차원에서 법률상의 보호받는 개인정보에 포함될 수도 있다.

2. 우리 회사에는 어떤 법률이 적용될까

Q | 개인정보보호에 대해 규율하는 법률은 어떤 것들이 있는가?

A | 우리나라에는 사회 전 분야에 모두 적용되는 개인정보보호에 관한 법률은 아직 없으며 각 분야별로 개인정보보호를 규율하는 법률이 존재하고 있다('11.2월 현재).

영리를 목적으로 개인정보를 수집 · 취급하는 사업자 등 민간 부문에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등이 적용된다.

국가 · 지방자치단체 · 학교 등 공공 부문에 대해서는 「공공기관의 개인정보보호에 관한 법률」 등이 적용된다.

좀 더 알아 봅시다

□ 현행 개인정보보호 법 체계

● 우리나라의 개인정보보호 법제는 정보통신, 금융 · 신용, 의료, 공공행정, 교육 등 개별 분야에 따라 각기 다른 법률이 제정 · 시행되고 있다.

– (민간 부문) 민간 부문은 분야별로 다양한 개인정보보호 관련 법률이 존재하고 있다. 이 중에서도 민간 영역의 규제범위가 가장 넓고 개인정보의 취급단계별로 상세한 보호원칙을 두고 있는 것은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법')이다.

민간 부문 개인정보보호 관련 법률

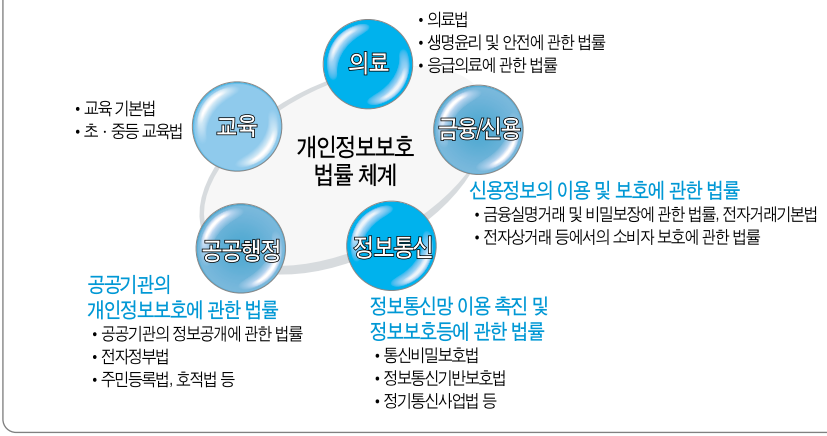
분 야	법 률
정보통신업 및 준용사업	정보통신망 이용촉진 및 정보보호 등에 관한 법률 통신비밀보호법, 전기통신사업법 등
금융 · 신용정보업	신용정보의 이용 및 보호에 관한 법률, 금융실명거래 및 비밀보장에 관한 법률 등
의료업	의료법, 건강검진기본법, 응급의료에 관한 법률, 생명윤리 및 안전에 관한 법률 등
위치정보사업	위치정보의 보호 및 이용 등에 관한 법률

– (공공 부문) 공공기관은 '공공기관의 개인정보보호에 관한 법률'이 적용되며, 이외에 교육분야 등에 대해서는 '초 · 중등교육법' 등에서도 규율하고 있다.

공공 부문 개인정보보호 관련 법률

분 야	법 률
공공부문 일반	공공기관의 개인정보보호에 관한 법률
주민등록 정보	주민등록법
정보공개	공공기관의 정보공개에 관한 법률
교육 부문	교육기본법, 초 · 중등 교육법

분야별 개인정보보호 관련 법률 현황



□ 개인정보보호법 제정 추진

● 최근 우리나라에서는 대량의 개인정보 유출사고가 끊임없이 발생하여 국민의 불안감이 급증하고 있으며, 반면 사회 전 분야에 걸쳐 적용되는 개인정보보호 일반법이 마련되어 있지 않아 법 적용의 사각지대가 발생하는 등 체계적인 개인정보보호 제도의 필요성이 나타나게 되었다.

● 이러한 문제점을 해소하기 위하여, 정부와 국회에서는 개인정보보호법의 제정을 추진하여 왔다. 개인정보보호법은 지난 17대 국회에서부터 꾸준히 논의가 이루어져 왔으며, 금번 제18대 국회에서 소관 상임위원회(행정안전위원회) 및 법제사법위원회 심의를 거쳐 마침내 '11년 3월 11일 국회 본회의를 통과하였다.

● 개인정보보호법은 법 의무적용 대상을 법원 등의 헌법기관과 모든 사업자, 각종 단체로 확대하고, 개인정보 취급단계별 보호기준을 상세히 규정하며, 개인정보 유출사실 통지 의무화 등 기술적 · 관리적 보호조치를 강화하는 내용을 담고 있다.

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보보호에 대한 일반법은 없으며 사회 각 분야별로 개별법 존재 (민간) 정보통신망법, 신용정보보호법 등 (공공) 공공기관 개인정보보호법 등	○ 개인정보 보호법이 공공, 민간 구분 없이 사회 전 분야에 적용됨 – 업무를 목적으로 개인정보를 처리하는 모든 자에 적용 (모든 공공기관, 민간사업자, 비영리 단체, 개인 등)

3. 준용사업자와 정보통신서비스 제공자

Q | 정보통신망법은 구체적으로 어떠한 업종에 적용되는가?

A | 정보통신망법의 개인정보보호 규정은 '정보통신서비스 제공자' 및 '준용사업자'에 대해 적용된다.

정보통신서비스 제공자는 "전기통신사업자 및 영리를 목적으로 정보통신망을 통하여 정보를 제공·매개하는 자"를 말하며, 여기에는 유·무선 전화사업자, 인터넷망 사업자, 인터넷 포털·게임·온라인쇼핑 등의 사업자가 해당된다.

준용사업자는 정보통신서비스 제공자 외의 사업자로서, 정보통신망법에서 따로 정하고 있는 업종을 말한다. 준용사업자에 대해서는 정보통신망법의 개인정보보호 규정이 적용된다. 정보통신망법 시행령·시행규칙에서는 여행업·호텔업 등을 준용사업자로 규정하고 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

제67조 (정보통신서비스 제공자 외의 자에 대한 준용) ① 정보통신서비스 제공자 외의 자로서 재화 등을 제공하는 자 중 대통령령으로 정하는 자가 자신이 제공하는 재화 등을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에는 제22조, 제23조, 제23조의2, 제24조, 제24조의2, 제25조, 제26조, 제26조의2, 제27조, 제27조의2, 제28조, 제28조의2 및 제29조부터 제32조까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자" 또는 "정보통신서비스 제공자 등"은 "재화 등을 제공하는 자"로, "이용자"는 "재화 등을 제공받는 자"로 본다. (이하 생략)

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제71조(정보통신서비스 제공자 외의 자의 범위) 법 제67조제1항 전단에서 "대통령령이 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 〈개정 2009.1.28〉

1. 「관광진흥법」 제3조제1항에 따른 여행업 또는 호텔업을 경영하는 자
2. 「항공법」 제2조제31호에 따른 항공운송사업을 경영하는 자
3. 「학원의 설립 · 운영 및 과외교습에 관한 법률」 제2조제1호에 따른 학원 또는 같은 조 제2호에 따른 교습소를 설립 · 운영하는 자
4. 그 밖에 재화 또는 용역을 제공하면서 회원제 또는 그와 유사한 형태로 개인정보를 수집하는 사업자로서 관계 중앙행정기관의 장과 협의하여 행정안전부령으로 정하는 자

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제6조 (정보통신서비스 제공자 외의 자의 범위) 영 제71조제4호에서 "행정안전부령으로 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 〈개정 2008.12.31〉

1. 「관광진흥법」 제3조제1항제2호나목에 따른 휴양 콘도미니엄업을 경영하는 자
2. 「유통산업발전법」 제2조제3호에 따른 대규모점포 중 대형마트 · 백화점 또는 쇼핑센터를 운영하는 자
3. 「유통산업발전법」 제2조제5호에 따른 체인사업을 운영하는 자
4. 「주택법」 제2조제5호에 따른 사업주체 중 주택건설사업을 시행하는 자
5. 「주택법」 제53조제1항에 따라 등록한 주택관리업자
6. 「건설기계관리법」 제2조제3호부터 제6호까지의 규정에 따른 건설기계대여업 · 건설기계정비업 · 건설기계매매업 및 건설기계폐기업을 하는 자
7. 「공인중개사의 업무 및 부동산 거래신고에 관한 법률」 제2조제4호에 따른 중개업자
8. 「자동차관리법」 제2조제7호에 따른 자동차매매업을 하는 자와 신조차의 매매 및 등록신청의 대행을 업으로 하는 자
9. 「여객자동차운수사업법」 제2조제4호에 따른 자동차대여사업을 하는 자
10. 「결혼중개업의 관리에 관한 법률」 제2조제5호에 따른 결혼중개업자
11. 「의료법」 제3조제1항에 따른 의료기관을 개설하여 의료업을 하는 자
12. 「직업안정법」 제4조제5호에 따른 유료직업소개사업을 하는 자
13. 「석유 및 석유대체연료 사업법」 제5조제1항에 따라 등록하여 석유정제업을 하는 자 중 같은 법 시행령 제9조제1항제1호 각 목의 석유정제시설을 모두 갖춘 자
14. 「체육시설의 설치 · 이용에 관한 법률」 제2조제3호에 따른 체육시설업자
15. 「영화 및 비디오물의 진흥에 관한 법률」 제2조제12호에 따른 비디오물의 대여업을 하는 자
16. 「출판문화산업 진흥법」 제2조제9호에 따른 출판문화산업의 종사자 중 서점을 운영하는 자
17. 「영화 및 비디오물의 진흥에 관한 법률」 제36조제1항에 따라 등록한 영화상영관 설치 · 경영자

좀 더 알아 봅시다

□ 정보통신망법 적용 대상

● 정보통신망법의 적용대상은 구체적으로 아래 표와 같다. 준용사업자는 자신이 제공하는 재화 등을 제공 받는 자의 개인정보를 수집 · 이용 · 제공하는 경우에 정보통신망법의 개인정보보호 규정이 적용된다. 이 경우 정보통신망법의 "정보통신서비스 제공자"는 "재화 등을 제공하는 자"가 되며, "이용자"는 "재화 등을 제공받는 자"가 된다.

정보통신망법 적용대상

구 분		업종 근거 규정 및 구분 기준
준용사업자	결혼중개업	결혼중개업의 관리에 관한 법률 제2조제5호
	의료기관	의료법 제3조제1항
	직업소개소	직업안정법 제2조의2 제5호
	정유사	석유 및 석유대체연료 사업법 제5조 제1항 동법시행령 제9조제1항제1호
	체육시설업	체육시설의 설치 · 이용에 관한 법률 제2조제3호
	비디오대여점	영화 및 비디오물의 진흥에 관한 법률 제2조 12호
	서 점	출판문화산업 진흥법 제2조제7호
	영화관	영화 및 비디오물의 진흥에 관한 법률 제36조제1항
	여 행	관광진흥법 제3조제1항
	호텔업	관광진흥법 제3조제1항
	항공운송사업	항공법 제2조 제31호
	학 원	학원의 설립 · 운영 및 과외교습에 관한 법률 제1조제1호
	교습소	학원의 설립 · 운영 및 과외교습에 관한 법률 제1조제2호
	휴양콘도미니엄	관광진흥법 제3조제1항 제2호나목
	할인점	유통산업발전법 제2조제3호(대규모 점포)
	백화점	
	쇼핑센터	
	체인사업	유통산업발전법 제2조제5호
	주택건설사업	주택법 제2조제5호
	주택건설업	주택법 제53조제1항
	건설기계대여 · 매매 · 정비 · 폐기업	건설기계관리법 제2조제3호~제6호

구 분		업종 근거 규정 및 구분기준
준용사업자	부동산중개업	공인중개사의 업무 및 부동산 거래신고에 관한 법률 제2조제4호
	자동차매매업, 매매 · 등록신청 대행업	자동차관리법 제2조제7호
	자동차대여사업	여객자동차 운수사업법 제2조제4호
정보통신서비스 제공자	전기통신사업자	기간통신사업자
		별정통신사업자
		부가통신사업자
	정보통신망을 통한 정보제공 · 매개사업자	전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자(영리목적만 해당)

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 정보통신서비스 제공자 및 준용사업자에 대해 정보통신망법 상의 개인정보보호 규정 적용(영리목적의 사업자만 포함)	○ 업무를 목적으로 개인정보를 처리하는 모든 자(개인정보처리자)에 대해 개인정보보호법 적용

4. 개인정보보호의 대상은 누구인가

Q | 내부 직원의 개인정보도 정보통신망법에 따른 개인정보보호 규정의 적용을 받는지 알고 싶다.

A | 정보통신망법의 개인정보보호 규정은 '이용자'에 대해서 적용된다. 이용자란 "사업자가 제공하는 서비스를 이용하는 자"를 의미하며, 회사의 고객, 멤버십 회원, 이벤트 참가자 등이 이에 해당한다.

따라서 정보통신망법은 이용자가 아닌 자의 개인정보를 수집 · 이용하는 경우에는 적용되지 않는다. 기업의 내부 직원은 이용자가 아니므로, 정보통신망법 상의 개인정보보호 규정이 적용되지 않는다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
>
> 4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

좀 더 알아 봅시다

□ 이용자의 개념

- "이용자"란 사업자가 제공하는 서비스를 이용하는 자를 의미한다. 여기에는 사업자의 온라인 회원같이 계속적으로 서비스를 이용하는 경우와 일회성 또는 비정기적으로 서비스를 이용하는 경우도 모두 포함된다. 예를 들어 일시적인 이벤트에 참가하는 자, 비회원 자격으로 물품을 구매하는 자 등도 모두 이용자에 포함된다.

● 사업자가 제공하는 서비스를 이용하는 자가 아닌 경우에는 정보통신망법이 적용되지 않는다. 예를 들어 사업자와 그 사업자의 직원간의 관계, 동호회와 동호회 회원 간의 관계는 서비스를 이용하는 관계가 아니므로, 정보통신망법이 적용되지 않는다.

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ "이용자"는 사업자가 제공하는 서비스를 이용하는 자를 말함 (정보통신망법 제2조) ○ 현행 정보통신망법은 "이용자"의 개인정보만 보호대상에 포함됨	○ "정보주체"는 그 정보의 주체가 되는 사람을 말함 (개인정보보호법 제2조) ○ 개인정보보호법(안)은 모든 정보주체의 개인정보가 보호대상에 포함됨 (근로자, 동호회 회원 등도 정보주체에 포함)

제 2 장

개인정보보호의 시작은 내부관리계획 수립부터

1. 내부관리계획 그게 뭐야

2. 내부관리계획 어떻게 작성해야 하나

제2장 개인정보보호의 시작은 내부관리계획 수립부터

1. 내부관리계획 그게 뭐야

Q | 사업자는 개인정보보호를 위한 내부관리계획을 의무적으로 수립하여야 한다는데, 내부관리계획이란 어떤 것인가?

A | 내부관리계획이란 사업자가 이용자의 개인정보를 보호하기 위해 마련하여야 하는 내부 규정 · 지침을 의미한다.

사업자는 이용자의 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 않도록 안전성을 확보하기 위하여 조직 내부의 개인정보 관리계획을 수립하여야 하며, 경영진으로부터 승인을 받은 후 이를 모든 임직원과 직원에게 공지하여 준수할 수 있도록 해야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.
>
> 1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립 · 시행

좀 더 알아 봅시다

□ 내부관리계획 수립의 필요성

● 사업자는 이용자의 개인정보를 취급함에 있어 개인정보가 분실 · 도난 · 누출 ·

변조 · 훼손되지 않도록 안전성 확보에 필요한 관리적 · 기술적 조치를 취하여야 한다(정보통신망법 제28조). 그 중 관리적 조치는 개인정보보호를 위한 조직과 인력, 제도에 관한 사항으로서, 특히 내부관리계획의 수립은 관리적 보호조치의 가장 핵심적인 사항에 해당한다.

- 사업자의 개인정보보호 내부관리계획 수립은 체계적이고 전사적(全社的)인 개인정보보호 활동이 그 목적이며, 이를 위해서는 해당 기업 경영진의 적극적인 참여와 지원이 필수적이다.

벌 칙

- 사업자가 내부관리계획을 수립하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

관련 위반사례

- ○○호텔은 멤버십 회원 등 다량의 개인정보를 수집 · 취급하고 있음에도 불구하고, 정보통신망을 통한 침해사고 대응을 위한 '정보보안지침' 만을 운영하고 있고 법령에 따라 반드시 수립하도록 되어 있는 개인정보보호를 위한 내부관리계획은 전혀 수립하지 않음

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 개인정보가 분실 도난 누출 변조 훼손되지 않도록 기술적 관리적 보호조치를 하여야 함(정보통신망법 제28조) ○ 관리적 보호조치에는 내부관리계획 수립, 개인정보관리책임자 지정, 물리적 접근방지 조치 등이 포함됨	○ 개인정보 처리자는 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 않도록 내부관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적 · 관리적 · 물리적 조치를 하여야 함(개인정보보호법 제29조) ※ 현행 법률의 취지와 동일함

2. 내부관리계획 어떻게 작성해야 하나

Q | 내부관리계획에 포함되어야 하는 구체적인 내용과 내부관리계획의 작성 방법을 알고 싶다.

A | **내부관리계획에는 개인정보관리책임자의 의무 · 책임에 관한 사항, 개인정보 처리 단계별 기술적 · 관리적 보호조치에 관한 사항, 정기적 자체감사에 관한 사항, 개인정보취급자에 대한 교육 등 개인정보보호를 위해 필요한 사항이 반드시 포함되어야 한다.**

내부관리계획은 해당 사업자의 의사결정자(CEO, CPO 등)에 대한 보고 및 승인 · 결재를 거쳐 시행하여야 한다. 또한 내부관리계획은 개인정보보호 관련 법 · 제도의 변경 사항, 기업의 개인정보 관련 사업내용 변경사항 등을 즉시 반영하여야 하며, 해당 사업자의 전 직원 및 수탁 · 용역업체도 교육 · 열람되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립 · 시행

(이하 생략)

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자 등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립 · 시행하여야 한다.

1. 개인정보관리책임자의 지정 등 개인정보보호 조직의 구성 · 운영에 관한 사항
2. 개인정보취급자의 교육에 관한 사항
3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부사항

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제4조(내부관리계획의 수립 · 시행) ① 사업자는 이용자의 개인정보를 보호하기 위해 다음 각 호의 사항을 포함하여 내부관리계획을 수립 · 시행하여야 한다.

1. 내부관리계획의 수립 및 시행에 관한 사항
2. 개인정보관리책임자의 의무와 책임에 관한 사항
3. 개인정보의 처리단계별 기술적 · 관리적 보호조치에 관한 사항
4. 정기적 자체감사에 관한 사항
5. 개인정보취급자에 대한 교육 등 그 밖에 개인정보보호를 위해 필요한 사항

② 소상공인은 제1항 제1호 및 제2호를 생략하여 내부관리계획을 수립할 수 있다.

좀 더 알아 봅시다

□ 내부관리계획 작성 방법

● 사업자의 업종, 사업 규모, 영업 특성 등에 따라서 다양한 개인정보 수집 · 취급 형태가 있을 수 있으므로, 각각의 사업자는 자사의 개별적인 특성을 반영하여 내부관리계획을 작성하여야 한다.

내부관리계획 작성 양식(예시)

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)

내부관리계획 작성 양식(예시)

제3장 개인정보관리책임자의 의무와 책임
제6조(개인정보관리책임자의 지정)
제7조(개인정보관리책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적 · 관리적 보호조치
제9조(물리적 접근제한)
제10조(출력 복사시 보호조치)
제11조(개인정보취급자 접근 권한 관리 및 인증)
제12조(개인정보의 암호화)
제13조(접근통제)
제14조(접근기록의 위변조 방지)
제15조(보안프로그램의 설치 및 운영)

제5장 정기적인 자체감사
제16조(자체감사 주기 및 절차)
제17조(자체감사 결과 반영)

제6장 개인정보보호 교육
제18조(개인정보보호 교육 계획의 수립)
제19조(개인정보보호 교육의 실시)

※ 상기 내부관리계획 작성양식은 하나의 예시로서, 이를 기반으로 내부실정에 맞게 내부관리계획을 수립하여야 함

관련 위반사례

- ○○영화관은 개인정보보호를 위한 내부관리계획을 수립하기는 하였으나, 그 내용은 법령상의 개인정보보호 조문을 그대로 옮겨놓았을 뿐이며, 해당 영화관의 업무 및 영업 특성을 반영한 교육, 자체감사, 개인정보관리책임자의 지정 등에 관한 사항은 전혀 반영되어 있지 않음

제 3 장 개인정보 관리책임자와 개인정보 취급자

1. 우리 회사의 개인정보 관리책임자는 누가 되어야 할까

2. 나 홀로 사업인데 개인정보 관리책임자를 두어야 하나

3. 개인정보 취급자란

제3장 개인정보 관리책임자와 개인정보 취급자

1. 우리 회사의 개인정보 관리책임자는 누가 되어야 할까

Q | 개인정보 관리책임자를 지정해야 한다는데, 어느 정도의 직급을 책임자로 지정하면 되는지 알고 싶다.

A | 법률은 회사의 임원 또는 이용자의 고충처리를 담당하는 부서의 장이 개인정보 관리책임자가 되도록 규정하고 있으므로 사업자는 반드시 이 요건을 충족하는 자를 개인정보 관리책임자로 지정해야 한다.

또한 사업자는 개인정보 관리책임자의 성명 · 부서의 명칭, 전화번호 등 연락처를 개인정보 취급방침에 명시하고 이용자가 언제든지 쉽게 확인할 수 있도록 공개해야 하며, 개인정보 관리책임자가 변경된 경우에도 변경 사항을 지체 없이 공지해야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조(개인정보 관리책임자의 지정) ① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제13조(개인정보 관리책임자의 자격요건 등) ① 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공 받은 자(이하 "정보통신서비스 제공자등"이라 한다)가 법 제27조제1항 본문에 따라 지정하는 개인정보 관리책임자는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자로 하여야 한다.

1. 임원
2. 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장

좀 더 알아 봅시다

□ 개인정보 관리책임자(CPO)의 자격요건

● 개인정보 관리책임자는 임원 또는 고충처리를 담당하는 부서의 장으로 지정하도록 법률에서 자격요건을 정하고 있다. 이는 회사의 의사결정 · 집행을 담당하는 지위에 있는 사람이 개인정보 관리책임자가 되게 함으로써, 전사적(全社的) · 체계적으로 개인정보보호 활동을 할 수 있도록 하기 위한 취지이다.

※ CPO(Chief Privacy Officer) : 개인정보 관리책임자

● 개인정보 관리책임자는 이용자의 개인정보보호 업무와 연관성이 있는 업무를 담당하는 임원을 지정하여야 한다.

- 회사의 임원 : 예) 정보보호, CRM 등을 담당하는 임원 등
- 이용자의 고충처리 담당 부서장 : 예) 고객서비스센터장, 고객보호팀장 등

토 막 상 식

회사의 임원이란?

기업의 이사회를 구성하여 회사의 업무를 수행하고 그에 대해 책임을 지는 대표이사, 이사 및 감사를 지칭한다(주식회사 기준, 상법 참조).
소상공인 · 소규모 사업자의 경우에는 영업주 · 점주 및 그에 준하여 사업을 책임지는 자를 '임원' 으로 볼 수 있다.

● 개인정보 관리책임자의 성명(또는 개인정보보호 업무 관련 부서의 명칭)과 연락처 등은 개인정보 취급방침에 명시하여 이용자에게 공개해야 한다. 형식적으로 사업자의 대표 전화번호나 이메일 등을 개인정보 관리책임자의 연락처로 기재해서는 안되며, 반드시 개인정보보호와 관련한 고충처리 · 상담을 처리할 수 있는 연락처여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조의2(개인정보 취급방침의 공개) ① 정보통신서비스 제공자 등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

② 제1항에 따른 개인정보 취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다.

1. ~ 6. (생략)

7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

개인정보 관리책임자 공개 예시

○○○ 회사는 이용자의 개인정보를 안전하게 이용할 수 있도록 최선을 다하고 있으며, 회원의 개인정보를 보호하고 개인정보와 관련된 불만사항 및 문의를 처리하기 위하여 아래와 같이 담당부서 및 개인정보 관리책임자를 지정하고 있습니다.

개인정보 관리책임자	개인정보 관리담당자
가. 개인정보 담당부서 : 고객지원본부 나. 개인정보 관리책임자 : ○○○ 본부장 다. 전화번호 : 02)1234-0001 라. Fax : 02)1234-1000 마. 메일 : 책임자@ooo.com	가. 개인정보 담당부서 : 고객지원본부 / 개인정보보호팀 나. 개인정보 관리담당자 : ○○○ 팀장 다. 전화번호 : 02)1234-1100 라. Fax : 02)1234-1000 마. 메일 : 담당자@ooo.com

개인정보 관리책임자 공개의 잘못된 사례

○ 사업자의 대표 전화번호를 기재하는 경우
예) 1588-××××

○ 사업자의 대표 이메일을 기재하는 경우
예) webmaster@ooo.com 등

● 사업자가 개인정보 관리책임자를 지정하지 않은 경우에는 2천만원 이하의 과태료가 부과된다.

'개인정보 관리책임자의 공개'와 관련된 항목

제6장 고객의 개인정보는 철저히 관리하자

→ 1. 개인정보 취급방침, 이것만은 꼭 기억하자 (96페이지)

관련 Q&A

Q | 홈페이지를 관리하는 외주 위탁업체에서 고객DB관리 및 상담 등을 모두 처리하고 있는데, 이 위탁업체의 대표를 개인정보 관리책임자로 지정해도 되는가?

A | 개인정보 관리책임자는 해당 사업자의 임원 또는 고충처리 담당부서장으로 지정해야 한다. 홈페이지 관리 및 고객 관리 업무를 외부에 위탁하여 처리하는 경우에도, **개인정보 관리책임자는 본사 내에서 개인정보보호 업무를 담당하는 관련 임원 또는 고충처리 담당부서장이 되어야 한다.**

Q | 개인정보보호 업무를 담당하는 임원을 개인정보 관리책임자로 지정하고 해당 임원의 전화번호·이메일을 개인정보 취급방침에 공개하였는데, 일반적인 상품·서비스 문의같이 사소한 상담까지도 모두 담당 임원의 전화로 걸려오고 있다. 어떻게 하면 좋은가?

A | 반드시 개인정보 관리책임자의 성명 및 직통 연락처를 개인정보 취급방침에 기재해야 하는 것은 아니며, **"개인정보보호 업무를 처리하는 관련 부서의 명칭 및 연락처"를 기재하여도 된다.** 다만, 사업자의 대표 전화번호나 이메일 등을 개인정보 관리책임자의 연락처로 기재하는 것은 안되며, 개인정보보호와 관련한 고충처리·상담을 처리할 수 있는 연락처를 공개하여야 한다.

관련 위반사례

- ○○학원은 개인정보 관리책임자를 임원 또는 고충처리 담당 부서의 장으로 지정하지 않고, 단순 실무자급에 불과한 A씨를 개인정보 관리책임자로 지정 · 공개

- ○○여행사에서 임원으로 재직하던 B씨는 개인정보 관리책임자로 지정되어 업무를 수행하다 퇴직하였으나, ○○여행사는 개인정보 관리책임자를 새롭게 지정하지 않고 B씨를 개인정보 관리책임자로 계속 홈페이지 상에 공개하고 있음

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 '개인정보 관리책임자'를 지정하여야 함 (정보통신망법 제27조)	○ 개인정보처리자는 '개인정보보호책임자'를 지정하여야 함 (개인정보보호법 제31조) ※ 현행 법률상의 '개인정보 관리책임자' 명칭이 '개인정보 보호책임자'로 변경 되었으나, 제도의 취지는 동일 ○ 개인정보 보호책임자는 개인정보보호 계획의 수립 · 시행, 불만처리 및 피해구제, 유출 · 오남용 방지를 위한 시스템 구축, 교육계획 수립 · 시행 등의 업무를 수행함

2. 나홀로 사업인데 개인정보 관리책임자를 두어야 하나?

Q | 비디오·DVD 대여점을 운영하는 개인 사업자이다. 별도의 직원은 없고 부인과 함께 점포를 운영하고 있는데, 우리 같은 소규모 개인사업자도 개인정보 관리책임자를 꼭 지정해야 하는가?

A | **"상시 종업원이 5명 미만"인 소규모 사업자는 개인정보 관리책임자를 지정하지 아니할 수 있다.** 이 경우에는 그 사업자의 사업주·대표자가 별도의 지정 절차 없이 자동적으로 개인정보 관리책임자가 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조(개인정보 관리책임자의 지정) ① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

② 제1항 단서에 따른 정보통신서비스 제공자등이 개인정보 관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 관리책임자가 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제7조 (개인정보 관리책임자의 자격요건 등) ① (생략)

② 상시 종업원 수가 5명 미만인 정보통신서비스 제공자 외의 자는 법 제27조제1항 단서 및 법 제67조제1항에 따라 개인정보 관리책임자를 지정하지 아니할 수 있다.

좀 더 알아 봅시다

□ 소규모 사업자의 개인정보 관리책임자 지정

● 상시 종업원 5명 미만의 소규모 사업자는 개인정보 관리책임자를 지정하지 않을 수

있으나, 소규모 사업자의 사업주 · 대표자 등은 개인정보 관리책임자로서의 직무를 수행하여야 한다(이용자 고충처리 등).

토 막 상 식

상시 종업원 수의 판단기준

상시 종업원(근로자)의 수는 일반적으로 "직전 사업연도의 매월 말일 현재의 상시 근로자 수를 합하여 12로 나눈 인원"을 의미한다(중소기업기본법 시행령 제5조제2항).

중소기업의 상시 종업원(근로자)는 일용근로자 및 3개월 이내 기간을 정해 근로하는 자(단기 아르바이트 등)를 제외한 근로자를 말한다(중소기업기본법 시행령 제5조제1항).

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 상시 종업원 5명 미만 소규모 사업자는 개인정보 관리책임자를 지정하지 않을 수 있고, 이 경우 사업주 · 대표자가 자동적으로 개인정보 관리책임자가 됨 (정보통신망법 제27조)	○ 법률에는 소규모 사업자의 개인정보 보호책임자 지정에 대한 규정은 없으며, 개인정보 보호책임자의 지정요건 및 자격요건 등은 시행령에 규정 예정 (개인정보보호법 제31조제6항)

3. 개인정보 취급자란?

Q | '개인정보 취급자'란 개인정보보호 업무를 직접적으로 담당하는 직원만을 지칭하는 것인지 알고 싶다.

A | **개인정보 취급자라 함은 이용자의 개인정보를 '취급'하는 자를 말한다.** 여기에는 회원가입, 탈퇴처리, 고충처리 등과 같이 개인정보보호 업무를 직접 담당하는 직원과 그 외에 업무상 필요에 의해 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등의 업무를 하는 자가 모두 포함된다.

> **사업자의 개인정보 보호조치 기준(제정 2010.12.30. 행정안전부 고시 제2010-86호)**
> **제2조(정의)** 이 기준에서 사용하는 용어의 뜻은 다음과 같다.
> 5. "개인정보취급자"라 함은 사업자의 사업장 내에서 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

□ 개인정보 취급자의 범위

- 개인정보 취급자란 이용자(고객)의 개인정보에 대한 접근권한을 가지고 업무상 개인정보를 처리하는 모든 자를 말한다.
  - 예를 들어 회원 가입과 탈퇴, 개인정보 관련 상담 · 고충처리, 개인정보관리 시스템 · DB 운영 등과 같이 직접적인 개인정보보호 업무에 종사하는 자는 물론이고, 그 외에 업무상 필요에 의해 고객의 개인정보를 열람 · 활용하고 있는 영업 · 마케팅 업무 종사자, A/S 업무 종사자 등도 모두 개인정보취급자에 포함된다.

□ 개인정보 취급자의 제한

● 사업자는 개인정보 취급자를 최소한으로 제한하여야 한다. 이는 업무상 개인정보 취급이 반드시 필요하지는 않음에도 불구하고 개인정보에 대한 접근권한이 무분별하게 부여됨에 따라 해당 직원에 의해 개인정보의 접근 및 유출, 오 · 남용이 발생하는 것을 방지하기 위한 취지이다.

개인정보보호법이 제정되면 이렇게 달라집니다

현 재	법 제정후
○ 개인정보취급자를 최소한으로 제한 (정보통신망법 제28조) ○ 개인정보취급자에 대한 교육, 개인정보처리시스템 접속기록의 보관 · 확인 · 감독 등 보호조치 규정 (정보통신망법 시행령 제15조)	○ 개인정보취급자에 대한 관리 · 감독, 교육, 보호조치 등 규정 (개인정보보호법 제28조)

관련 Q&A

Q | 업무 처리를 위해서 아르바이트 직원에게 고객 개인정보를 열람할 수 있도록 했는데, 이 경우도 개인정보 취급자에 해당하는가?

A | 아르바이트 등 임시직 직원도 업무상 필요에 의해 개인정보를 열람 · 처리하고 있다면 개인정보 취급자에 해당된다. 따라서 이 경우에도 개인정보의 열람 · 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한해야 하며, 보안서약서를 징구하는 등 필요한 관리조치를 취하여야 한다.

관련 위반사례

- ○○화재보험회사는 '고객 차량조회 시스템'을 업무상 필요상 최소한의 범위 안에서만 열람되도록 하였어야 하나, 이를 어기고 보험대리점 직원에게도 아무런 제약 없이 시스템을 통한 고객정보 열람을 허용함에 따라 A 보험대리점 직원이 이를 악용하여 고객정보를 유출

사업자를 위한 개인정보보호 질의·응답집

제 4 장 개인정보를 수집하고 이용하려면

1. 회원가입 · 이벤트 시 고객의 동의를 받자

2. 민감한 개인정보를 수집하고 있지는 않은가

3. 개인정보는 최소한으로 수집하자

4. 14세 미만 아동의 개인정보 수집은 이렇게 하자

5. 수집 · 이용목적이란 무엇일까

6. 목적외 이용이 되지 않게 하려면

7. 개인정보 활용 목적이 달라지면 무엇을 해야 하나

제4장 개인정보를 수집하고 이용하려면

1. 회원가입 · 이벤트 시 고객의 동의를 받자

Q | '온라인 이벤트'를 개최하는 경우에도 개인정보 수집에 관하여 동의절차를 꼭 거쳐야 하는지 궁금하다.

A | 사업자가 이용자의 개인정보를 수집하는 경우에는 수집 · 이용 목적, 수집 개인정보 항목, 개인정보 보유 · 이용 기간을 이용자에게 알리고 동의를 받아야 한다.

따라서 일반적인 회원 · 멤버십 가입을 위해 개인정보를 수집하는 경우는 물론이고, 한시적 · 임시적인 이벤트 행사 개최, 비회원을 대상으로 한 물품 판매 등을 위해 개인정보를 수집하는 경우에도 고지사항을 알리고 동의를 받아야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제22조(개인정보의 수집 · 이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
>
> 1. 개인정보의 수집 · 이용 목적
> 2. 수집하는 개인정보의 항목
> 3. 개인정보의 보유 · 이용 기간

좀 더 알아 봅시다

□ 개인정보 수집 동의를 얻어야 하는 경우

● 사업자가 "이용자의 개인정보를 이용하기 위해 수집하는 경우"라 함은 온라인 ·

오프라인을 불문하고 회원 가입, 이벤트 참여, 상품 판매 계약, 수강 등록 등 이용자의 개인정보를 요구하는 모든 경우를 의미한다.

개인정보 수집 · 이용시 동의를 얻어야 하는 경우(예시)

구분	예시
회원가입	• 인터넷 웹사이트 회원 가입 • 백화점, 할인점, 항공사, 프랜차이즈, 영화관, 정유사 등의 멤버십 또는 포인트 제도 가입 등
서비스 제공	• 결혼중개업의 서비스 이용을 위해 가입신청서 작성 • 피트니스클럽 가입신청서 작성 • 학원 수강을 위해 수강생이 등록신청서 작성 • 자동차 매매 또는 렌트를 위해 계약서 작성 등
이벤트 행사	• 경품행사 등 이벤트 참여를 위한 개인정보 요구 • 무료쿠폰 발행, 무료 제휴서비스(보험 등) 가입을 위해 개인정보 요구 • 상담, A/S 신청 등록을 위한 개인정보 요구 등

□ 동의 획득시 고지사항

● 이용자의 개인정보를 수집하는 경우에는 아래의 사항을 알리고 동의를 받아야 한다.

① 개인정보의 수집 · 이용 목적

② 수집하는 개인정보 항목

③ 개인정보 보유 · 이용기간

● 이들 고지사항은 개인정보의 수집사유에 따라 가능한 구체적으로 상세히 알려야 하며, 이중 하나라도 누락되어서는 아니 된다.

이벤트를 위한 개인정보 수집시 동의 획득 예시

○ 개인정보의 수집 이용목적 : 경품 당첨 시 본인 확인, 경품배송
○ 수집하는 개인정보의 항목 : 성명, 휴대전화번호, 이메일, 주소
○ 개인정보의 보유 및 이용기간 : 이벤트 종료 후 제세공과금 처리, 상품배송 완료시까지 보유 후 파기

동의함 □ 동의안함□

□ 동의를 받지 않아도 되는 경우

● 다음의 경우에는 이용자의 동의 없이도 개인정보를 수집 · 이용할 수 있다.

① 서비스 이용계약 이행을 위해 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우

– (예) 서비스 이용 과정에서 결제기록 등 불가피하게 계속적으로 생성되는 정보도 개인정보의 일종으로 볼 수 있으나, 매번 생성 · 수집시마다 이용자에게 고지하고 동의를 받는 것은 현실적으로 곤란하므로 이 경우에는 동의 없이 개인정보 수집 가능

② 서비스 제공에 따른 요금정산에 필요한 경우

– (예) 사업자의 서비스 제공에 대한 요금 미납액이 있을 경우, 정당한 채권추심 절차에 따라 요금정산이 완료 될 때까지 이용자 동의 없이 개인정보 수집 가능

③ 이 법 또는 다른 법률의 특별한 규정이 있는 경우

– (예) 정보통신망법 제31조의 규정에 따라, 만 14세 미만 아동의 개인정보 수집시 법정대리인의 동의획득을 위한 성명 · 연락처 등 최소한의 정보는 동의 없이 아동으로부터 수집 가능

정보통신망 이용촉진 및 정보보호 등에 관한 법률

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

관련 Q&A

Q | 홈페이지에서 회원가입을 받을 때 「개인정보 취급방침」 전체를 고객에게 알리고 동의를 받고 있다. 이러한 방법도 괜찮은가?

A | 이전에는 개인정보 수집시 개인정보 취급방침에 동의내용을 기재하여 포괄적으로 동의를 받을 수 있었으나, 정보통신망법 개정(2007.08.07)에 따라 동의내용을 따로 고지하여 동의를 얻도록 변경되었다. 따라서 사업자는 개인정보를 수집하는 경우에 개인정보 취급방침을 게재하여 동의를 얻는 것은 허용되지 않으며, "수집 · 이용목적, 수집 항목, 보유 · 이용기간"을 이용자가 명확하게 인지하고 확인할 수 있도록 기재하여 동의를 얻어야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률 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.

Q | 오프라인에서 경품 이벤트를 진행하려고 하는데, 응모권이 너무 작아 법률에서 정한 개인정보 수집 고지사항을 모두 기재하는 것이 어렵다. 어떻게 하면 좋은가?

A | 오프라인에서 개인정보를 수집하는 경우에도 "수집 · 이용목적, 수집 항목, 보유 · 이용기간"을 빠짐없이 고지하여 동의를 얻어야 한다.

다만, 용지가 작은 참가신청서 등과 같이 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우에는 이용자에게 동의 내용을 확인할 수 있는 방법(경품 이벤트에 대한 동의 내용이 게재되어 있는 인터넷 주소, 동의 내용을 안내받을 수 있는 사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.

> '동의내용을 표시하기 어려운 경우'와 관련된 항목
>
> 제5장 고객의 개인정보를 제3자에게 제공 · 위탁하려면
> → 9. 동의 받는 방법 총정리 (87페이지)

관련 위반사례

- ○○투어는 인터넷 홈페이지에서 회원가입을 받을 때는 개인정보 수집시의 동의 내용(수집 · 이용목적, 수집항목, 보유 · 이용기간)을 모두 고지하고 동의를 받고 있었으나, 오프라인에서 여행상품 판매계약을 체결하면서 개인정보를 수집할 때에는 계약서에 동의내용을 고지하지 않고 계약을 체결하였음
- ○○쇼핑센터는 경품 이벤트를 진행하면서, 이벤트 응모권에 동의내용(수집 · 이용목적, 수집항목, 보유 · 이용기간)을 고지하지 않고 개인정보를 수집

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ (수집원칙) 개인정보 수집시 반드시 동의를 받아야 함 ○ (고지사항) 1) 수집 · 이용목적 2) 수집 항목 3) 보유 · 이용기간 (정보통신망법 제22조)	○ (수집원칙) 다음의 요건에 해당하는 경우 개인정보 수집 가능 ① 정보주체의 동의 ② 법률의 특별한 규정 또는 법령상 의무준수를 위해 불가피 ③ 공공기관 소관업무 수행에 불가피 ④ 정보주체와의 계약체결 · 이행을 위해 불가피 ⑤ 정보주체 등의 생명 · 신체 · 재산 이익을 위해 필요(사전 동의가 곤란한 경우) ⑥ 개인정보처리자의 정당한 이익 달성을 위해 필요(명백히 정보주체 권리보다 우선하는 경우) ○ (정보주체 동의를 얻어 수집하는 경우의 고지사항) 1) 수집 · 이용목적 2) 수집 항목 3) 보유 · 이용기간 4) 정보주체에게 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법 제15조)

2. 민감한 개인정보를 수집하고 있지는 않은가

Q | 장애우에 대한 요금감면 혜택을 제공하기 위해서는 상세한 장애등급 정보가 필요한데, 수집할 수 있는지?

A | 사업자는 사상 · 신념 · 과거의 병력(病歷) 등과 같이 "이용자 개인의 권리 · 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 민감한 개인정보"를 수집해서는 안된다.

다만, 특정한 서비스를 제공하기 위하여 이용자의 동의를 받은 경우나, 다른 법률에 따라 특별히 수집이 허용된 경우에는 민감정보를 수집할 수 있다.

장애우나 기초생활수급자 등에 대한 요금감면 혜택을 제공하기 위해 민감정보를 수집하는 경우에는 그 수집 · 이용목적 등을 명확히 고지하고 동의를 받아 수집할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제23조(개인정보의 수집의 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리 · 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다.

좀 더 알아 봅시다

□ 민감정보의 개념

● 개인의 권리 · 이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보는 이른바 '민감정보' 로 분류된다. '민감정보' 에는 사상, 신념, 과거의 병력(病歷) 이외에도

인종, 민족, 정치적 성향, 노조가입 여부, 전과기록, 신체장애 정보, 성생활 · 성적취향 정보 등이 포함된다.

□ 민감정보를 수집해야 하는 경우

● 민감정보는 일반적인 개인정보에 비해 개인의 사생활 침해 우려가 크기 때문에 법률은 원칙적으로 민감정보 수집을 금지하고 있다. 다만 서비스의 유형 특성에 따라서는 부득이하게 민감정보를 수집해야 하는 경우가 있다. 이 때에는 이용자의 동의를 받거나, 다른 법률에 따라 수집 대상 개인정보로 허용된 경우에 한해 민감정보를 수집할 수 있다.

● 예를 들어 「전기통신사업법」에서는 장애인이나 저소득층에 대해 통신 요금감면 혜택을 규정하고 있는데, 이를 위해서는 전기통신사업자가 서비스 가입단계에서 신체장애 정보, 기초생활수급자 해당여부 등의 정보를 수집할 필요가 있다. 이때에는 민감정보의 수집 · 이용목적(‘「전기통신사업법」에 따른 요금감면 혜택 제공’)을 명확히 알리고 동의를 받아 수집 · 이용할 수 있다.

토 막 상 식

통신서비스의 요금감면 대상

통신서비스의 요금감면 대상은 장애인(장애인 복지시설 · 단체 포함), 기초생활 수급자 중 18세 미만 65세 이상이거나 중증장애인인 자, 국가유공자 중 전상군경 · 공상공무원, 5.18 민주화운동 부상자 등이다. (「전기통신사업법」 시행령 제2조제3항)

● 사업자가 이용자의 동의 없이 민감 정보를 수집한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

● ○○국제결혼중개회사는 국제결혼 성사를 위해 회원의 인종 · 민족 등 민감정보를 수집하면서, 이를 수집하는데 대한 동의를 전혀 받지 않음

현 재	법 제정후
○ 사업자는 사상, 신념, 과거의 병력(病歷) 등 민감 개인정보를 수집할 수 없음 ○ 다만, 이용자의 동의를 받거나 또는 다른 법률에 의해 수집이 허용된 경우는 수집할 수 있음 (정보통신망법 제23조)	○ 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보 및 기타 정보주체의 사생활을 현저히 침해할 우려가 있는 정보는 처리할 수 없음 (개인정보보호법 제23조) ※ 현행 법률의 취지와 동일함

3. 개인정보는 최소한으로 수집하자

Q | 고객들에게 보다 빠른 전화상담 서비스를 제공하기 위하여, 전화 상담 전에 반드시 주민등록번호를 입력하도록 하고, 주민등록번호를 입력하지 않은 사람(비회원)에 대해서는 상담 서비스를 제공하지 않을 계획이다. 이러한 방법이 문제가 없는지 알고 싶다.

A | 사업자가 이용자의 개인정보를 수집하는 경우에는 **서비스 제공을 위하여 필요한 최소한의 정보(필수정보)와 개인별 맞춤서비스 등을 위한 상세정보(선택정보)를 구분하여 수집하여야 한다.** 그리고 이용자가 필수정보 외의 개인정보를 제공하지 않는다는 이유로 그 서비스의 제공을 거부해서는 아니 된다.

주민등록번호는 전화상담 서비스 제공에 반드시 필수적인 정보로 보기는 어려우므로, 회원 · 비회원 구분을 위해서 모든 전화상담 고객에게 주민등록번호를 요구하는 것은 과도한 개인정보 수집에 해당될 수 있다.

> **정보통신망 이용촉진 및 정보보호등에 관한 법률**
>
> 제23조(개인정보의 수집의 제한 등) ② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다.

좀 더 알아 봅시다

□ 필요 최소한의 정보수집

● 사업자는 마케팅 활용 등 다양한 목적을 위해서 개인정보를 수집할 필요가 있으나, 필요 이상의 개인정보까지 과도하게 수집 · 집적하게 된다면 개인정보가 유출된

경우 피해가 더욱 확산될 우려가 있다. 따라서 관련 법률은 개인정보 수집시 필수정보와 선택정보를 구분하고, 선택정보를 제공할지의 여부는 이용자 스스로의 선택에 따르도록 하고 있다.

□ 필수정보와 선택정보의 구분 기준

● 필수정보와 선택정보의 구분은 해당 서비스의 특성 등을 고려하여 판단하여야 한다.

서비스 특성에 따른 필수정보의 예시

구분	예시
결혼경력(결혼여부, 재혼여부, 자녀수 등)	• 결혼중개서비스에 가입하는 경우, 필수정보가 될 수 있음
금융정보(신용카드, 계좌정보 등)	• 온라인 쇼핑몰에서 물품 구매 및 결제를 하는 경우, 필수정보가 될 수 있음

● 사업자가 필요 최소한의 정보 외의 개인정보(선택정보)를 제공하지 아니한다는 이유로 서비스 제공을 거부하는 경우에는 3천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 회원가입시에는 필수정보와 선택정보를 구분해서 수집하고 있지만, 개인정보 취급방침의 "수집 개인정보 항목"에는 필수정보/선택정보를 따로 구분하지 않고 있다. 문제가 없는가?

A | 개인정보 취급방침에도 실제 수집하는 필수정보와 선택정보를 반드시 구분하여 명시하여야 한다.

관련 위반사례

- ○○리조트는 멤버십 회원가입 신청서를 통해 개인정보를 수집하는 과정에서 '직장 부서 · 직급, 최종학력, 연소득, 주거형태, 동산/부동산 보유 현황' 등 상세한 개인정보를 모두 필수적으로 기재하도록 하고, 항목이 누락될 경우에는 회원가입을 불허

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 서비스 제공에 필요한 최소한의 개인정보(필수정보)를 수집해야 함 ○ 필수정보 외의 개인정보 미제공을 이유로 서비스 제공을 거부할 수 없음 (정보통신망법 제23조)	○ 개인정보 처리자는 개인정보 수집 목적에 필요한 최소한의 개인정보만을 수집해야 함 ※ 현행 법률의 취지와 동일함 ○ 필요 최소한의 개인정보(필수정보)에 해당한다는 입증책임은 개인정보 처리자에게 있음 (개인정보보호법 제16조)

4. 14세 미만 아동의 개인정보 수집은 이렇게 하자

Q | 초등학생을 대상으로 하는 온라인 교육서비스를 제공하려 한다. 만 14세 미만 아동의 회원가입은 부모의 동의가 필요하다고 들었는데, 부모에게 연락하여 동의를 받으려면 최소한 부모의 성명이나 연락처 정보가 있어야 하는데 이러한 정보는 어떻게 얻어야 하는가?

A | 사업자가 만 14세 미만 아동의 개인정보를 수집 · 이용 · 제공하기 위해서는 부모 등 법정대리인으로부터 동의를 받아야 한다.

다만, 사업자가 법정대리인의 성명이나 연락처 등을 모르는 경우 법정대리인의 동의를 받는 것이 곤란하므로, 이 경우 **사업자는 법정대리인의 성명 · 연락처 등 동의획득에 필요한 최소한의 개인정보를 요구할 수 있다.**

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제31조 (법정대리인의 권리) ① 정보통신서비스 제공자등이 만 14세 미만의 아동으로부터 개인정보 수집 · 이용 · 제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 한다. 이 경우 정보 통신서비스 제공자는 그 아동에게 법정대리인의 동의를 받기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다.

좀 더 알아 봅시다

□ 아동 개인정보 수집제한

● 14세 미만 아동은 개인정보의 중요성에 대한 인식이 충분치 않고, 정보를 평가하거나 서비스의 진위를 파악하는 능력이 부족하여 사업자에게 자신이나 부모의

정보를 무분별하게 제공함으로써 불이익을 당할 우려가 있다.

● 이에 따라 법률에서는 만 14세 미만 아동의 개인정보를 수집하는 경우에는 부모 등 법정대리인의 동의를 얻도록 함으로써 아동 및 법정대리인의 개인정보를 보다 엄격하게 보호하고 있다.

토 막 상 식

법정대리인

아동 등에 대해 법률상 대리권을 행사할 수 있는 자를 말한다. 일반적으로는 민법의 규정에 따라 부모(친권자)가 법정대리인이 된다. 이 외에 부모의 사망 등으로 친권자가 없어진 경우에는 후견인이 법정대리인이 된다.

□ 법정대리인의 동의를 위한 정보 요구

● 아동을 대상으로 하는 각종 온라인 서비스가 특화되어 있는 반면, 아동은 항상 법정대리인과 함께 서비스를 이용하는 것이 아니므로 서비스 가입시마다 법정대리인과 동행하여 동의를 하도록 하는 것은 실제 사업 현장에서는 매우 번거롭고 불편을 야기할 수 있다.

● 따라서 법률에서는 법정대리인의 동의를 받기 위해 성명 · 연락처 등 최소한의 정보를 미리 요구할 수 있도록 하고 있다. 다만 이 정보들은 법정대리인의 동의 획득의 목적으로만 사용되어야 하며, 일정 기간이 지나도 법정대리인의 회신이 없거나 또는 법정대리인이 수집에 대한 거부의사를 명백히 밝힌 때에는 법정대리인의 그 개인정보를 지체 없이 파기해야 한다.

벌 칙

● 사업자가 법정대리인의 동의를 받지 않고 만 14세 미만 아동의 개인정보를 수집하는 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

관련 위반사례

● ○○학원은 만 14세 미만 아동의 개인정보를 수집하는 경우에는 법정대리인의 동의를 얻어야 함에도 불구하고, 하교하는 초등학교 아동들을 대상으로 이름, 학년, 반, 전화번호, 부모연락처, 부모직업 등의 개인정보를 부모 동의 없이 수집한 뒤 이를 이용하여 학원 홍보활동을 함

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 만 14세 미만 아동의 개인정보 수집시 법정대리인의 동의를 받아야 함 (정보통신망법 제31조)	○ 만 14세 미만 아동의 개인정보 처리시 법정대리인의 동의를 받아야 함 ※ 현행 법률의 취지와 동일함 (개인정보보호법 제22조제5항)

5. 수집 · 이용목적이란 무엇일까

Q | 신상품 출시를 안내하는 홍보 이메일을 보내려고 한다. 지난번 경품 이벤트에 응모했던 고객 리스트를 활용하여 상품광고를 해도 문제가 없는지 알고 싶다.

A | 사업자는 이용자의 개인정보를 수집하는 경우 '수집 · 이용목적'을 알리고 동의를 얻어야 한다. '수집 · 이용목적'이란 개인정보가 사용되는 목적과 범위 · 내용을 구체적으로 나타낸 것을 말한다.

사업자가 수집한 개인정보는 이용자로부터 동의 받은 '수집 · 이용목적'의 범위안에서만 이용할 수 있다. 만약 동의 받은 수집 · 이용목적이 변경되거나 추가된 경우에는 변경 · 추가된 목적에 대해 별도의 동의를 받아야 한다.

경품 이벤트를 통해 개인정보를 수집하였는데 이벤트 활용 목적으로만 동의를 받고 "별도의 상품 광고"에 대해서는 동의를 받지 않았다면, 해당 개인정보는 상품 출시 안내 이메일 발송 등의 광고 목적으로 이용할 수 없으며, 이를 이용하기 위해서는 별도의 동의를 받아야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제24조(개인정보의 이용 제한) 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

좀 더 알아 봅시다

□ 수집 · 이용목적의 범위

● 사업자는 이용자의 동의를 얻은 '수집 · 이용목적' 범위 안에서만 개인정보를

이용해야 한다. '수집 · 이용목적'은 최대한 구체적으로 상세하게 설명되어야 하며, 사업자가 개인정보를 수집할 때에는 이용자에게 이를 알리고 동의를 획득하여야 한다. 일부의 경우 매우 모호하게 표현된 '수집 · 이용목적'을 이용자에게 알리고 동의를 얻는 경우가 있는데 이는 허용되지 않는다.

● 이용자의 동의 없이 개인정보를 수집할 수 있는 경우는

1) 서비스 제공 계약이행에 필요한 경우

2) 서비스 제공에 따른 요금정산에 필요한 경우

3) 법률에 특별한 규정이 있는 경우이다.

이러한 예외 사유에 해당되어 수집한 개인정보는 그 해당 목적의 범위 내에서만 이용할 수 있다. 예컨대 요금정산을 위해 수집한 요금액 납부 또는 미납 사실 등에 관한 개인정보는 반드시 요금 정산의 목적으로만 이용되어야 하며, 별도의 목적으로 이용하는 것은 허용되지 않는다.

● 사업자가 이용자의 개인정보를 동의받은 목적과 다른 목적으로 이용한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

● ○○호텔은 회원가입을 받기 위해 고객의 개인정보를 수집하면서 '개인정보 수집 · 이용목적'을 구체적이고 상세하게 명시하지 않고, 단지 "고객에게 서비스를 제공하기 위한 목적, 고객에게 혜택을 제공하기 위한 목적" 등으로 매우 모호하게 표현하여 동의를 받았으며, 이후 이를 근거로 제휴 서비스 마케팅 등을 실시

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 이용자의 개인정보를 동의 받은 목적과 다른 목적으로 이용할 수 없음 (정보통신망법 제24조)	○ 개인정보처리자는 정보주체의 동의를 받은 수집 목적의 범위 내에서 개인정보 이용 가능하며, 그 범위를 초과한 이용 금지 ※ 현행 법률의 취지와 동일함 (개인정보보호법 제15조, 제18조)

6. 목적외 이용이 되지 않게 하려면

Q | 치과의원에서 치아교정 환자들의 교정 결과를 사진으로 촬영하여 의원 홈페이지의 "교정 성공 사례"에 게시하려는 경우에 문제는 없는가?

A | 사업자는 이용자의 개인정보를 수집하는 경우 '수집·이용목적'을 고지하고 동의를 얻어야 한다. 사업자가 수집한 개인정보는 그 수집·이용목적의 범위 내에서만 이용할 수 있으며, 이용자로부터 동의받은 수집·이용목적을 벗어나서 이용할 수 없다.

병원에서 환자의 진료결과 사진을 홍보 목적으로 활용하기 위해서는 '촬영한 사진을 병원의 홍보 목적'으로 게재한다는 사실을 이용자(환자)에게 명확히 알리고 동의를 얻어야 한다.

만일 수집한 개인정보를 별도의 고지·동의 절차 없이 홍보 목적으로 임의로 사용한다면 이는 '개인정보의 목적외 이용 행위'에 해당된다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제24조(개인정보의 이용 제한) 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

좀 더 알아 봅시다

□ 목적외 이용 금지

● 개인정보보호 관련 법률·제도가 체계화되기 이전에는 사업자가 자신의 고객

개인정보를 영업 활동에 사용하는 것에 대해 별다른 제약이 없었다. 그러나 최근에는 개인정보의 활용 가치가 높아지면서, 정보주체(개인)가 자신의 개인정보가 언제 어디서 어떻게 활용되는지에 대해 스스로 결정하고 통제할 수 있는 '개인정보 자기결정권'이 인정되게 되었다. 특히, 개인정보를 어떤 목적으로 어떻게 이용하겠다는 '수집 · 이용목적'의 범위 내에서만 이용되어야 하며, 이를 벗어나서 임의로 이용하는 것은 정보주체에 대한 개인정보 자기결정권을 침해하는 행위가 된다.

- 법률은 사업자가 이용자(고객)의 개인정보를 임의로 여러 목적에 이용하는 것을 금지하고 있으며, 고객의 동의를 얻은 '수집 · 이용목적' 내에서만 이용하도록 하고 있다.

- 사업자가 이용자의 개인정보를 동의받은 목적과 다른 목적으로 이용한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

관련 Q&A

Q | 학교 졸업앨범, 동창회 명부 등 공개 정보를 이용한 마케팅은?

A | 이른바 "공개되어 있는 개인정보"는 당초 공개된 목적 내에서만 이용할 수 있다. 예컨대 동창회 명부라면 해당 회원들의 상호 연락 및 친목 도모에만 이용될 수 있으며 회원의 동의를 얻지 않은 마케팅 행위 등에는 이용할 수 없다.

관련 위반사례

- ○○성형외과 병원은 환자의 성형전후 얼굴사진을 병원 홍보목적으로 이용하기 위해 환자 본인의 동의를 얻었어야 하나, 이에 대한 동의를 받지 않고 임의로 병원 홈페이지에 "성형 우수사례 사진"으로 게재

- ○○보험사는 고객들의 개인정보를 별도의 보험상품 마케팅에 이용하기 위해 고객들의 동의를 받지 않고 새로운 보험 대출상품 등이 출시될 때마다 개인정보를 이용해 광고 · 마케팅을 실시

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 이용자의 개인정보를 동의 받은 목적과 다른 목적으로 이용할 수 없음 (정보통신망법 제24조)	○ 개인정보처리자는 정보주체의 동의를 받은 수집 목적의 범위 내에서 개인정보 이용 가능하며, 그 범위를 초과한 이용 금지 (개인정보보호법 제15조, 제18조) ※ 현행 법률의 취지와 동일함

7. 개인정보 활용목적이 달라지면 무엇을 해야 하나요

Q | 서점의 멤버십 회원을 대상으로 도서할인 이벤트 안내 이메일을 발송하려고 한다. 그런데 회원들이 작성했던 멤버십 가입신청서에는 "마케팅 활용"에 대한 고지사항이 따로 기재되어 있지 않았다. 이 경우 이메일을 보내도 문제는 없는가?

A | **원래의 개인정보 수집. · 이용목적이 변경되거나 추가되는 경우에는 별도의 동의를 받아야 한다.**

즉, 최초 멤버십 가입시에 기본적인 서비스 목적으로만 동의를 받고 "마케팅 활용"에 대해서는 따로 동의를 받지 않았다면 이벤트 안내 이메일 발송 등 마케팅 행위에 이용할 수 없으며, 이를 위해서는 별도의 동의를 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제24조(개인정보의 이용 제한) 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의 받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

좀 더 알아 봅시다

□ 이용목적 변경시 동의 획득

● 사업자는 이용자의 동의를 얻은 '수집 · 이용목적' 범위 안에서만 개인정보를 이용해야 한다. 그러나 이용자들에게 서비스를 제공하면서 수집 및 이용목적이 추가되거나 확대되는 경우가 발생하며, 이 때 사업자는 이용자에게 변경된 내용으로 다시 동의를 받아야 한다.

수집 · 이용목적 변경시 동의를 얻어야 하는 경우(예시)

- 상품 배송 목적으로만 수집한 개인정보를 자사 상품의 통신판매 광고에 이용 시
- 고객 만족도 조사, 판촉행사, 경품행사 만을 위해 수집한 개인정보를 자사의 할인 판매 행사 안내용 광고물 발송에 이용 시
- A/S 센터에서 불편 처리를 위해서만 수집한 개인정보를 자사의 신상품 광고에 이용 시
- 회원으로 가입하기 위하여 제공한 정보를 회원가입과 무관한 우편 주문 판매에 이용 시
- 임상목적으로 촬영한 환자의 수술사진을 병원 홍보 목적으로 공개하는 경우

● 사업자가 이용자의 개인정보를 동의받은 목적과 다른 목적으로 이용한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

관련 위반사례

● ○○초고속인터넷 사업자는 개인정보 수집 · 이용목적을 변경하면서 고객의 동의를 받아야 하나, 고객 가입 당시에 '부가서비스 홍보' 목적에 대해 고지 · 동의를 받지 않았으며 이후 A 부가서비스가 출시되자 변경된 개인정보 수집 · 이용목적에 대해 고지 · 동의를 얻지 않고 A 부가서비스 홍보를 실시

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 이용자의 개인정보를 동의받은 목적과 다른 목적으로 이용할 수 없음 (정보통신망법 제24조)	○ 개인정보처리자는 정보주체의 동의를 받은 수집 목적의 범위 내에서 개인정보 이용 가능하며, 그 범위를 초과한 이용 금지 (개인정보보호법 제15조, 제18조) ※ 현행 법률의 취지와 동일함

사업자를 위한 개인정보보호 질의·응답집

제 5 장 개인정보를 제3자에게 제공 · 위탁하려면

1. 수집한 정보를 제3자에게 제공할 때 지켜야 할 사항

2. 이런 경우도 제3자 제공인가

3. 수사기관이 개인정보를 요구할 때는

4. 제3자 제공과 개인정보 취급위탁 구별하기

5. 개인정보 업무를 외주업체에 위탁할 때 주의사항

6. 개인정보 취급위탁시에는 언제나 동의를 받아야 하나

7. 개인정보 취급위탁 계약을 체결할 때의 주의사항은

8. 대리점의 개인정보 유출방지를 위한 노력

9. 동의 받는 방법 총정리

10. 영업을 양도하거나 합병할 때는

제5장 개인정보를 제3자에게 제공 · 위탁하려면

1. 수집한 정보를 제3자에게 제공할 때 지켜야 할 사항

Q | △△호텔 내에 면세점이 새로이 입점하게 된 것을 계기로, 호텔 멤버십 고객정보를 면세점과 공유하고 면세점은 이를 활용하여 할인 이벤트 홍보를 하기로 하였다. 호텔 내에 면세점이 입점해 있고 명칭도 "△△호텔 면세점"이라고 쓰는데 이런 경우에도 고객의 동의를 받아야 하는가?

A | 사업자가 이용자(고객)의 개인정보를 제3자에게 제공하는 경우에는 아래의 사항을 고지하고 동의를 얻어야 한다.

① 개인정보를 제공받는 자
② 제공받는 자의 이용 목적
③ 제공하는 개인정보 항목
④ 제공받는 자의 보유 · 이용기간

호텔과 면세점이 호텔 고객정보를 공유하고 이벤트에 활용하기로 하였다면 호텔 고객정보를 제3자(면세점)에 제공하는데 대해 고객들에게 알리고 동의를 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제24의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

② 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

좀 더 알아 봅시다

□ 개인정보 제3자 제공 규제의 취지

● 이용자의 개인정보가 원래 수집한 사업자가 아닌 제3자에게 제공될 경우 해당 이용자(고객)의 권익 침해가능성이 매우 높아지므로, 관련 법률에서는 개인정보가 제3자에게 제공되는 경우에 대해 이용자 본인의 동의를 받도록 하는 등 엄격한 규제를 두고 있다.

● 따라서, 사업자가 개인정보를 제3자에게 제공할 때에는 이용자가 개인정보 제공에 대한 사실을 명확히 인지하도록 하고, 개인정보 제공 여부를 이용자 스스로 선택할 수 있도록 조치하여야 한다.

토 막 상 식

"제3자"란 구체적으로 누구를 말하나

"제3자"란 이용자의 개인정보를 수집 보유하고 있는 사업자와, 그 사업자로부터 개인정보 취급을 위탁받은 사업자(수탁자), 그 사업자로부터 영업을 양수한 자(영업양수자)를 제외한 모든 자를 의미한다.

개인정보 제3자 제공에 대한 동의 획득(예시)

□ **개인정보 제3자 제공**

당사가 제공하는 포인트 서비스 및 이벤트 정보안내를 위해 아래와 같이 개인정보를 제3자에게 제공하고 있습니다.

○ 개인정보를 제공받는 자 : △△신용카드사 (제휴카드 발급자에 한함)
○ 이용목적 : 포인트 거래에 필요한 본인확인, 포인트 거래대금 정산, 포인트 이용관련 고객문의 및 고충해결, 포인트 관련 제휴행사 및 서비스 홍보
○ 제공하는 개인정보 항목 : 성명, 주민등록번호, 이메일, 제휴카드번호, 거래정보, 주소, 전화번호
○ 보유 및 이용기간 : 제휴카드 회원 탈퇴시까지, 다만, 잔여포인트가 있는 경우에는 해당 포인트 정산시까지

동의함 □ 동의안함□

□ "제공"의 의미

● 개인정보를 "제공"한다는 것의 사전적 의미는 개인정보를 제3자에게 건네는 행위를 말한다. 그러나 법률상의 개인정보 "제공"이란 이용자의 개인정보를 저장매체(디스크, 테이프, USB, 플래시메모리 등)에 담아 직접 건네는 행위, 네트워크를 통해 제공하는 행위, 개인정보 DB를 제3자가 열람 · 복사할 수 있도록 접근권한을 부여하는 행위, 개인정보 DB시스템을 제3자와 공유하여 사용하는 행위 등이 모두 포함됨을 주의하여야 한다.

● 사업자가 이용자의 동의를 얻지 않고 개인정보를 제3자에게 제공한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

관련 위반사례

- ○○서점은 제휴업체와 개인정보를 제공 · 공유하면서 이를 알리고 동의를 받지 않고, 영업의 특성상 제휴업체가 빈번히 변경된다는 이유로 회원가입신청서 상에 "개인정보를 제공받는 자(제휴업체명) 및 개인정보의 제공 목적"을 고지하지 않고 개인정보를 여러 제휴업체에 제공

- ○○마트는 "개장 기념 경품이벤트"를 실시하면서, 경품행사에 응모한 고객의 정보가 제휴 생명보험사에 제공되어 「휴일 무료 상해보험」에 가입된다는 사실을 고지하지 않고 동의를 얻지 않음

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자가 이용자의 개인정보를 제3자에게 제공하려는 경우 아래 사항을 이용자에게 알리고 동의 획득 ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 (정보통신망법 제24조의2)	○ 개인정보처리자는 정보주체의 동의를 받은 경우 등에 개인정보를 제3자에게 제공 가능(동의를 받을 때는 아래 사항 고지) ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용목적 ③ 제공하는 개인정보 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법 제17조)

2. 이런 경우도 제3자 제공인가

Q | 같은 그룹 내의 호텔, 여행, 쇼핑몰 사이트 등 회원정보 DB를 통합하고 1개의 ID로 로그인이 가능하게 하는 이른바 '패밀리 사이트' 제도를 도입하려 한다. 같은 그룹 내부의 계열사이기 때문에 고객들의 별도 동의는 필요 없을 것 같은데, 그대로 진행해도 괜찮은지 알고 싶다.

A | 제3자는 이용자(고객)로부터 동의를 받고 개인정보를 수집한 해당 사업자를 제외한 모든 법인, 단체 등을 의미하므로, 같은 그룹 내부의 계열사라 하더라도 개인정보의 수집 · 이용목적이 다른 별도의 법인에 해당한다면 제3자에 해당한다.

따라서 그룹 계열사 간이라도 패밀리 사이트라는 명목으로 개인정보를 제공 · 공유하기 위해서는 제3자 제공에 따른 사항을 알리고 동의를 얻어야 한다.

좀 더 알아 봅시다

□ 패밀리 사이트의 개인정보 제공 · 공유

● 개인정보가 제3자에게 제공되는 경우에는 "제공받는 자, 제공받는 자의 이용목적"을 알리고 이용자의 동의를 얻어야 한다. 즉, 최초에 개인정보를 수집한 자가 아닌 다른 자에게 개인정보가 이전되고, 그 제3자가 개인정보를 이용하는 목적이 최초에 개인정보를 수집한 자와 다른 경우에는 법률이 규정하는 "개인정보의 제3자 제공"에 해당된다.

● 최근에 이른바 '패밀리 사이트' 등의 명목으로 기존의 홈페이지를 통합 · 구축하는 경우가 있다. 이 때에는 단지 '계열사' 또는 '같은 그룹"이라는 명목만으로 개인정보 제공 · 공유가 무조건 허용되지는 않는다. 해당 계열사가 이용자(고객)

로부터 동의를 받고 개인정보를 수집한 사업자와 별도의 법인이고, 원래의 개인정보의 수집 · 이용목적이 다르면 제3자 제공에 해당하므로 이에 대해 동의를 얻어야 한다.

● 만약 처음에 홈페이지를 구축할 때부터 계열사 간의 패밀리 사이트를 구축하는 경우에는 '개인정보의 수집 · 이용목적' 등에 패밀리 사이트에 관련된 내용을 명확히 고지하여야 하며, 각각의 사이트를 이용자가 선택하여 가입할 수 있도록 조치하여야 한다.

● 사업자가 이용자의 동의를 얻지 않고 개인정보를 제3자에게 제공한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

● ○○쇼핑몰은 자사의 여행, 도서 등 계열사간 서비스를 패밀리 사이트로 통합하면서, 기존 계열사 회원들의 개인정보를 제3자 제공에 대한 동의 없이 신설된 패밀리 사이트에 일괄 회원가입시킴

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자가 이용자의 개인정보를 제3자에게 제공하려는 경우 아래 사항을 이용자에게 알리고 동의 획득 ① 개인정보를 제공받는 자 ②개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 (정보통신망법 제24조의2)	○ 개인정보처리자는 정보주체의 동의를 받은 경우 등에 개인정보를 제3자에게 제공 가능(동의를 받을 때는 아래 사항 고지) ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용목적 ③ 제공하는 개인정보 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법 제17조) ※ 현행 법률의 취지와 동일함

3. 수사기관이 개인정보를 요구할 때는

Q | 경찰서로부터 수사를 위하여 회원의 개인정보를 제출하여 달라는 협조 문서를 받았다. 본인의 동의 없이 회원정보를 수사기관에 제공하여도 되는지 궁금하다.

A | 사업자가 이용자의 개인정보를 제3자에게 제공하기 위해서는 원칙적으로 이용자의 동의를 얻어야 하나, 법률에 특별한 규정이 있는 경우에는 동의 없이 개인정보를 제공할 수 있다.

형사소송법, 통신비밀보호법, 전기통신사업법 등은 검찰 · 경찰 등 수사기관에서 수사목적을 위해 정당한 절차를 거쳐 요구하는 경우 관련 자료를 제출할 수 있도록 규정하고 있으므로, 이용자 본인의 동의 없이 개인정보 제공이 허용된다.

그러나 범죄수사를 위해 관련 법률에 따라 개인정보를 제공하는 경우에도 수사에 필요한 최소한의 범위 개인정보를 제공해야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제24의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. (이하 생략)

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

1. (생략)
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

형사소송법

제199조 (수사와 필요한 조사) ① 수사에 관하여는 그 목적을 달성하기 위하여 필요한 조사를 할 수 있다. 다만, 강제처분은 이 법률에 특별한 규정이 있는 경우에 한하며, 필요한 최소한도의 범위 안에서만 하여야 한다.

②수사에 관하여는 공무소 기타 공사단체에 조회하여 필요한 사항의 보고를 요구할 수 있다.

좀 더 알아 봅시다

- 이용자의 동의 없이 개인정보를 제3자에게 제공하는 것은 원칙적으로 금지하고 있다. 다만, "다른 법률에 특별한 규정이 있는 경우"에는 동의 없이도 제공할 수 있다. 이는 공익을 달성하기 위한 목적으로 법률에 근거가 있는 개인정보 제공은 이용자의 개인정보 자기결정권보다 우위에 있다고 인정하고 있는 것이다.

- 예를 들어, 형사소송법 제199조는 수사기관이 수사 목적으로 필요한 조사를 할 수 있고, 공무소 · 공사단체에 조회하여 필요한 사항을 요구할 수 있도록 규정하고 있다. 따라서 수사기관이 정당한 수사목적을 위해 개인정보 제출을 요구하였다면 그 상대방은 특별한 사정이 없는 한 관련 자료를 제출하여야 한다. 다만 회원 DB 전체의 제출을 요구하는 등 과도한 개인정보 요구에 대해서는 그 제출이유 및 근거 등을 수사기관에 확인하여야 한다.

- 통신비밀보호법 및 전기통신사업법에서는 검사, 사법경찰관 등 수사기관에서 수사목적을 위해 '전기통신사업자'에게 자료 제출을 요구하는 경우에 대해 상세한 요건 및 절차를 두고 있다.

통신비밀보호법 및 전기통신사업법에 따른 개인정보 제공

	통신비밀보호법	전기통신사업법
요청기관	검사, 사법경찰관	법원, 검사, 수사관서 장
요청대상	전기통신사업자	전기통신사업자
요청자료	통신사실 확인자료 (가입자의 전기통신 일시, 개시 · 종료시간, 발 · 착신 통신번호, 사용도수, 접속로그, 위치추적 자료)	이용자 개인정보 (성명, 주민등록번호, 주소, 전화번호, 아이디, 가입일 · 해지일)
요청절차	관할 지방법원 허가(서면)	서면(자료제공 요청서)

관련 Q&A

Q | 온라인게임사인데, 이용자가 해킹피해를 경찰에게 신고하기 위해 자신의 접속로그 기록을 제공해줄 것을 요청하였다. 통신비밀보호법에 따르면 수사기관만 접속 로그기록 등의 통신사실 확인자료를 제공할 수 있도록 규정하고 있는데 그렇다면 이용자 본인에게도 제공하면 안되는 것 아닌가?

A | 통신비밀보호법은 "누구든지" 동 법의 규정에 의하지 아니하고는 통신사실 확인자료를 제공할 수 없도록 규정하고 있다. 따라서, 이용자 본인이 통신사실확인자료 제공을 요구하는 경우에도 통신비밀보호법에 따른 제공근거가 없으므로 제공해서는 아니된다는 견해가 있었다.

그러나 통신비밀보호법은 수사기관에 대한 개인정보 제공의 요건과 절차를 규정한 법률이며, 이용자는 자신의 개인정보에 대한 열람을 요구할 수 있으므로, 통신비밀보호법에 따른 통신사실 확인자료 제공 제한은 이용자 본인에게는 적용되지 않는다. 즉, 이용자는 자신의 접속로그 기록 등을 사업자에게 요구하여 제공받을 수 있다.

4. 제3자 제공과 개인정보 취급위탁 구분하기

Q | 개인정보 관련 법률에서는 개인정보를 제3자에게 '제공'하는 경우와, 개인정보를 제3자에게 '취급위탁'하는 경우를 따로 규정하고 있는데, 구체적인 차이를 알고 싶다.

A | 법률은 '제3자에 대한 제공' 및 '제3자에 대한 취급위탁'을 각각 별도로 규정하고 있다.

개인정보 제3자 제공이란 "개인정보를 제공받는 자(제3자)의 목적"을 위해 개인정보를 제3자에게 제공하는 것을 말한다.

반면, 개인정보 취급위탁이란 "사업자의 목적"을 위해 개인정보의 수집 · 처리 · 이용 등의 업무를 제3자에게 위탁하는 것을 말한다.

이에 따라서, 개인정보를 제3자에게 '제공'하는 경우에는 '제공받는 자의 이용목적'을 알리고 동의를 받아야 한다. 한편 개인정보의 취급업무를 제3자에게 '위탁'하는 경우에는 '취급위탁을 하는 업무의 내용'을 알리고 동의를 받도록 하고 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제24조의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

제25조(개인정보의 취급위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"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 취급위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 취급위탁을 하는 업무의 내용

좀 더 알아 봅시다

● 개인정보 취급이 제3자와 연관되는 경우는

1) 기업 간의 제휴, 공동마케팅, 공동이벤트 등을 위해 개인정보를 이전하는 경우(제3자 제공)

2) 업무효율화나 비용절감 등을 위해서 내부 업무를 자체적으로 처리하지 않고 외부 업체나 대리점 · 위탁점 등에 아웃소싱하기 위해 개인정보 취급업무를 위탁하는 경우(취급위탁)

로 나누어 볼 수 있다.

● 개인정보의 제3자 제공 및 취급위탁은 이용자의 개인정보를 제3자가 관리하는 형태는 동일하지만, 개인정보의 처리목적이나 관리범위 등이 다르므로 법률에서는 양자를 구분하여 규정하고 있다.

– **(제3자 제공)** 개인정보를 제공받는 자(제3자)의 목적을 위해 개인정보가 제공되는 경우를 말한다. 사업자가 업무제휴나 공동마케팅 등을 위해서 외부 업체에 개인정보를 제공하는 경우가 이에 해당한다. 이용자(고객)는 자신의 개인정보가 제3자에게 제공

되는지 사전에 알기 어려우므로, 정보주체(고객)의 의사에 반해 개인정보가 제공되는 일이 없도록 엄격한 규제가 필요하다.

– (**취급위탁**) 사업자의 목적을 위해 개인정보의 취급업무를 제3자에게 위탁하는 경우를 말한다. 사업자가 내부 업무를 대리점, 위탁점과 같은 외부 위탁업체(아웃소싱 업체)를 통해 처리하는 경우가 이에 해당한다. 취급위탁은 사업자와 수직적 업무관계에 있는 대리점, 위탁점 등에서 개인정보가 처리되는 것으로서, 사실상 사업자의 내부에서 개인정보가 처리되는 것과 유사하다.

제3자 제공 및 취급위탁의 구분

구분	제3자 제공	취급위탁
처리목적	**개인정보를 제공받는 자**의 이익 · 목적을 위해 개인정보를 제3자에게 제공	**사업자**의 이익 · 목적을 위해 개인정보 취급업무를 제3자에게 위탁
관리범위	개인정보를 **제공받는 자(제3자)**의 관리범위에 속함	취급위탁을 받은 자(수탁자)가 개인정보를 운영하지만, **사업자**의 관리범위에 속함
예 시	백화점(제공하는 자)이 신용카드사(제공받는 자)와 업무제휴를 맺고, 백화점 고객 개인정보를 신용카드사에 제공 → 신용카드사는 자사의 제휴카드 발급 마케팅에 백화점 고객정보를 이용	백화점(사업자)이 콜센터 업체(수탁자)와 위탁계약을 맺고, 백화점 고객 개인정보를 콜센터 업체에서 관리 · 운영 → 콜센터 업체는 백화점의 고객상담 업무에 백화점 고객정보를 이용

업무위탁의 종류 (예시)

구분	유형	제3자 제공
내부업무 위탁	기본업무 위탁	○ 급여, 인사관리 업무, 직원채용 업무, 청소관리, 주차관리 업무 등의 위탁
	전산관리 위탁	○ 전산시스템(웹, DB 등)의 개발 · 관리 업무, 시스템 보안관리 업무 등의 위탁
영업업무 위탁	계약체결 위탁	○ 아웃바운드(비고객) 텔레마케팅, 방문판매 등 재화 · 용역의 판매 권유 업무위탁 (예) 대리점을 통한 통신서비스 가입, 전화 텔레마케팅 광고
	계약이행 위탁	○ 상품 배송 · 설치 업무, 상담 업무, 고객 불만처리 업무, 채권추심 업무 등의 위탁

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보를 취급위탁하는 경우 아래 사항을 고지하고 동의를 획득 ① 개인정보 취급위탁을 받는 자 ② 개인정보 취급위탁을 하는 업무의 내용을 알리고 동의 받아야 함 ○ 다만 계약의 이행을 위하여 필요한 경우 개인정보 취급방침에 공개하거나 통지로 갈음할 수 있음 (정보통신망법 제25조)	○ 개인정보를 취급위탁하는 경우 아래 사항을 공개하면 취급위탁 허용 ① 위탁하는 업무의 내용 ② 수탁자 ※ 현행 법률상의 동의획득 규정을 삭제함으로써 취급위탁 요건 완화 (개인정보 보호법 제26조)

5. 개인정보 업무를 외주업체에 위탁할 때 주의사항

Q | 여행사를 운영하면서 예약확인 및 고객 상담업무를 전문 콜센터에서 처리하고 있는데, 자사에서 진행하는 고객 대상 이벤트와 여행상품 홍보 업무도 해당 콜센터에서 모두 진행하려고 한다. 관련 법률상 문제는 없는지 알고 싶다.

A | 사업자가 제3자에게 개인정보의 수집, 보관 등 취급업무를 위탁하는 경우에는 취급위탁을 받는 자(수탁자) 및 취급위탁을 하는 업무의 내용을 고지하고 이용자의 동의를 받아야 한다.

다만, 서비스 제공계약의 이행을 위해 필요한 경우에는 위의 고지 · 동의절차를 거치지 않고, 취급위탁을 받는 자 및 취급위탁을 받는 업무의 내용을 개인정보 취급방침에 공개하거나 이용자에게 통지하여, 이를 대신할 수 있다.

질의와 같이 본래의 서비스 이행을 위한 취급위탁 업무가 아닌 별도의 이벤트, 홍보 등의 업무를 위탁하기 위해서는 이용자의 별도 동의를 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제25조(개인정보의 취급위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"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 취급위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 취급위탁을 하는 업무의 내용

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

좀 더 알아 봅시다

□ 개인정보 취급위탁 규제의 취지

● 최근 사업자의 업무 효율화, 비용 절감 등 다양한 목적으로 각종 업무를 외부에 위탁하는 사례가 증가하고 있다. 즉, 기본적인 고객상담, A/S 업무 이외에도 상품 배송, 마케팅, 전산 관리, 근로자 급여 및 인사관리 등 다양한 형태의 업무 위탁이 일반화되는 추세이다.

● 대부분의 업무위탁은 개인정보를 수집한 사업자가 제3자에게 개인정보를 이전하여 처리하므로, 해당 이용자의 권익 침해가능성이 높아진다. 따라서 개인정보 취급업무를 제3자에게 위탁하는 경우도 원칙적으로 이용자 본인의 동의를 받도록 하고 있다.

□ 개인정보 취급위탁시 고지사항 및 동의 획득

● 개인정보 취급위탁시에는 아래의 사항을 이용자에게 알리고 동의를 획득하여야 한다.

① 취급위탁을 받는 자(수탁자)

② 취급 위탁을 하는 업무의 내용

개인정보 취급위탁 동의획득 예시

□ 개인정보 취급위탁

당사의 서비스 이행을 위해 아래와 같이 개인정보 취급업무를 위탁합니다.

취급위탁을 받는 자	취급위탁을 하는 업무의 내용
○○ 텔레마케팅	△△제휴상품 및 서비스에 대한 홍보 및 안내

동의함 □ 동의안함□

● 사업자의 종류나 규모에 따라서는 전국단위 영업을 하는 여행사 · 항공사 대리점, 백화점 · 쇼핑센터의 콜센터 등과 같이 '취급위탁을 받는 자'가 매우 많기 때문에, 이를 일일이 열거하고 동의를 받기 어려운 경우가 있다.

이 경우에는 대표적인 업체명, 업체수 등을 기재하고 상세한 내역은 개인정보 취급방침에 게재하여 이용자가 확인할 수 있도록 조치할 수 있다. 물론 이 경우에도 고지사항이 게재된 인터넷페이지 주소 등을 동의문에 안내하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제12조(동의획득방법) ① (생략)

② 정보통신서비스 제공자 등은 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소 · 사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.

● 사업자가 이용자의 동의를 얻지 않고 개인정보 취급을 제3자에게 위탁한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금이 부과된다.

● ○○쇼핑센터는 고객정보를 이용한 제휴상품 홍보 텔레마케팅을 외주업체에 위탁하면서 고객에 대해 고지 및 동의를 얻었어야 하나, 이러한 절차 없이 단순히 개인정보 취급방침에 고지한 뒤 텔레마케팅 업무를 취급위탁함

6. 개인정보 취급위탁시에는 언제나 동의를 받아야 하나

Q | 요금고지서를 우편 DM으로 발송하는 업무를 외부 업체에 위탁하려 하는 경우에 고객이 우편 DM 발송의 위탁에 대해 동의하지 않는다면, 본사에서 일일이 직접 배송을 해야 하는가?

A | **요금고지서 DM 발송, 상담, A/S 등 "서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 취급위탁"은 이용자의 동의 없이도 가능하다.**

이 경우 사업자는 위탁업무의 내용 및 수탁자를 개인정보 취급방침에 공개하거나 이용자에 대해 통지하여야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제25조(개인정보의 취급위탁) ① (생략)
>
> ② 정보통신서비스 제공자 등은 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

좀 더 알아 봅시다

- "서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 취급위탁"이란 만일 해당 업무를 위탁하지 않으면 이용자에게 정상적인 서비스를 제공하기 어려운 경우로서, 일반적으로 고객 상담, A/S 업무, 제품 배송 등이 이에 포함된다.

- 이러한 필수적인 업무위탁에 대해서도 이용자의 동의 유무에 따라 위탁의 허용 여부를 결정하게 한다면, 만일 이용자가 위탁에 동의하지 않은 경우에는 본사

에서 모든 업무를 직접 처리해야 하는 불합리한 결과가 나타나게 된다. 따라서 "서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 취급위탁"에 대해서는 동의를 받지 않아도 취급위탁이 가능하도록 규정하고 있다.

□ 서비스 제공에 필요한 개인정보 취급위탁시 공개 · 통지 사항

● "서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 취급위탁" 시에는 아래의 사항을 개인정보 취급방침에 공개하거나 이용자에게 통지하여야 한다.

① 취급위탁을 받는 자 (수탁자)

② 취급위탁을 하는 업무의 내용

서비스 제공에 필요한 개인정보취급 업무위탁 예시

- ○ 전화, 온라인 등을 이용한 고객 상담업무
- ○ 요금고지서 및 DM 발송
- ○ 제품의 배송
- ○ 제품의 A/S 및 반품 등 불만처리
- ○ 연체요금 정산을 위한 채권추심업무 위탁 등

관련 Q&A

Q | 서비스 제공에 필수적인 개인정보 취급위탁은 따로 동의를 받지 않아도 되는 대신 관련 사항을 공개하여야 하는데, 구체적 공개 방법은?

A | 서비스 제공에 관한 계약 이행을 위해 필요한 취급위탁은 아래 2가지 방법 중 택일하여 이용자에게 공개하거나 알리면 된다.

① 취급위탁을 받는 자 및 취급위탁을 하는 업무의 내용을 개인정보 취급방침에 명시하고, 인터넷 홈페이지 게재, 점포 · 사무소 게재 · 비치, 간행물 · 소식지 · 홍보지 · 청구서 등에 지속 게재 등의 방법으로 공개

② 취급위탁을 받는 자 및 취급위탁을 하는 업무의 내용을 전자우편 · 서면 · 모사전송 · 전화 또는 이와 유사한 방법에 따라 이용자에게 알림

관련 Q&A

Q | 병원과 의료정보 전달시스템 관리업체 간에 환자의 정보를 공유하는 것도 취급위탁에 따른 동의를 받아야 하는가?

A | 의료법 등에 따른 전자처방전, 전자의무기록 등의 공유 · 제공을 위해 관리업체를 활용하는 것은 "서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 취급위탁"에 해당하므로 별도의 동의획득 없이 이용자에 대한 공개 · 통지만으로 위탁이 가능하다.

관련 위반사례

- ○○투어는 고객에 대해 전화를 통한 여행 계약 체결 안내와 같은 필수 업무를 외주업체에 위탁하고 있으나, 이러한 업무위탁에 대해 개인정보취급방침에 공개하거나 고객에게 통지하지 않고 취급위탁을 계속함

7. 개인정보 취급위탁 계약을 체결할 때의 주의사항은

Q | 고객센터 업무를 아웃소싱하려고 한다. 아웃소싱 업체와 개인정보 취급위탁 계약을 체결할 때에 계약서에 반드시 포함시켜야 하는 사항은 무엇이 있는가?

A | 수탁자(아웃소싱 업체)와 취급위탁 계약을 체결할 때에는 계약서에 수탁자명, 수탁업무명, 개인정보취급기간(계약기간), 수탁자의 개인정보 취급목적, 위탁자의 관리 · 감독 사항, 보호조치, 수탁자의 책임 등을 명시하는 것이 바람직하다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제25조(개인정보의 취급위탁) ①~② (생략)

③ 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리 · 감독하여야 한다.

⑤ 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다.

좀 더 알아 봅시다

- 제3자 제공에 비해 취급위탁의 허용요건을 완화하는 이유는 취급위탁을 위해 제공한 개인정보가 위탁자의 관리범위 안에 포함되어 있어 개인정보 취급위탁시에는 위탁자가 해당 개인정보에 대한 철저한 관리 · 감독을 하여야 함을 의미한다.

● 이를 위해서는 위탁자와 수탁자가 취급위탁 계약을 체결할 때부터 계약서에 관련 사항을 명확히 반영하고, 개인정보 침해방지를 위한 보호 조치가 수탁업체에 확보되도록 정함과 동시에 위탁자와 수탁자와의 책임관계를 명확하게 규정함으로써 실효적인 관리 · 감독 체계를 확보하여야 한다.

● 따라서, 사업자가 수탁자와 위탁계약을 체결하는 때에는 다음의 사항을 포함하여 계약서를 작성하는 것이 바람직하다.

취급위탁 계약서 반영 사항(예시)

- 수탁자명 (정확한 법인명)
- 수탁업무명 (구체적 업무 명시)
- 계약기간 (개인정보 취급기간)
- 수탁자의 개인정보 취급목적
- 위탁자의 관리 · 감독 사항
- 수탁자의 기술적 · 관리적 보호조치
- 침해사고 발생시 수탁자의 책임
- 개인정보 침해로 인한 손해배상 책임
- 계약종료 시 개인정보 반환 또는 파기에 관한 사항 등

관련 위반사례

● ○○여행사는 여행지 현지에서의 고객서비스를 위해 이른바 지역 여행사와 업무위탁계약을 체결하였으나, 개인정보 수탁업무에 대한 내용 및 기술적 · 관리적 보호조치 등 관한 사항을 위탁계약서에 전혀 반영하지 않고 업무 위탁계약을 체결하여 운영

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 계약서(문서)에 포함되어야 하는 사항에 대해서는 별도 규정 없음	○ 개인정보 처리자가 개인정보 처리 업무를 위탁하는 경우 다음 내용이 포함된 문서로 처리하여야 함 1. 위탁업무 수행 목적 외 개인정보 처리 금지 2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항 3. 기타 개인정보의 안전한 관리를 위하여 대통령령으로 정하는 사항 (개인정보보호법 제26조제1항)

8. 대리점의 개인정보 유출방지를 위한 노력

Q | 대리점 직원이 고객의 개인정보를 부정 이용하여 고객에게 피해를 입힌 사례가 발생한 경우, 대리점 직원의 행위에 대하여 본사에 책임이 있는가?

A | 위탁자(본사)는 수탁자(대리점)에 대해 법률의 개인정보보호 규정을 준수하도록 관리 · 감독할 의무가 있으며, **수탁자가 법령을 위반하여 이용자에게 손해를 발생시킨 경우에는 위탁자가 이에 대한 책임을 지도록 하고 있다.**

따라서 사례와 같은 대리점 직원의 행위에 대해서는 본사가 손해배상 책임을 부담한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제25조(개인정보의 취급위탁) ①~② (생략)

③ 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리 · 감독하여야 한다.

⑤ 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자 등의 소속 직원으로 본다.

좀 더 알아 봅시다

● 일반적으로 위탁(위임) 계약에 있어서 그 행위로 인한 법률효과는 수탁자가 아니라

위탁자(본사)에 귀속된다. 또한 개인정보 취급과 관련한 위탁에 있어서 위탁자의 관리 · 감독 책임에 대해 별도의 규정이 없다면, 대부분의 위탁자는 개인정보 침해로 인한 책임을 상대적 약자인 수탁자에게 전가하게 될 우려가 있다. 이러한 취지에서 관련 법률은 위탁자의 관리 · 감독 책임과 더불어 특히 손해배상은 위탁자가 책임지도록 규정하고 있다.

● 본사와 대리점이 취급위탁계약을 체결하고자 하는 때에는 대리점의 개인정보 유출 방지를 비롯한 개인정보 보호 조치 의무를 명문화하여야 한다. 또한, 본사와 대리점과의 책임관계를 명확하게 하고, 재위탁에 관한 사항도 계약 내용에 포함토록하여 실효성 있는 관리 · 감독 체계를 마련하여야 한다.

관련 Q&A

Q | T/M업무를 위탁 중에 이용자가 T/M 거부의사를 밝혔음에도 불구하고 이후에도 수탁업체에서 계속 T/M을 실시하여 문제가 되었다면 이는 본사의 책임이 아니지 않는가?

A | 위탁자에게는 개인정보 취급위탁에 대한 관리 · 감독 책임 및 민사상 손해배상 책임이 부여되어 있으므로, T/M 거부에 대한 조치 등을 관리 · 감독하지 못한 책임이 부과된다.

관련 위반사례

● 수탁업체 직원이 아파트 MDF실에서 경쟁관계에 있는 통신업체의 고객 개인정보를 빼낸 행위에 대해, 본사의 담당 직원도 관리책임 미비를 이유로 수사기관에 입건

9. 동의 받는 방법 총 정리

Q | 여행사에서는 주로 전화로 문의 · 예약을 받는 경우가 많다. 그런데 전화로 개인정보를 수집할 경우, 고지사항을 모두 알리고 동의를 받으려면 통화시간이 매우 길어진다. 이용자의 동의획득을 위한 다른 방법은 없는가?

A | **법률은 인터넷 사이트, 서면, 전자우편, 전화 등 각각의 서비스 유형에 따른 동의 획득 방법을 규정하고 있다.**

전화로 개인정보 수집에 대한 동의를 얻고자 하는 경우에는, 동의 내용을 이용자에게 알리고 구두로 동의를 얻거나, 또는 고지사항이 기재된 인터넷 주소 등을 안내하고 추후 구두로 동의를 얻는 방법을 이용할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제26조의2(동의를 받는 방법) 제22조제1항, 제23조제1항 단서, 제24조의2제1항 · 제2항, 제25조제1항, 제26조제3항 단서 또는 제63조제2항에 따른 동의(이하 "개인정보 수집 · 이용 · 제공 등의 동의"라 한다)를 받는 방법은 개인정보의 수집매체, 업종의 특성 및 이용자의 수 등을 고려하여 대통령령으로 정한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제12조(동의획득방법) ① 정보통신서비스제공자등이 법 제26조의2에 따라 동의를 얻는 방법은 다음 각 호의 어느 하나와 같다. 이 경우 정보통신서비스제공자등은 동의를 얻어야 할 사항(이하 "동의 내용"이라 한다)을 이용자가 명확히 인지하고 확인할 수 있도록 표시하여야 한다.

1. 인터넷 사이트에 동의 내용을 게재하고 이용자가 동의 여부를 표시하도록 하는 방법
2. 동의 내용이 기재된 서면을 이용자에게 직접 교부하거나, 우편 또는 모사전송을 통하여 전달하고 이용자가 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
3. 동의 내용이 기재된 전자우편을 발송하여 이용자로부터 동의의 의사표시가 기재된 전자우편 을 전송받는 방법
4. 전화를 통하여 동의 내용을 이용자에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법

② 정보통신서비스제공자등은 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소 · 사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.

좀 더 알아 봅시다

□ 동의를 획득해야 하는 경우

● 개인정보 수집, 제3자 제공, 개인정보 취급 위탁 등에 대해 이용자의 동의를 획득하여야 한다.

동의를 획득해야 하는 경우

정보통신망법 조항	주요내용
제22조 제1항	개인정보를 수집하는 경우(동의를 받은 사항에 대해 변경이 발생한 경우 포함)
제23조제1항	민감한 개인정보를 수집하는 경우
제24조의2 제1항	개인정보를 제3자에게 제공하는 경우
제24조의2 제2항	개인정보를 제공받은 자가 또다른 제3자에게 개인정보 제공하는 경우
제25조 제1항	개인정보를 취급위탁하는 경우
제26조제3항	영업양수자 등이 목적외로 개인정보 이용 · 제공하는 경우

□ 매체별 동의획득 방법

● 개인정보의 수집, 제공, 이용, 위탁 등에 대해 동의를 획득하는 방법은 매체별로 다음과 같다.

매체	동의 받는 방법
인터넷	동의 내용을 기재하고 이용자가 동의 여부를 선택하도록 하는 방법 (동의 항목에 체크하게 하거나, 아이콘을 클릭하는 방식)
서 면	동의 내용이 기재된 서면을 이용자에게 직접 교부하거나, 우편 또는 모사전송(FAX) 등을 통해 이용자에게 전달한 후, 이용자가 서명날인하여 제출하는 방법
전자우편	동의 내용이 기재된 전자우편을 발송한 후 이용자로부터 동의서가 기재된 전자우편을 회신받는 방법
전 화	• 전화를 통해 동의 내용을 이용자에게 알리고 동의를 얻는 방법 • 동의내용이 기재된 인터넷 주소 등 동의내용을 확인할 수 있는 방법을 안내하고 추후 전화통화로 동의를 얻는 방법

□ 동의 내용을 전부 표시하기 어려운 경우의 동의획득 방법

● 사업자는 개인정보 수집 매체의 특성상 동의내용을 전부 표시하기 어려운 경우에는 동의 내용이 기재된 “인터넷 주소”나 동의 내용을 안내받을 수 있는 “전화번호” 등을 안내하고 동의를 얻을 수 있다.

□ 전화를 통한 동의를 얻는 경우에 녹취 여부

● 전화로 동의를 얻는 경우에 다른 매체와는 달리 기본적으로 음성(구두)을 통해 동의 의사표시를 하므로, 나중에 이용자가 동의를 했는지 여부를 어떻게 입증할 것인가의 문제가 나타난다. 이를 위해서는 고지사항을 이용자에게 안내하고 동의의사를 확인하는 대화를 녹취하여 입증자료로 삼아야 한다.

관련 Q&A

Q | PDA단말기를 이용한 서비스 이용계약을 체결하는 경우에 개인정보 수집 · 이용에 대한 동의방법으로 고객이 PDA단말기에 직접 서명하는 것도 가능한가?

A | PDA단말기를 통하여 서명을 하는 방식도 가능하다. 다만, 이 경우 개인정보 수집시의 고지사항을 이용자에게 명확히 고지하고 동의를 얻어야 한다. 고지사항이 많으면 동의내용을 확인할 수 있는 방법(인터넷 주소 등)을 안내하여야 한다.

10. 영업을 양도하거나 합병할 때는

Q | 다른 사업자와 영업을 합병하게 되어서 고객을 대상으로 통지를 하려고 하는데, 우리 회사 및 합병 회사가 모두 다 통지를 해야 하는가?

A | 영업 양도, 합병 등으로 개인정보를 이전하는 경우에는 개인정보를 이전하는 자 및 이전받는 자가 "개인정보 이전 사실, 이전받는 자의 성명(명칭) · 주소 · 전화번호 등 연락처, 이용자가 개인정보 이전을 원하지 않는 경우 동의철회 방법 · 절차"를 이용자에게 알려야 한다.

다만, 개인정보를 이전하는 자(사업자)가 관련 사실을 알린 경우에는 이전받는 자(영업양수자 등)는 알리지 않아도 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제26조 (영업의 양수 등에 따른 개인정보의 이전) ① 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도 · 합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다) · 주소 · 전화번호 및 그 밖의 연락처
3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차

② 영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실을 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다. 다만, 정보통신서비스 제공자등이 제1항에 따라 그 이전사실을 이미 알린 경우에는 그러하지 아니하다.

좀 더 알아 봅시다

● 영업양도 · 합병 등의 경우에는 기존 사업자가 가지고 있던 개인정보 DB 등 영업자산에 대한 권리 · 의무가 포괄적으로 승계되므로, 개인정보의 제3자 제공이나 취급위탁처럼 개인정보 이전에 대한 통제를 엄격하게 할 필요가 없다. 또한 영업양도 · 합병 등에 대해 일일이 정보주체의 동의를 받도록 할 경우에는 현실적으로 많은 시간과 비용을 요하며 결과적으로는 기업결합 자체를 사실상 불가능하게 할 우려도 있다.

● 따라서 영업양도 · 합병 등은 개인정보 이전에 관한 사항을 이용자에게 사전에 알리고, 이에 따라 이용자가 조치를 취함으로써 이전을 가능하도록 하고 있다.

토 막 상 식

"영업양도"와 "합병"

'영업양도'는 영업과 관련한 재산, 영업비결, 고객관계, 경영조직 등 일체를 이전하는 행위(계약)을 말하며, '합병'은 둘 이상의 회사가 계약에 의해서 하나의 회사로 합치는 것을 말한다. 즉, 합병은 당사회사의 일부 또는 전부가 소멸하며, 존속회사 또는 신설회사가 소멸하는 회사의 모든 권리 · 의무를 포괄적으로 승계한다.

● 원칙적으로 영업 양도자 및 양수자는 모두 통지의무가 있으나, 영업양도자가 미리 통지한 경우는 양수자는 통지를 하지 않아도 된다. 이는 관련한 사항을 이미 양도자로부터 통지받아 조치를 취할 수 있음에도 양수자로부터 통지를 받도록 의무화하는 것은 불필요하기 때문이다.

● 영업 양도 · 합병 등으로 개인정보를 이전하는 경우에는 아래의 사항을 이용자에게 알려야 한다.

① 개인정보를 이전하려는 사실

② 개인정보의 이전을 받는 자(영업 양수자 등)의 성명(법인의 경우에는 법인의 명칭) · 주소 · 전화번호 그 밖의 연락처

③ 이용자가 개인정보의 이전을 원하지 않는 경우 그 동의를 철회할 수 있는 방법 및 절차

● 영업의 양도 · 합병에 관한 사실을 통지하는 방법은 인터넷 홈페이지 게시 및 전자우편, 서면, 모사전송, 전화 등을 이용하여 통지하면 된다. 이용자의 연락처를 알 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 영업 양도 · 합병에 관한 사실을 게시해야 한다.

영업 양도 · 합병시 통지문 (예시)

○○는 2011년 1월 1일자로 □□□ 사업 및 홈페이지의 운영을 ×××사에 양도하게 되었습니다. 이로 인해 회원 여러분의 개인정보 또한 ×××사에 이전하게 되었습니다.
□□□ 홈페이지 운영을 양도 받은 ×××사의 세부사항은 다음과 같습니다.
법인명 : ×××사
주 소 : 서울시 강남구 역삼동 xxx ○○번지
전화번호 : 02 123 4567
기타 연락처 : 담당자@xxxxxx.xxx
개인정보의 이전을 원하지 않는 경우 당사 홈페이지(www.xxxxx.xxx)에서 회원탈퇴를 하실 수 있습니다.

● 천재 · 지변, 기타 사유 등으로 홈페이지 게시도 곤란한 경우에는, 전국을 보급지역으로 하는 2개 이상의 일반 일간신문에 관련 사항을 1회 이상 공고하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제11조(영업의 양도 등에 따른 개인정보 이전 시의 통지) ① 법 제26조제1항 각 호 외의 부분 및 제2항 본문에서 "대통령령이 정하는 방법"이란 전자우편 · 서면 · 모사전송 · 전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다.
② 정보통신서비스제공자등 또는 영업양수자등이 과실 없이 이용자의 연락처를 알 수 없는 경우에 해당되어 제1항의 방법에 따라 통지할 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 게시하여야 한다.
③ 천재 · 지변 그 밖에 정당한 사유로 제2항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 자유와 기능보장에 관한 법률」에 따른 전국을 보급지역으로 하는 2 이상의 일반일간신문(이용자의 대부분이 특정지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일반일간신문)에 1회 이상 공고하는 것으로 갈음할 수 있다.

● 사업자가 영업 양도 · 합병 등에 따른 개인정보 이전사실을 알리지 않은 경우에는 2천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 쇼핑몰을 양도하려고 하는데, 관련 법률을 보니 '지체 없이' 통지하라는 내용이 있다. 어느 정도의 시점에서 통지를 해야 하는가?

A | 영업 양도 · 합병 등이 이사회 의결 등을 통해 공식화된 이후에는 즉시 이용자들에게 통지를 하여야 한다. 소규모 사업자의 경우에는 영업양도 계약을 체결하는 등 영업양도가 확실시되는 시점에서 통지하여야 한다.

관련 위반사례

- ○○케이블 방송사는 초고속인터넷 서비스를 운영하다가 이를 A 통신사업자에게 양도하면서 고객들에게 별도의 통지를 전혀 하지 않아, "영업양도 · 합병 시 통지 의무" 위반의 책임을 물어 ○○만원의 손해배상 소송

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우 아래 사항을 이용자에게 통지 1. 개인정보 이전 사실 2. 개인정보를 이전받는 자의 성명, 주소, 전화번호 및 그 밖의 연락처 3. 정보주체가 개인정보의 이전을 원하지 않은 경우 조치 할 수 있는 방법 및 절차 (정보통신망법 제25조)	○ 개인정보처리자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우 아래 사항을 정보주체에게 통지 ※ 현행 법률의 취지와 동일함 (개인정보보호법 제27조)

제 6 장 고객의 개인정보는 철저히 관리하자

1. 개인정보 취급방침, 이것만은 꼭 기억하자
2. 개인정보 취급방침을 알리는 방법
3. 개인정보 취급방침을 변경할 때는
4. 해킹과 불법 접근을 차단하려면
5. 내부직원의 유출을 방지하려면
6. 개인정보 암호화 꼭 해야 하나
7. 보안프로그램은 어떻게 설치 · 이용하면 될까
8. 개인정보에 대한 접근권한은 최소한으로
9. 물리적인 접근제한 조치를 하려면
10. 개인정보를 출력 · 복사할 때는

제6장 고객의 개인정보는 철저히 관리하자

1. 개인정보 취급방침, 이것만은 꼭 기억하자

Q | 사업자는 '개인정보 취급방침'이라는 것을 작성해서 게시해야 한다고 들었는데, 구체적으로 어떠한 내용을 담아야 하는지 알고 싶다.

A | 사업자는 '개인정보 취급방침'을 정하고, 이용자(고객)가 언제든지 쉽게 확인할 수 있도록 공개하여야 한다.

개인정보 취급방침에는 아래의 사항이 반드시 포함되어야 하며, 그 외에도 이용자가 추가적으로 알아야 할 개인정보보호 관련 사항이 있다면 포함하여 공개해야 한다.

① 개인정보의 수집 · 이용 목적, 수집하는 항목, 수집방법
② (개인정보를 제3자에게 제공하는 경우) 제공받는 자의 성명(또는 법인 명칭), 제공 받는 자의 이용 목적, 제공 항목
③ 개인정보의 보유 · 이용기간, 파기절차, 파기방법
(다른 법률에 따라 보존해야 하는 경우에는 보존근거 및 보존 항목)
④ (개인정보 취급위탁을 하는 경우)개인정보 취급위탁을 하는 업무 내용 및 수탁자
⑤ 이용자 및 법정대리인의 권리와 행사방법
⑥ 인터넷 접속파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 거부에 관한 사항
⑦ 개인정보 관리책임자의 성명(또는 개인정보보호 업무 및 관련고충을 처리하는 부서의 명칭), 전화번호 등 연락처

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조의2(개인정보 취급방침의 공개) ① (생략)
② 제1항에 따른 개인정보 취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다.
1. 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목 및 수집방법

2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기 절차 및 파기방법(제29조 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존 근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 취급방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

좀 더 알아 봅시다

□ 개인정보 취급방침의 공개 의무화

● 사업자의 개인정보 처리기준과 보호조치 등을 외부에 공개하도록 의무화함으로써, 이용자(고객)는 그 사업자가 어떻게 개인정보를 처리하고 보호하는지를 쉽게 확인할 수 있으며, 자기 개인정보의 수집·이용·제공 여부를 판단할 수 있다. 또한, 사업자는 대외적으로 개인정보 처리의 투명성을 높이고 부족한 부분을 개선할 수 있도록 함으로써 자율적인 개인정보보호 노력을 장려할 수 있다.

'개인정보 취급방침 공개'와 관련된 항목

제6장 고객의 개인정보는 철저히 관리하자

→ 2. 개인정보 취급방침을 알리는 방법 (101페이지)

토 막 상 식

외국에도 개인정보 취급방침이 있을까?

미국, 일본, 유럽 등 대부분의 주요 국가에서도 우리나라와 마찬가지로 인터넷 웹사이트 등에서 개인정보 취급방침을 게시하는 것이 일반적이다. 외국에서는 주로 'Privacy Policy'라는 명칭으로 취급방침을 공개하고 있는데, 여기에 기재되는 내용은 개인정보의 수집 · 이용에 관한 사항, 개인정보의 제공 · 공유에 관한 사항, 관리책임부서의 연락처 등이다.

□ 개인정보 취급방침 작성시 유의점

● 개인정보 취급방침에 포함되는 사항은 그 사업자의 서비스 현황을 반영하여 최대한 구체적이고 정확하게 표현하여야 한다. 예를 들어 「개인정보의 수집 · 이용 목적」을 단순히 "서비스 제공", "다양한 콘텐츠 제공" 등과 같이 추상적이고 모호한 표현으로 기재하는 것은 바람직 하지 않다.

● 또한, 개인정보 취급방침에 명시된 사항들은 그 사업자가 이용자(고객)에게 동의를 받기 위해 알리는 사항들과 일치하여야 한다. 예를 들어 개인정보 취급방침에 기재된 「개인정보의 수집 · 이용 목적」은 회원가입시 이용자에게 알리고 동의를 받는 「개인정보의 수집 · 이용 목적」과 일치하여야 한다.

'개인정보 수집 · 이용 목적'과 관련된 항목

제4장 개인정보를 수집하고 이용하려면

→1. 회원가입 · 이벤트 시 고객의 동의를 받자 (38페이지)

● 또한, 개인정보 취급방침은 단순히 인터넷 웹사이트에서의 개인정보 처리현황만을 다루는 것이 아니라, 그 사업자가 서비스를 제공하는 모든 영역에 있어서의 개인정보 처리기준을 명시 · 공개하는 것임을 유의하여야 한다. 즉, 인터넷 웹사이트 외에 전화 · 서면 등을 통해서도 회원 가입을 받고 있다면, 개인정보 취급방침에도 '전화 · 서면을 통한 개인정보 수집과 관련한 사항'이 모두 명시되어 있어야 한다.

- 사업자가 개인정보 취급방침을 공개하지 아니한 경우에는 2천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 신입직원 채용을 위해 온라인 입사지원 사이트를 개설하였는데, 이때에도 '개인정보 취급방침'을 작성·공개하여야 하는가?

A | 현행 정보통신망법은 영리를 목적으로 개인정보를 수집·이용하는 사업자와 이용자(고객)와의 관계에 대해서 적용된다. 따라서 '신입직원 채용을 위한 웹사이트'는 법률의 적용대상이 아니므로, 온라인 입사지원 사이트의 개인정보 취급방침을 공개해야 할 법적인 의무는 없다. 그러나 해당 기업의 자체적인 판단에 따라 개인정보 취급방침을 작성·공개하는 것은 무방하다.

관련 위반사례

- ○○백화점은 홈페이지에 개인정보 취급방침을 게재하고는 있으나, 개인정보 취급 위탁사항, 개인정보 관리책임자 지정 등 개인정보 취급방침에 반드시 포함시켜야 하는 사항을 일부 누락하여 게재

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ '개인정보 취급방침' 작성 및 공개 (정보통신망법 제27조의2) 1. 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목 및 수집방법 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭), 제공 받는 자의 이용 목적과 제공하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기 절차 및 파기방법 (개인 정보를 보존하여야 하는 경우에는 그 보존근거와 보존 항목) 4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 포함) 5. 이용자 및 법정대리인의 권리와 그 행사방법 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항 7. 개인정보 관리책임자의 성명(또는 관련 부서 명칭)과 그 전화번호 등 연락처	○ '개인정보 처리방침' 수립 및 공개 (개인정보보호법 제30조) 1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유기간 3. 개인정보의 제3자제공에 관한 사항(해당되는 경우에만 정한다) 4. 개인정보의 처리 위탁에 관한 사항(해당되는 경우에만 정한다.) 5. 정보주체의 권리 · 의무 및 그 행사 방법에 관한 사항 6. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한사항 ※ 현행 법률의 취지와 동일하며, 다만 '개인정보 취급방침' → '개인정보 처리방침'으로 명칭이 변경됨

2. 개인정보 취급방침을 알리는 방법

Q | 우리 회사는 인터넷 홈페이지가 있지만, 고객 가입과 서비스 제공은 점포나 대리점을 통해서 이루어지고 있다. 이런 경우 홈페이지에 개인정보 취급방침을 공개하지 않아도 되는가?

A | 사업자가 개인정보 취급방침을 공개할 때에는 개인정보의 수집장소와 매체 등을 고려하여 다음 중 하나 이상의 방법으로 공개하여야 한다.

① 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 이용자가 볼 수 있도록 하는 방법
(글자 크기, 색상 등을 활용하여 개인정보 취급방침을 쉽게 확인할 수 있도록 표시해야 함)
② 점포 · 사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하여 열람하도록 하는 방법
③ 같은 제목으로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물 · 소식지 · 홍보지 · 청구서 등에 지속적으로 게재하는 방법
④ 재화 또는 용역을 제공하기 위한 계약서에 게재하여 배포하는 방법

질의와 같이 점포 및 대리점을 통해서만 고객 가입과 개인정보를 수집하는 경우에도, 위 항목 중 하나 이상의 방법으로 개인정보 취급방침을 공개하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조의2(개인정보 취급방침의 공개) ① 정보통신서비스 제공자 등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

정보통신망 이용촉진 및 정보보호등에 관한 법률 시행규칙

제8조 (개인정보 취급방침의 공개 방법 등) ① 정보통신서비스 제공자 외의 자는 법 제27조의2제1항 및 제67조제1항에 따라 개인정보의 수집 장소와 매체 등을 고려하여 다음 각 호 중 어느 하나 이상의 방법으로 개인정보 취급방침을 공개하되, 그 명칭을 '개인정보 취급방침'이라고 표시하여야 한다.

1. 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 법 제27조의2제2항 각 호의 사항을 재화 또는 용역을 제공받는 자가 볼 수 있게 하는 방법. 이 경우 글자 크기, 색상 등을 활용하여 개인정보 취급방침을 쉽게 확인할 수 있도록 표시하여야 한다.
2. 점포 · 사무소 안의 보기 쉬운 장소에 써서 붙이거나 갖춰 놓고 열람하게 하는 방법
3. 같은 제목으로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물 · 소식지 · 홍보지 · 청구서 등에 지속적으로 게재하는 방법
4. 재화 또는 용역을 제공하기 위한 이용계약서에 게재하여 배포하는 방법

좀 더 알아 봅시다

□ 개인정보 취급방침의 공개 방법 취지

● 개인정보 취급방침은 이용자(고객)로 하여금 사업자가 어떠한 기준에 따라 개인정보를 처리하고 보호하는지를 쉽게 확인할 수 있도록 하기 위한 취지이다. 그러나 만일 개인정보 취급방침의 공개 방법이 통일되어 있지 않으면, 이용자는 개인정보 취급방침의 공개 여부를 확인하기 어렵다. 이에 따라 관련 법률에서는 개인정보 취급방침 공개방법 표준을 제시하고 있다.

□ 개인정보 취급방침의 공개시 주의할 점

● 이전에는 사업자에 따라 "개인정보 보호정책", "개인정보 취급정책" 등 다양한 용어가 혼재되어 사용되기도 하였으나, 현재는 반드시 "개인정보 취급방침"이라는 명칭을 사용하여야 한다.

- 개인정보 취급방침은 위의 4가지 방법 중 어느 하나 이상의 방법을 선택하여 공개하여야 하며, 이용자(고객)가 가장 많이 이용하는 매체 · 장소에 우선적으로 개인정보 취급방침을 공개하여야 한다.

- 인터넷 홈페이지에 개인정보 취급방침을 공개할 경우에는 글자 크기, 색상 등을 활용하여 알기 쉽게 표시하여야 한다. 구체적으로는 다른 고지사항보다 큰 글씨나 굵은 글씨(볼드체)를 사용하고 눈에 띄는 색상을 사용하면 된다.

〈홈페이지 개인정보 취급방침 공개 예시〉

회사소개 채용공고 이용약관 **개인정보 취급방침** 청소년보호정책

관련 위반사례

- ○○호텔은 웹사이트 상에 개인정보 취급방침을 공개하고 있으나, 이용자가 쉽게 인지할 수 있도록 글자 크기 · 색상 등을 다르게 하지 않고 다른 고지사항과 똑같은 글자크기 및 색상으로 표시

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 이용자가 쉽게 확인할 수 있도록 행정안전부령이 정하는 방법에 따라 공개 (정보통신망법 제27조의2)	○ 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인 할 수 있도록 대통령령으로 정하는 방법에 따라 공개 (개인정보보호법 제30조)

3. 개인정보 취급방침을 변경할 때는

Q | 고객들에게 새로운 서비스를 제공함에 따라서 개인정보의 수집 · 이용목적, 수집하는 항목 등도 새롭게 변경되었다. 이러한 경우에는 개인정보 취급방침에 어떻게 반영하여야 하나?

A | 개인정보 취급방침을 변경하려면 변경 이유, 변경 내용을 아래의 방법에 따라서 지체없이 이용자에게 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하여야 한다.

① 인터넷 홈페이지 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
② 서면 · FAX · 전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법
③ 점포 · 사무소 안의 보기 쉬운 장소에 써서 붙이거나 갖춰 놓는 방법
④ 이용계약서에 게재하여 배포하는 방법

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제27조의2(개인정보 취급방침의 공개) ③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 취급방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제8조(개인정보 취급방침의 공개 방법 등) ② 법 제27조의2제3항 및 제67조제1항에 따른 개인정보 취급방침의 변경 이유 및 내용은 다음 각 호 중 어느 하나 이상의 방법으로 공지한다.

1. 정보통신서비스 제공자 외의 자가 운영하는 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
2. 서면 · 모사전송 · 전자우편 또는 이와 비슷한 방법으로 재화 또는 용역을 제공받는 자에게 공지하는 방법
3. 점포 · 사무소 안의 보기 쉬운 장소에 써서 붙이거나 갖춰 놓는 방법
4. 재화 또는 용역을 제공하기 위한 이용계약서에 게재하여 배포하는 방법

좀 더 알아 봅시다

□ 개인정보 취급방침 변경방법 규정 취지

● 개인정보 취급방침에 기재된 내용은 사업자의 서비스 변경 · 폐지, 인력 · 내부 조직의 변경 등에 따라서 달라질 수 있다. 그러나 이러한 변경사항들이 개인정보 취급방침에 제때 반영되지 않는다면, 이용자(고객)는 어떤 내용이 어떻게 바뀌었는지를 확인하기 어렵다. 이에 따라 법률에서는 개인정보 취급방침을 변경할 때에는, 변경이유 · 변경사유를 고지하도록 하고 있다.

□ 개인정보 취급방침 변경시 주의할 점

● 개인정보 취급방침 변경 고지를 할 때에는 해당 개인정보 취급방침의 변경 · 시행 일자도 명확히 기재함으로써 이용자가 변경된 개인정보 취급방침의 적용 시기를 알 수 있도록 조치해야 한다.

개인정보 취급방침 변경 공지문(예시)

1. 시행 일시 : 20XX. 03. 01
2. 변경 사유 : I-PIN 서비스 도입에 따른 수집항목 변경 안내
3. 변경 내용

변경 전	**1.1 개인정보 수집 항목** – 성명, 아이디(ID), 주민등록번호, 주소, 이메일, 휴대전화번호, 결제 정보
변경 후	**1.1 개인정보 수집 항목** – 성명, 아이디(ID), 주소, 이메일, 휴대전화번호, 결제정보 (I-PIN을 입력하여 회원으로 가입하는 경우에는 주민등록번호를 수집하지 않음)

개인정보 관련 사항 변경시 취급방침 공개 사항과 동의받아야 할 사항

변경항목 \ 변경에 따른 조치		개인정보 취급방침 변경	이용자의 별도동의 획득	동의획득 관련 정보통신망법 조항
1	개인정보 수집 · 이용목적	O	O	제22조제1항제1호
	수집하는 개인정보 항목	O	O	제22조제1항제2호
	수집 방법	O	X	-
2	(개인정보를 제3자에게 제공하는 경우) 제공받는 자의 성명	O	O	제24조의2제1항제1호
	제공받는 자의 이용목적	O	O	제24조의2제1항제2호
	제공하는 개인정보 항목	O	O	제24조의2제1항제3호
3	개인정보 보유 · 이용기간	O	O	제22조제1항제3호
	개인정보 파기절차 · 파기방법	O	X	-
4	(개인정보 취급을 위탁하는 경우) 취급위탁을 하는 업무의 내용 및 수탁자	O	O (다만 서비스 계약이행에 필요한 위탁의 경우는 동의 불필요)	제25조제1항제1호 및 제2호
5	이용자 및 법정대리인 권리와 행사 방법	O	X	-
6	인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 · 거부에 관한 사항	O	X	-
7	개인정보 관리책임자의 성명 (부서 명칭)과 연락처	O	X	-

관련 위반사례

- ○○학원은 학원 안내 전화상담을 담당하던 업체가 A콜센터에서 B콜센터로 변경됨에 따라, 이를 개인정보 취급방침에 반영하고 그 변경사실을 이용자에게 공지하였어야 하나, 실제로는 개인정보 취급방침에 변경내용을 반영하기만 하고 이용자에게 변경사실을 공지하지는 않음

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보 취급방침을 변경하는 경우에는 그 이유 및 변경사항을 행정안전부령으로 정하는 방법에 따라 지체없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치 (정보통신망법 제27조의2)	○ 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개 (개인정보보호법 제30조)

4. 해킹과 불법 접근을 차단하려면?

Q | 최근에 해킹을 통한 개인정보 유출사례가 언론에 많이 보도되고 있는데, 우리 회사의 개인정보 DB에 대한 해킹을 차단하려면 어떤 조치를 취해야 하는가?

A | 정보통신망을 통해 개인정보에 불법적으로 접근하는 행위를 방지하기 위해서 침입차단시스템 · 침입탐지시스템 등 접근 통제장치를 설치하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조 (개인정보의 보호조치) ① 정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제9조(개인정보의 보호조치) ② 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다.

2. 개인정보에 대한 권한 없는 접근을 차단하기 위한 암호화와 방화벽 설치 등의 조치

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제11조(접근통제) ① 사업자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 · 운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

좀 더 알아 봅시다

□ 접근 통제장치의 종류

● 정보통신망을 통한 불법적인 접근을 차단 · 통제할 수 있는 장치로는 침입차단시스템, 침입탐지시스템, 침입방지시스템 등이 있다.

- (**침입차단시스템**) 일반적으로 방화벽(firewall)이라고도 부르며, "개인정보처리시스템에 대한 접속권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 차단 · 제한할 수 있는 시스템"을 말한다.
- (**침입탐지시스템**) 사업자의 개인정보처리시스템에 접속한 IP, 트래픽 등을 재분석하여 불법적인 정보 유출시도를 탐지할 수 있는 시스템을 말한다.
- (**침입방지시스템, 기타**) 최근에는 침입차단시스템과 침입탐지시스템이 동시에 구현되어 있는 침입방지시스템(IPS; Intrusion Prevention System)이나 웹 방화벽, 보안 운영체제(Secure OS) 등도 널리 이용되고 있다.

□ 설치 방법

● 다양한 상용 침입차단 · 탐지시스템 및 공개 · 무료 S/W 등이 있으므로, 해당 사업자의 규모, 서비스 유형, 개인정보처리시스템 특성 등에 따라 접근 통제장치를 설치 · 운영하면 된다.

정보보호 평가 · 인증 제품 확인방법

① 국가정보원 IT보안인증사무국 웹사이트 방문 (http://service2.nis.go.kr/)
② Quick Menu에서 '인증제품목록' 선택
③ 다음의 방법에 따라 제품 검색
- 침입차단시스템 : 검색창에서 '제품 유형'을 선택 후 'FW'를 입력하고 '검색' 클릭
- 침입탐지시스템 : 검색창에서 '제품 유형'을 선택 후 'IDS'를 입력하고 '검색' 클릭
- 침입방지시스템 : 검색창에서 '제품 유형'을 선택 후 'IPS'를 입력하고 '검색' 클릭
- 웹 방화벽 : 검색창에서 '제품 유형'을 선택 후 '웹방화벽'를 입력하고 '검색' 클릭
- 보안운영체제 : 검색창에서 '제품 유형'을 선택 후 '접근통제시스템'을 입력하고 '검색' 클릭

토 막 상 식

정보보호제품 평가 · 인증제도

정보보호제품 평가 · 인증제도는 민간업체가 개발한 정보보호제품의 안정성 · 신뢰성을 정부가 보증함으로써 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도를 말한다. 우리나라에서는 1998년부터 정보보호제품 평가 · 인증제도를 도입했으며, 2002년부터는 국제공통평가기준(Common Criteria)에 따라 정보보호제품을 평가 · 인증하고 있다.

- 접근 통제장치의 설치 · 운영 등 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 · 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금이 부과된다.

관련 Q&A

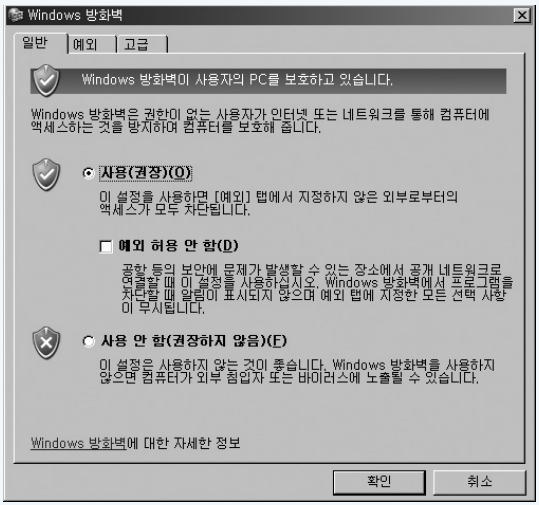
Q | 소규모 사업자는 별도의 개인정보처리시스템 없이 PC만 이용해서 업무를 처리하는 경우가 많다. 이런 경우에도 침입차단 · 탐지시스템을 설치 · 운영해야 하는가?

A | 소규모 사업자의 경우에는 해당 사업자의 규모에 맞게 시스템을 운영하면 된다.

- (자체 시스템 및 서버가 없는 중소 · 영세 사업자) 인터넷데이터센터(IDC)나 호스팅 업체 등에서 제공하는 보안서비스를 이용
- (개인사업자) PC를 이용해서만 업무를 처리하는 경우에는 PC운영체제에서 자체 제공하는 방화벽 기능을 이용하거나 PC용 침입차단시스템 등의 S/W를 이용

※ Windows XP에서의 방화벽 설정 방법

시작 → 설정 → 제어판 → 보안센터 → Windows 방화벽 → '사용'에 체크 → 확인 클릭



※ 공개용(무료) S/W를 사용하는 경우에는 보안 수준을 사전 점검할 필요가 있음
(한국인터넷진흥원 '공개용 웹방화벽을 이용한 홈페이지 보안' 참조,
http://www.krcert.or.kr/firewall2/)

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등 접근 통제장치를 설치·운영 (정보통신망법 제28조제1항제2호)	○ 개인정보처리자는 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 이행 (구체적 조치는 대통령령으로 정함) (개인정보보호법 제29조)

5. 내부직원의 개인정보 유출을 방지하려면

Q | 내부 직원이 개인정보처리시스템에서 개인정보를 유출하는 행위를 방지하기 위해서는 어떤 조치를 취하면 되는가?

A | 사업자는 내부 직원 등에 의한 개인정보의 유출을 방지하기 위하여 접속기록의 보존 및 위조 · 변조 방지를 위한 조치를 취하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조 (개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

3. 접속기록의 위조 · 변조 방지를 위한 조치

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제9조(개인정보의 보호조치) ② 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다.

3. 접속기록의 위조 · 변조 방지를 위한 조치

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제12조(접속기록의 위 · 변조방지) ① 사업자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인 · 감독하여야 하며, 최소 6개월 이상 접속기록을 보존 · 관리하여야 한다.

② 개인정보취급자의 접속기록이 위 · 변조되지 않도록 해당 접속기록을 별도의 물리적인 저장 장치에 보관하고 정기적으로 백업을 수행하여야 한다.

좀 더 알아 봅시다

□ 접속기록 위 · 변조 방지조치 취지

● 개인정보의 대량 유출사고는 해킹과 같은 외부의 공격으로 발생하는 경우도 있으나, 내부의 직원(본사 직원, 대리점 · 영업점 직원 등)에 의해 유출되는 경우도 상당수 발생하고 있다.

● 그러나 만일 내부 직원의 개인정보처리시스템 접속 현황에 대한 기록이 없거나 위 · 변조되었다면, 실제 내부 직원에 의한 개인정보 유출이 발생했다 하더라도 유출사고의 원인조차 파악할 수 없게 된다.

– 따라서 개인정보처리시스템의 접속기록를 보존하고 해당 접속기록이 위 · 변조되지 않도록 관리하는 것은 내부 직원에 의한 악의적인 접근 · 유출시도를 예방하고, 사고 발생시 사고원인을 파악할 수 있는 중요한 수단이 된다. 이러한 취지에서 법률은 개인정보처리시스템에 대한 접속기록을 보존하고 위 · 변조되지 않도록 조치를 취할 것을 규정하고 있다.

□ 접속기록 위 · 변조 방지조치 세부 내용

● 사업자는 개인정보 취급자(직원 등)가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보존 · 관리해야 하며, 월 1회 이상 정기적으로 확인 · 감독하여야 한다.

– 접속기록의 항목에는 개인정보 취급자의 식별정보, 이용자(고객)의 식별정보, 접속일시, 접속지, 수행업무 등이 포함되어야 한다.

접속기록 항목(예시)

취급자 식별정보	정보주체 식별정보	접속일시	접속지	수행업무
홍길동(K00050)	성춘향(850301)	20XX.05.01 15:00:00	172.168.11.11	온라인상담

벌 칙

● 접근기록의 위조 · 변조 방지를 위한 조치 등 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 · 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금이 부과된다.

관련 위반사례

● ○○쇼핑몰은 고객 개인정보처리시스템 접속기록에 대한 보존 · 관리 조치를 전혀 실시하지 않아, 내부직원이 직무수행상 필요한 경우가 아님에도 불구하고 단순 호기심 등으로 고객 개인정보 및 구매내역 등을 손쉽게 무단 열람

● ○○학원은 개인정보처리시스템에 대한 접속기록의 저장 공간이 부족하다는 이유로, 접속기록을 최소 6개월 간 보존해야 함에도 불구하고 단지 1개월간만 보관한 뒤 모두 파기

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 접속기록의 위조 · 변조 방지를 위한 조치를 하여야 함 (정보통신망법 제28조제1항제3호)	○ 개인정보 처리자는 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치 이행 (구체적 조치는 대통령령으로 정함) (개인정보보호법 제29조)

6. 개인정보 암호화 꼭 해야 하나

Q | 규모가 작은 중소기업으로 인터넷 회원수도 많지 않고 보유하고 있는 개인정보도 성명, ID, 비밀번호, 주민등록번호, 주소 등 비교적 단순한 경우인데도 꼭 암호화를 해야 하나?

A | 사업자는 개인정보를 안전하게 저장·전송하기 위하여 암호화 기술 등을 이용한 보안조치를 취하여야 한다.

질의한 사업자의 경우에는 비밀번호의 일방향 암호화 저장, 주민등록번호의 안전한 암호화 저장, 인터넷 회원의 로그인시 보안서버 적용 등의 조치를 이행하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조 (개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제15조(개인정보의 보호조치) ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장
2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제9조(개인정보의 보호조치) ② 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다.

2. 개인정보에 대한 권한 없는 접근을 차단하기 위한 암호화와 방화벽 설치 등의 조치

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제10조(개인정보의 암호화) ① 사업자는 주민등록번호, 신용카드번호, 계좌번호 등 중요 개인정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

② 사업자는 비밀번호 및 바이오정보가 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 사업자는 정보통신망을 통해 이용자의 개인정보 등을 송 · 수신할 때에는 보안서버 등의 조치를 통해 이를 암호화하여야 한다.

④ 중요 개인정보를 업무용 컴퓨터에 저장하여 관리하는 경우 암호화 소프트웨어나 일반 업무용 프로그램(엑셀, 한글 등)에서 제공하는 암호화 방법을 사용하여야 한다.

좀 더 알아 봅시다

□ 개인정보 암호화의 취지

● 개인정보가 암호화되지 않고 저장 또는 전송되고 있다면, 만일 내 · 외부의 불법적인 접근이나 공격에 의해 해당 개인정보가 유출 · 노출되었을 경우 개인정보의 내용을 확인하여 손쉽게 2차 범죄에 악용할 수 있게 된다. 그러나 개인정보가 안전하게 암호화되어 관리되고 있다면 해당 개인정보가 유출 · 노출되었다 하더라도 2차 범죄에 악용되는 것을 방지할 수 있다.

□ 개인정보 암호화의 세부 기준

● 개인정보 저장시 암호화

– (비밀번호, 바이오정보) 비밀번호 및 바이오정보는 복호화되지 아니하도록 '일방향 암호화' 하여 저장하여야 한다. 일방향 암호화를 적용한 개인정보는 사업자가 그 내용을 알 수 없으므로, 예컨대 이용자가 비밀번호의 분실 등을 이유로 비밀

번호를 알려달라고 요청하는 경우에는 이에 응할 방법이 없다. 따라서 이러한 경우에는 다른 수단을 사용하여(예를 들어 생년월일, 주소, 연락처 등의 정보를 이용자에게 확인하는 방법) 이용자의 신원을 확인한 뒤 이용자에게 임시로 비밀번호를 부여하여 로그인하도록 하고, 그 이후에 이용자 본인이 원하는 새로운 비밀번호를 설정하도록 하여야 한다.

– (주민등록번호, 금융정보) 주민등록번호 및 계좌번호 · 신용카드번호 등 금융정보는 유 · 노출시 2차 피해가 발생할 가능성이 매우 높으므로, 이 정보들은 '안전한 암호알고리즘' 으로 암호화하여 저장하여야 한다.

토 막 상 식

일방향 암호화 / 안전한 암호 알고리즘

일방향 암호화란 개인정보에 '일방향 함수(해쉬 함수)'를 적용하여 암호화하는 방식을 말한다. 개인정보에 일방향 암호화를 적용하면 원래의 개인정보로 복호화 할 수 없다.

'안전한 암호 알고리즘'이란 최소 80비트 이상의 보안강도를 가지는 대칭키 암호 알고리즘을 말한다.(자세한 사항은 한국인터넷진흥원 암호이용 활성화 홈페이지(http://seed.kisa.or.kr) – 자료실 – "암호 알고리즘 및 키 길이 이용 안내서"를 참조)

● 개인정보 전송시 암호화

– 사업자가 정보통신망을 통하여 이용자의 개인정보를 송 · 수신할 경우에는 보안서버 등을 이용하여 암호화 전송함으로써 노출 및 불법적인 접근으로 인한 2차 피해를 방지하여야 한다.

※ 보안서버 구축에 관한 자세한 사항은 한국인터넷진흥원 보안서버 홈페이지 참조(http://secsv.kisa.or.kr)

● 암호화 기술 등을 이용한 보안조치 등 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 · 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금이 부과된다.

관련 Q&A

Q | 서비스 제공이나 상담 등을 위해서는 회원들의 주민등록번호 앞 6자리(생년월일)를 활용할 경우가 많은데, 주민등록번호를 모두 암호화하면 암호화/복호화에 따라 시스템에 상당한 부하가 발생한다. 별다른 방법이 없는가?

A | 주민등록번호, 계좌번호, 신용카드번호 등은 원칙적으로 전부 암호화해야 하나, 시스템 운영이나 고객 식별을 위해 해당 개인정보를 활용해야 하는 경우에는 그 개인정보의 일부만을 암호화할 수 있다.

- (주민등록번호) 생년월일 및 성별을 포함한 앞 7자리를 제외하고 뒷자리 6개 번호 이상을 암호화 (예) 750101-1######
- (신용카드번호) 카드유형 정보를 포함한 6자리를 제외하고 뒷자리 10개 이상을 암호화 (예) 4902-20##-####-####

관련 위반사례

- ○○백화점은 고객 개인정보 암호화 조치의무를 이행하지 않고 단순한 평문으로 개인정보를 보관하여 오다가, 해커의 공격에 의해 대량의 개인정보를 유출당함
- ○○온라인게임사는 이용자의 ID, 비밀번호 등 개인정보를 암호화되지 않고 평문으로 로그파일에 저장되도록 함에 따라, 기술적 보호조치 미비를 이유로 고객들로부터 손해배상 소송

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 사업자는 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하여야 함 (정보통신망법 제28조제1항제4호)	○ 개인정보 처리자는 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치 이행 (구체적 조치는 대통령령으로 정함) (개인정보보호법 제29조)

7. 보안프로그램은 어떻게 설치 · 이용하면 될까

Q | 바이러스 방지를 위한 백신 프로그램을 설치해야 한다고 해서 프로그램을 구입하고 PC에 설치하였다. 더 이상의 보호조치는 필요 없는가?

A | **사업자는 백신 소프트웨어의 설치 · 운영 등 컴퓨터 바이러스에 의한 침해 방지 조치를 취하여야 한다.**

백신 소프트웨어는 최초에 설치하는 것도 중요하지만, 이후 지속적으로 업데이트 하여 최신의 컴퓨터 바이러스나 악성코드를 방지할 수 있도록 최선의 상태를 유지시키는 것이 필요하다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조 (개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실 · 도난 · 누출 · 변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적 · 관리적 조치를 하여야 한다.

5. 백신 소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제9조(개인정보의 보호조치) ② 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다.

4. 침해사고 방지를 위한 보안프로그램의 설치 및 운영

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제13조(보안프로그램의 설치 및 운영) 사업자는 개인정보를 개인정보처리시스템 또는 업무용 컴퓨터에 보관하는 경우에는 보안프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 개인정보의 취급 및 처리와 관련된 모든 업무용 컴퓨터에 대해 백신 소프트웨어의 자동 업데이트 사용 또는 엔진 업데이트 여부를 최소 일 1회 이상 확인
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 소프트웨어의 제작업체에서 업데이트 공지가 있는 경우 관련 백신 소프트웨어의 엔진 업데이트 및 패치 설치

좀 더 알아 봅시다

□ 악성 프로그램의 개념

● '악성 프로그램'이란 의도적으로 다른 인터넷 이용자에게 피해를 주고자 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미한다. 여기에는 컴퓨터 바이러스(Computer Virus), 인터넷 웜(Internet Worm), 트로이목마 등이 있다.

– 악성 프로그램은 컴퓨터나 서버, 데이터베이스에 저장된 자료를 손상시키거나 유출시킴으로써 정상적인 작업을 방해한다. 특히 최근에는 개인정보를 유출시키기 위한 목적의 악성 프로그램이 많이 등장하고 있다. 이를 방지하기 위해 백신소프트웨어 등을 이용하여 악성 프로그램을 제거하거나 감염되지 않도록 예방할 필요가 있다.

□ 백신 프로그램 운영 방법

● 악성 프로그램은 계속해서 진화 · 발전되어 유포되고 있다. 이에 대응하여 백신 프로그램 제조사는 새로운 악성 프로그램에 대응할 수 있도록 업데이트 기능을 제공하고 있다.

– 따라서 백신 소프트웨어는 최소 주 1회 이상 주기적으로 갱신 점검을 하는 것이 바람직하며, 이때 인터넷을 이용한 자동 업데이트/실시간 감지 기능 등을 활용하면 보다 편리하고 신속하게 갱신 · 점검을 할 수 있다.

– 만일 긴급한 악성 프로그램 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지가 있는 경우에는 즉시 최신 소프트웨어로 갱신 · 점검해야 한다.

● 보안패치는 운영체제(OS)나 응용 프로그램에 내재된 보안 취약점 보완을 위해 해당 운영체제나 프로그램 제조사에서 배포하는 소프트웨어를 말한다. 운영체제 제작사 등에서 업데이트 공지가 있는 경우 신속히 최신 보안패치를 적용하는 것이 필요하며, 가능하면 자동적으로 보안패치가 업데이트 되도록 할 필요가 있다.

토 막 상 식

Windows XP 보안패치 업데이트 방법은?

① 인터넷 익스플로러 실행
② 도구 → Windows Update 실행
③ 최신 업데이트 소프트웨어 확인 및 설치

※ 자동 보안패치 설정 방법은 한국인터넷진흥원 보호나라 웹사이트 참조
(http://www.boho.or.kr/pccheck/pcch_05.jsp?page_id=5)

벌 칙

● 컴퓨터바이러스에 의한 침해방지 조치 등 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 · 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금이 부과된다.

관련 위반사례

● ○○콘도미니엄은 운영체제 및 보안프로그램을 정기적으로 업데이트 및 관리하지 않고 있다가, 보안패치 미적용에 따른 시스템 취약점이 발생하여 해킹에 의한 개인정보 유출 피해를 입음

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 백신소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지 조치 (정보통신망법 제28조제1항제5호)	○ 개인정보 처리자는 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치 이행 (구체적 조치는 대통령령으로 정함) (개인정보보호법 제29조)

8. 개인정보에 대한 접근권한은 최소한으로

Q | 고객모집 영업을 위해서 본사 외에 대리점, 위탁점에도 개인정보처리시스템 접속을 허용하려고 한다. 접근권한을 부여할 때 지켜야 할 기준에 대해 알고 싶다.

A | 사업자는 개인정보를 취급하는 자를 최소한으로 제한하여야 한다. 특히 **개인정보처리시스템에 대한 접근권한은 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 한다.**

질의와 같이 대리점, 위탁점에 개인정보처리시스템에 대한 접근권한을 부여하는 경우에도 업무의 성격에 따라 반드시 필요한 범위 내에서 최소한의 자에게 접근권한을 부여해야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제28조 (개인정보의 보호조치) ② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제9조(접근권한, 인증 및 계정관리) ① 사업자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여 하여야 한다.

② 사업자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우에는 지체없이 접근권한을 변경 또는 말소하여야 하며, 주기적으로 접근권한을 관리하여야 한다.

③ 사업자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관하여야 한다.

좀 더 알아 봅시다

□ 개인정보 취급자의 제한

- 사업자는 개인정보 취급자를 최소한으로 제한하여야 한다. 이는 개인정보에 대한 접근권한이 무분별하게 부여됨에 따라 해당 직원에 의해 개인정보의 접근 및 유출, 오 · 남용이 발생하는 것을 방지하기 위한 취지이다.

- 개인정보 취급자의 전보, 퇴직 등으로 인사이동이 발생한 경우에 그 사람이 보유하고 있던 접근권한에 대한 관리가 즉시 이루어지지 않으면 예기치 않은 불법적 접근 · 침해가 발생할 우려가 있다. 따라서 인사이동이 있는 경우에는 그 사람이 보유하고 있는 접근권한을 지체없이 변경 또는 말소해야 한다. 개인정보 취급자의 인사이동에 따른 접근권한 관리를 보다 효율적으로 처리하기 위해서는, 업무인수인계서 또는 퇴직 점검표 등에 개인정보처리시스템 접근권한 관리 항목을 반영하고 확인을 받는 것이 좋다.

- 또한, 사업자는 개인정보 처리시스템에 대한 접근권한 부여, 변경, 말소에 대한 내역을 기록하고, 그 기록을 최소한 5년간 보관하여야 한다.

관련 위반사례

- ○○통신사업자는 본사 및 대리점의 직원에 대해 개인정보처리시스템에 대한 접근권한을 제한없이 부여하여 왔으며, 위탁영업점(대리점)의 직원 A는 이를 악용하여 사전 승인 없이 개인정보를 임의로 열람 · 조회 · 출력

9. 물리적인 접근제한 조치를 하려면

Q | 고객을 대상으로 이벤트를 진행하고 있는데, 개인정보가 포함된 응모권을 사무실에 놔두고 있다. 이렇게 개인정보 자료를 보관해도 특별한 문제는 없는가?

A | 사업자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소에 대한 별도의 출입통제 절차를 수립하여야 하며, 접근기록을 보관하여야 한다.

질의와 같은 이벤트 응모권 등 개인정보가 기재된 자료 · 서류는 사무실 내의 별도의 장소에 보관하고 출입통제를 하거나, 최소한 잠금장치를 마련하여 보관하는 등 물리적인 접근방지 조치를 취하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

제9조 (개인정보의 보호조치) ① 법 제28조제1항 및 제67조제1항에 따른 개인정보의 안전성 확보에 필요한 관리적 조치는 다음 각 호와 같다.

3. 개인정보의 안전한 보관을 위한 잠금장치 등 물리적 접근방지 조치

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제6조(물리적 접근 제한) ① 사업자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 별도의 출입통제 절차를 수립하여야 하며 접근기록을 보관 하여야 한다.

② 사업자는 개인정보가 포함된 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

좀 더 알아 봅시다

□ 물리적 접근제한 조치

● 개인정보를 취급하는 사업자는 그 개인정보를 시스템에 보관하거나 또는 문서,

출력물 등으로 보관하는 경우도 많다. 따라서 개인정보처리시스템에 대한 전산적 접근통제 외에, 이러한 물리적 보관 장소에 대해서도 접근제한 조치를 취할 필요가 있다.

● 물리적 보관 장소에 대해서는 잠금장치 등이 마련되어야 하고, 사업장에 출입하는 절차와는 별도의 출입통제 절차가 마련되어야 한다. 즉, 개인정보를 물리적으로 보관하는 장소에 출입할 수 있는 권한을 부여받은 직원만이 출입이 가능하도록 해야 하며, 그 외에는 비록 직원이라도 출입을 허용해서는 안된다.

□ 보조저장매체의 보관

● 최근에는 USB 메모리, 외장하드디스크와 같은 이동식 보조저장매체를 사용하여 업무를 처리하는 경우가 늘어나면서, 이러한 이동식 보조저장매체를 통한 개인정보 유출이 새로운 문제가 되고 있다.

● 사업자는 개인정보가 포함된 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

● 물리적인 접근제한 조치 등 기술적 · 관리적 조치를 하지 아니하여 이용자의 개인정보를 분실 · 도난 · 누출 · 변조 · 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금이 부과된다.

● ○○정유사의 직원 A는 고객 개인정보를 아무런 통제절차 없이 외장형 하드디스크, USB 메모리 등에 편집 · 저장한 뒤 외부로 유출

10. 개인정보를 출력 · 복사할 때는

Q | 우리 회사는 업무성격상 개인정보를 종이에 출력하는 경우가 많다. 이 경우 어떠한 보호조치를 취해야 하는지 알고 싶다.

A | 사업자가 개인정보를 종이로 출력하거나 보조저장매체에 복사할 경우에는 **출력 · 복사물의 일련번호, 형태, 일시, 목적, 출력 · 복사한 자의 소속 · 성명, 전달받을 자, 파기 책임자에 관한 사항을 기록하고 개인정보관리책임자의 승인을 받아야 한다.**

사업자의 개인정보 보호조치 기준 (제정 2010.12.30. 행정안전부 고시 제2010-86호)

제8조(출력 · 복사시 보호조치) ① 개인정보 취급자가 개인정보를 종이로 출력 또는 보조저장매체에 복사할 경우에는 다음 각 호의 사항을 기록하고 개인정보 관리책임자의 승인을 받아야 한다. 출력 · 복사물을 다시 출력 또는 복사하는 경우에도 또한 같다.

1. 출력 · 복사물 일련번호
2. 출력 · 복사물의 형태
3. 출력 · 복사일시
4. 출력 · 복사의 목적
5. 출력 · 복사한 자의 소속 및 성명
6. 출력 · 복사물을 전달 받을 자
7. 출력 · 복사물의 파기(예정)일자
8. 출력 · 복사물의 파기 책임자 등

좀 더 알아 봅시다

□ 출력 · 복사시 보호조치

● 개인정보 유출의 대부분은 내부 개인정보 취급자에 의해서 발생하고 있으며 대부분

인쇄물 출력이나 외장하드, CD/DVD, USB 메모리 등 보조저장매체에 복사하는 형태로 이루어지고 있다.

● 따라서 내부 개인정보 취급자가 업무상 개인정보를 인쇄 · 복사할 경우에는 사전 통제절차를 거치도록 하고 내역을 기록하도록 함으로써, 개인정보 유출을 사전 방지하는 효과를 거두는 한편 만약 유출사고가 발생한 경우에는 유출 경로를 확인할 수 있다.

□ 출력 · 복사시 기록할 사항

● 출력 · 복사시 기록할 사항에 대한 세부적 사항은 다음과 같다.

– (**일련번호**) 별도 일련번호가 부여되는 영수증, 신용카드 전표, 탑승권 등은 출력 · 복사물 일련번호를 기록하지 아니할 수 있다. 한편 일련번호 기록은 디지털 워터마킹 기능을 활용할 수도 있다.

– (**형태**) 출력 · 복사물의 형태는 '종이인쇄' 또는 '이동식 보조저장매체' 등으로 구분된다. 다만 출력 · 복사물의 형태를 반드시 "종이인쇄", "USB메모리 복사" 등과 같이 기록할 필요는 없으며 분류가 가능한 약어를 사용하는 것도 무방하다.

– (**파기(예정)일자, 파기책임자**) 개인정보의 출력 · 복사물의 파기일자나 파기책임자를 사전에 알 수 없는 경우가 있다. 이러한 때에는 관련 사항을 기록하지 않을 수 있다.

※ 이용자 본인이 출력 · 복사를 요구하는 경우, 법률에 따라 개인정보를 제공하는 경우 등

제 7 장 고객의 개인정보 권리, 언제 어디서나 당당하게

1. 고객이 회원 탈퇴를 요구할 때는

2. 가입은 쉽게 탈퇴는 가입보다 더 쉽게

3. 이용자가 수집동의에 대한 증빙을 요구할 때는

4. 개인정보 이용 내역을 요구하는 경우는

5. 개인정보의 이용 정정 요구는 이렇게 대응하자

6. 지체없이 필요한 조치란

7. 개인정보 파기는 언제 어떻게 해야 하는가

8. 개인정보 파기의 예외사유는

제7장 고객의 개인정보 권리, 언제 어디서나 당당하게

1. 고객이 회원 탈퇴를 요구할 때는

Q | 이용자가 회원 탈퇴를 요구했을 때는 어떤 조치를 취해야 하는지 알고 싶다.

A | **이용자로부터 회원탈퇴 요구를 받은 경우, 사업자는 원칙적으로 수집된 개인정보를 파기하고 회원 자격을 말소하는 등의 조치를 지체없이 취해야 한다.**

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제30조 (이용자의 권리 등) ① 이용자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 수집 · 이용 · 제공 등의 동의를 철회할 수 있다.
>
> ③ 정보통신서비스 제공자 등은 이용자가 제1항에 따라 동의를 철회하면 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.

좀 더 알아 봅시다

□ 동의철회에 따른 조치

- 이용자는 자신의 개인정보를 사업자가 수집 · 이용 · 제공하는데 동의할 권리가 인정되는 한편, 언제든지 그 동의를 철회할 권리도 있다.

- 그러나, 실제 사업자의 영업 형태에서는 "개인정보의 수집 · 이용 · 제공 동의 철회"라는 용어보다는 "회원탈퇴 신청, 서비스 거부신청" 등의 용어가 자주 사용되므로, 이용자의 요구가 어느 유형의 동의철회에 해당하는지를 판단하여 필요한 조치를 취해야 한다. 동의 철회에 따른 필요한 조치의 예시는 아래와 같다.

동의 철회에 따른 필요한 조치 예시

구분	실제 유형	필요한 조치 예시
수집 동의 철회	- 회원 · 멤버십의 탈퇴 · 해지 신청	회원 자격 말소, 개인정보 파기 ※ 개인정보 파기는 다른 법률에 의해 보존이 필요한 경우는 제외
이용 동의 철회	- 제품 홍보 메일 수신을 허용한 고객이 메일 수신을 거부하는 경우 - 부가서비스를 신청했던 고객이 그 부가서비스 이용을 거부하는 경우	홍보 메일 발송 중지 조치 부가서비스 제공 중지 조치
제공 동의 철회	- 제휴 이벤트에 따라 제휴사에 개인정보 제공을 허용했던 이용자가 그 제공을 취소하는 경우 (이벤트 참가 취소)	제3자 제공된 개인정보의 파기 · 회수

□ 만 14세 미만 아동의 동의철회권

● 만 14세미만 아동의 개인정보에 대한 수집 · 이용 · 동의 철회는 그 아동의 법정 대리인이 행사할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제31조(법정대리인의 권리) ① (생략)

② 법정대리인은 해당 아동의 개인정보에 대하여 제30조제1항 및 제2항에 따른 이용자의 권리를 행사할 수 있다.

□ 이용자 권리의 공개

● 사업자는 개인정보의 수집 · 이용 · 제공에 대한 동의철회권 등 이용자의 권리를 개인정보 취급방침에 게재하여 공개하여야 한다.

'개인정보 취급방침'과 관련된 항목

제6장 고객의 개인정보는 철저히 관리하자

→1. 개인정보 취급방침, 이것만은 꼭 기억하자 (96페이지)

벌 칙

● 이용자의 개인정보 수집 · 이용 · 제공 등의 동의 철회에도 불구하고 사업자가 지체없이 개인정보를 파기하는 등 필요한 조치를 하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 회원탈퇴 신청이 있는 경우 회원DB에서는 개인정보를 삭제하지만 홍보메일 DB에서는 삭제되지 않아 회원탈퇴 후에도 홍보메일이 발송되는 경우가 있다. 이러한 경우도 문제가 될 수 있는가?

A | 이용자의 회원탈퇴 신청(동의 철회)시 기본적인 회원자격 말소 등은 물론이고, 홍보메일 수신 등 회원 자격에 따르는 모든 서비스 등도 지체없이 중지 조치를 취해야 한다.

관련 위반사례

● ○○호텔은 회원이 웹사이트를 통하여 회원탈퇴 신청을 한 경우, 탈퇴 조치는 즉시 취해주고 있으나 회원 개인정보 파기 등 '탈퇴에 따르는 조치'는 이행하지 않아 나중에 광고 메일이 탈퇴 회원에게 전송

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 이용자는 사업자에 대하여 언제든지 개인정보 수집 · 이용 · 제공 등의 동의를 철회할 수 있음 (정보통신망법 제30조)	○ 정보주체는 개인정보처리자에 대하여 자신의 개인정보의 정정 · 삭제 · 처리 정지를 요구할 수 있음 (개인정보보호법 제36조, 제37조)

2. 가입은 쉽게 탈퇴는 가입보다 더 쉽게

Q | 할인점 고객을 대상으로 온·오프라인 가입신청을 받는 멤버십 제도를 운영하고 있는데 멤버십 탈퇴는 잔여 포인트 조회·정산 등을 위해 반드시 할인점 고객센터에 내방하여 처리하도록 하고 있다. 이러한 방식에 문제는 없는지 알고 싶다.

A | **사업자는 개인정보의 수집·이용·제공 등에 대한 동의 철회(회원탈퇴 신청 등) 방법, 개인정보에 대한 열람·제공·오류정정 요구 방법을 개인정보의 수집(회원가입) 방법보다 쉽게 하여야 한다.**

따라서 질의와 같이 멤버십 가입신청을 온·오프라인으로 모두 받고 있다면, 멤버십 탈퇴신청도 오프라인은 물론 온라인으로도 탈퇴가 가능하도록 조치하여야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제30조 (이용자의 권리 등) ⑥ 정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

좀 더 알아 봅시다

□ 수집보다 더 쉬운 동의철회 방법

- 법률은 이용자의 개인정보 동의철회 및 열람·제공·오류정정 요구는 개인정보 수집보다 쉽게 하도록 정하고 있다. 이는 일부 사업자들이 회원 확보·유지를 위하여 가입은 손쉽게 하는 반면 탈퇴는 까다롭게 하는 경우를 방지하기 위한 취지이다.

- 예를 들어, 온라인 웹사이트를 통해 가입신청을 받았다면 탈퇴신청도 웹사이트를 통해 손쉽게 이루어질 수 있도록 조치하여야 한다. 일부 사업자의 경우 회원탈퇴

처리시 요금정산, 포인트 정산, 신원확인 등을 이유로 오프라인에서의 처리를 요구하는 경우가 종종 있으나, 만약 온라인으로 회원가입을 받았다면 이러한 요금정산 등의 조치도 온라인에서 처리되어야 한다.

● 다만, 온라인으로 회원탈퇴를 처리하는 경우에는 오프라인에 비해 회원 본인이 맞는지 확인하는 것이 상대적으로 어려우므로, 예컨대 본인이 아닌 제3자가 악의적으로 회원탈퇴 처리를 하는 등의 피해가 나타날 수 있다.

예) 타인의 게임사이트 ID, 비밀번호를 도용한 후 게임아이템을 절취한 뒤 회원탈퇴 신청을 하는 사례

– 이러한 피해사례를 방지하기 위해서는, 온라인 회원탈퇴 처리시에 패스워드 및 기타 인증정보(공인인증서, 휴대폰인증, 아이핀 등)를 이용하여 본인인증을 추가로 실시하는 것이 안전하다.

토 막 상 식

웹사이트 회원탈퇴 기능 구현 안내서

한국인터넷진흥원은 웹사이트를 통한 안전한 회원탈퇴 기능을 구현하기 위한 안내서를 제공하고 있다.

www.kisa.or.kr → 자료실 → 관련법령 → 안내서 · 해설서 → 웹사이트 회원탈퇴 기능 구현 안내서

● 사업자가 개인정보의 수집 · 이용 · 제공 등에 대한 동의 철회 방법, 개인정보에 대한 열람 · 제공 · 오류정정 요구 방법을 개인정보 수집방법보다 쉽게 하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 웹사이트에 반드시 "회원탈퇴" 메뉴를 만들어야 하는가? 이메일, 전화 등을 통해 회원탈퇴 신청을 받는 것은 안되는가?

A | 전화나 이메일 등을 통한 회원탈퇴 조치도 가능하다. 다만 전화나 이메일을 통한 회원탈퇴 요청은 웹사이트에서의 회원탈퇴 전용 메뉴보다 불편한 점이 있고, 무엇보다 회원 본인인지의 확인(본인 인증)이 어려울 수 있다. 따라서 온라인 가입 회원에 대해서는 가능한 웹사이트에서 본인인증 및 회원탈퇴 조치가 이루어지도록 "회원탈퇴 메뉴"를 구성하는 것이 바람직하다.

Q | 게임사이트를 운영하고 있는데, ID 도용 및 이에 따른 게임아이템 절취 사건이 자주 발생하고 있어 부득이 회원탈퇴 신청시 신원 확인을 위해 이용자 본인의 신분증(주민등록증 등) 사본을 반드시 요구하고 있다. 법률상 문제는 없는가?

A | 이용자의 회원탈퇴는 가입보다 쉽게 하여야 하므로, 가입시 요구되지 않았던 신분증 사본 등을 탈퇴시에 요구하는 것은 법률 위반에 해당한다.
타인에 의한 악의적인 회원탈퇴를 방지하기 위해서는 온라인 상에서 비밀번호 외에 별도의 인증정보(공인인증서, 휴대폰인증, 아이핀 등)를 받아 신원을 확인하거나, 주민등록증 진위확인 서비스를 이용하여 본인인지 여부를 확인하는 방법을 이용할 수 있다.

토 막 상 식

주민등록증 진위확인 서비스

주민등록증 상의 성명, 주민등록번호, 발급일자 정보 및 공인인증서를 이용하여 그 주민등록증의 진위 여부를 확인할 수 있는 방법이다.

이용방법 : 민원24(www.minwon.go.kr) → 확인서비스 → 주민등록증 진위확인
(서비스 이용을 위해서 공인인증서 필요)

관련 Q&A

Q | 사망한 사람의 회원탈퇴를 유가족이 대리하여 요청할 수 있는가?

A | 이용자 본인이 사망한 경우는 유가족이 회원의 사망확인서, 가족관계등록부 등을 구비하여 탈퇴를 신청할 수 있다.

관련 위반사례

- ○○어학원은 학원 수강 이력이 있는 회원은 온라인 회원탈퇴 신청만으로 회원탈퇴를 해주지 않고 오프라인에서 별도의 상담원의 면담을 거쳐야만 탈퇴할 수 있도록 함으로써, 개인정보 동의철회(탈퇴) 방법을 회원가입 방법보다 쉽게 하도록 규정한 관련 법률을 위반

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보의 수집 등에 대한 동의철회 방법은 개인정보 수집방법보다 쉽게 하여야 함 (정보통신망법 제30조)	○ 개인정보의 수집 등에 대한 동의철회 방법을 개인정보 수집방법보다 쉽게 하는데 대한 별도 규정 없음 ○ 개인정보의 정정 · 삭제 요구 방법 등에 필요한 사항은 대통령령으로 정함 (개인정보보호법 제35조, 제36조, 제37조)

3. 이용자가 수집동의에 대한 증빙을 요구할 때는?

Q | 프랜차이즈 외식업체를 운영하고 있는데, 고객들에게 서면으로 멤버십 가입 신청서를 받은 뒤 포인트 적립이나 신메뉴 안내 등의 서비스를 제공해 왔다. 그런데 어떤 고객이 자신은 멤버십 가입신청서에 동의한 적이 없다면서 확인을 요구해 왔다. 이런 경우 어떻게 해야 하는가?

A | 이용자로부터 개인정보 수집 동의 여부에 대한 확인요구를 받은 경우에는 지체 없이 해당 회원의 가입신청서를 제시하여 동의 기재란의 자필서명 여부 등을 열람 · 확인할 수 있도록 하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제30조(이용자의 권리 등) ① (생략)

② 이용자는 정보통신서비스 제공자 등에 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 제공자 등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자 등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자 등에게 개인정보 수집 · 이용 · 제공 등의 동의를 한 현황

③ (생략)

④ 정보통신서비스 제공자 등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

좀 더 알아 봅시다

□ 개인정보 수집 · 이용 · 제공 동의내역 요구

- 이용자는 사업자에 대하여 자신의 개인정보 또는 개인정보를 이용하거나 제3자에게 제공한 현황, 이용자가 수집 · 이용 · 제공 등에 대해 동의한 현황에 대해 열람 · 제공 · 오류정정을 요구할 수 있다.

– (온라인) 개인정보처리시스템과 연동하여 이용자의 동의내역 요구를 즉시 열람 · 조회할 수 있도록 하여야 한다.

– (서면 등 오프라인) 이용자의 동의내역 요구가 있는 경우, 서면 가입신청서, FAX, 전화 녹취 자료 등을 지체없이 제시하여야 한다.

'개인정보 수집 · 이용 · 동의내역 요구'와 관련된 항목

제7장 고객의 개인정보 권리, 언제 어디서나 당당하게
→ 4. 개인정보 이용내역을 요구하는 고객은 (139페이지)

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 이용자는 사업자에 대해 자신의 개인정보, 개인정보 이용 및 제3자 제공 현황, 개인정보 수집 · 이용 · 제공 등의 동의를 한 현황에 대해 열람 · 정정을 요구할 수 있음 (정보통신망법 제30조제2항, 제4항)	○ 개인정보처리자는 정보주체로부터 정당하게 개인정보를 수집하였고 동의를 획득하였다는 것을 입증하여야 함 (개인정보보호법 제16조제1항, 제22조제2항)

4. 개인정보 이용내역을 요구하는 고객은

Q | 고객이 현재까지 부가서비스 가입내역 등의 개인정보 이용내역을 전부 확인시켜 줄 것을 요구하고 있다. 개인정보 이용내역 분량이 매우 많은데, 이러한 경우에는 어떻게 조치하면 되는가?

A | 사업자는 이용자의 열람·제공 요구가 있는 경우에는 지체없이 필요한 조치를 취하여야 한다.

질의와 같이 부가서비스 가입내역 등 개인정보 이용내역을 요구한 경우에는 비록 그 해당 기간이 길고 분량이 많다 하더라도 지체없이 열람·제공하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제30조 (이용자의 권리 등) ② 이용자는 정보통신서비스 제공자 등에 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 제공자 등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자 등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자 등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

④ 정보통신서비스 제공자 등은 제2항에 따라 열람 또는 제공을 요구받으면 지체없이 필요한 조치를 하여야 한다.

좀 더 알아 봅시다

□ 열람·제공 및 정정 요구권

● 이용자가 개인정보 열람·제공 및 정정을 요구할 수 있는 사항은 아래와 같다. 개인정보 그 자체 뿐만 아니라 개인정보의 이용·제3자 제공 현황 등도 포함됨에 유의하여야 한다.

열람 · 제공, 정정을 요구할 수 있는 사항

1. 사업자가 가지고 있는 이용자의 개인정보
2. 사업자가 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 이용자가 사업자에게 개인정보 수집 · 이용 · 제공 등의 동의를 한 현황

□ 열람 · 제공 및 정정 요구에 따른 조치

● 이용자가 개인정보의 열람 · 제공, 오류정정을 요구한 경우에는 사업자는 지체없이 그에 따른 필요한 조치를 취하여야 한다.

열람 · 제공, 오류 정정 요구시 필요한 조치 예시

요구대상	필요한 조치 예시
사업자가 보관하고 있는 개인정보	온라인을 통한 개인정보 조회메뉴 제공, 회원명부 등 서류를 원본 그대로 또는 복사하여 이용자에게 제공 등
개인정보 이용 · 제3자 제공 현황	부가서비스 가입내역, 홍보 이메일 · 전화 발송내역, 제휴사에 대한 개인정보 제공내역 등을 온라인 조회메뉴를 통해 제공하거나 관련 서류로 제공
개인정보 수집 · 이용 · 제공 등의 동의 현황	온라인을 통한 회원가입 동의여부, 서면 가입신청서 원본 등을 제공

※ 열람 · 제공 후 오류가 있는 경우에는 그에 대한 정정 조치 포함

● 이용자의 오류 정정 요구에도 불구하고 지체없이 조치를 취하지 못하는 경우가 있을 수 있다. 이 때에는 그 사유를 이용자에게 알리고, 필요한 조치를 할 때까지는 해당 개인정보를 이용 · 제공하여서는 안된다.

● 또한, 이용자의 열람 · 제공 및 정정 요구도 이용자의 동의철회 요구와 마찬가지로 개인정보 수집보다 쉽게 하여야 한다. 예를 들어, 온라인 웹사이트를 통해 회원

가입을 받은 경우라면 개인정보의 열람도 온라인으로 가능하도록 조치하여야 한다.

벌 칙

● 이용자가 본인에 관한 개인정보의 열람 및 제공을 요구하였으나 사업자가 지체없이 필요한 조치를 하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 이용자는 사업자에 대하여 본인의 개인정보에 대한 열람·제공 및 오류에 대한 정정을 요구할 수 있음 (정보통신망법 제30조)	○ 정보주체는 개인정보 처리자가 처리하는 자신의 개인정보 열람을 요구할 수 있음 (개인정보보호법 제35조)

5. 개인정보의 이용 · 정정 요구는 이렇게 대응하자

Q | 고객들에 대하여 우리 회사 서비스의 광고 메일 및 전화(TM) 홍보를 실시하고 있는데, 어떤 고객이 수신거부를 요청하였다. 이 경우 취해야 할 조치는 무엇인가?

A | 이용자가 광고메일 및 전화 TM에 대한 수신거부를 요청한 경우에 사업자는 지체 없이 발송 중지 및 리스트 삭제 등 필요한 조치를 취하여야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> 제30조 (이용자의 권리 등) ① 이용자는 정보통신서비스 제공자 등에 대하여 언제든지 개인정보 수집 · 이용 · 제공 등의 동의를 철회할 수 있다
>
> ③ 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.

좀 더 알아 봅시다

□ 광고성 전자우편 발송, 전화 TM 등에 대한 수신거부

- 최근 온라인을 기반으로 한 사업 활성화에 따라 대부분의 사업자는 고객을 대상으로 이메일, 전화 등을 통해 광고나 마케팅을 실시하고 있다. 그러나 수시로 전송되는 대량의 광고성 메일이나 전화TM으로 이용자들이 불편을 호소하는 사례 또한 증가하고 있다.

- 이에 따라 이용자가 개인정보를 광고 · 마케팅 등에 이용하는데 동의하였다 하더라도 이후에 동의를 철회할 수 있도록 규정함으로써 개인정보가 무분별하게 광고 · 마케팅에 이용되는 것을 방지하고 있다.

● 특히, 현행 법률은 광고성 메일 · 전화에 대해서는 "수신거부" 제도를 별도로 규정하고 있다. 즉 수신자의 명시적인 수신거부 의사에 반하여 영리목적의 광고성 전자우편을 전송할 수 없다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제50조(영리목적의 광고성 정보 전송 제한) ① 누구든지 전자우편이나 그 밖에 대통령령으로 정하는 매체를 이용하여 수신자의 명시적인 수신거부의사에 반하는 영리목적의 광고성 정보를 전송하여서는 아니 된다.

● 이용자가 개인정보 이용에 대한 동의를 철회하였음에도 불구하고 사업자가 지체없이 필요한 조치를 하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 이용자가 마케팅 등 개인정보 이용에 대한 동의를 철회한 경우, 사업자는 지체없이 필요한 조치를 취하여야 함 (정보통신망법 제30조)	○ 정보주체는 개인정보 처리자에 대하여 자신의 개인정보의 정정 · 삭제 · 처리정지를 요구할 수 있음 (개인정보보호법 제36조, 제37조) ○ 개인정보 처리자는 정보주체에게 재화 · 서비스를 홍보하거나 판매를 권유하기 위하여 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 함 (개인정보보호법 제22조제3항)

6. 지체없이 필요한 조치란

Q | 멤버십 가입 고객이 자신의 가입 내역과 서비스 이용내역을 조회해줄 것을 요구하였는데, 관련 서류와 기록을 모두 찾아 해당 고객에게 제공하는데 시간이 소요되었다. 그런데 해당 고객은 법률의 규정에 따라 "지체없이" 필요한 조치를 취하지 않았다며 항의를 해왔다. "지체없이"가 구체적으로 얼마만큼의 기간을 의미하는 것인지 알고 싶다.

A | "지체없이"는 이용자의 요구에 대한 조치를 가장 우선순위를 두어 처리하는데 소요되는 시간을 말한다.

질의와 같이 오프라인에서의 서류 조사 등에 시간이 다소 소요되고, 사업자가 고의로 업무처리를 지연한 사정이 없다고 보이는 이상 이는 법률에 따른 "지체없이" 필요한 조치를 취한 경우에 해당된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제30조 (이용자의 권리 등) ③ 정보통신서비스 제공자 등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.

④ 정보통신서비스 제공자 등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

좀 더 알아 봅시다

□ 지체없이 필요한 조치

● 이용자가 개인정보 수집 등에 대한 동의를 철회하였거나 개인정보 등에 대한 열람 · 제공 및 정정을 요구한 경우 사업자는 "지체없이" 필요한 조치를 취하여야 한다. "지체없이"의 기간 · 내역을 일률적으로 정하는 것은 곤란하며, 이용자의

요구 내용, 사업자의 업무 특성 등을 종합적으로 고려하여 해당 사업자의 조치가 지체없이 이루어진 것인지를 개별적으로 판단하여야 한다.

– 예를 들어 온라인으로 회원 가입한 고객의 탈퇴 신청은 다른 별도의 사정이 없는 한 온라인으로 즉시 조치가 가능하여야 하며, 오프라인 회원가입 고객의 열람 · 정정 요구는 다른 업무에 우선하여 최대한 신속하게 해당 서류를 조회 · 열람이 가능하도록 하는 것이 "지체없이" 필요한 조치를 취한 것에 해당된다.

관련 Q&A

Q | 우리 회사의 웹사이트에는 별도의 회원탈퇴 메뉴가 없고, 게시판이나 메일을 통해서 탈퇴신청을 접수 · 처리하고 있다. 그런데 어떤 회원이 게시판에 3번에 걸쳐 회원탈퇴를 요구하는 글을 남겼는데 담당 직원이 다른 업무로 바빠 처리를 하지 못하였다. 어떤 문제가 되는가?

A | 사업자는 이용자의 개인정보의 수집 · 이용 · 제공 등에 대한 동의를 철회하거나, 개인정보 등에 대한 열람 · 제공을 요구한 경우에는 지체없이 필요한 조치를 하여야 한다.

질의와 같이 온라인을 통한 회원탈퇴 신청의 경우에는 즉시 처리가 가능한 것이 통상적이므로, 바쁘다는 이유만으로 3번에 걸친 회원탈퇴 요구를 처리하지 못한 것은 "지체없이" 필요한 조치를 취하지 않은 것에 해당한다.

관련 위반사례

- ○○사업자는 회원탈퇴 요구를 지체없이 처리하였어야 함에도 불구하고, 고객 A씨가 수차례에 걸쳐 회원 탈퇴를 요구하였음에도 특별한 이유 없이 한달 이상 회원탈퇴 처리를 지연

7. 개인정보 파기는 언제 어떻게 해야 하는가

Q | 할인마트의 고객들을 대상으로 경품추첨 이벤트를 실시하였는데, 이벤트 종료 후 이벤트 응모신청서는 어떻게 처리하면 되는지 알고 싶다.

A | 경품추첨 이벤트가 종료된 때에는 응모자로부터 개인정보의 보유 · 이용기간에 대해 별도의 동의를 얻지 않았다면, 지체없이 개인정보가 기재된 응모신청서를 파기하여야 한다.

> **정보통신망 이용촉진 및 정보보호 등에 관한 법률**
>
> **제29조 (개인정보의 파기)** 정보통신서비스 제공자 등은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보를 지체없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.
>
> 1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항 · 제2항에 따라 동의를 받은 개인정보의 수집 · 이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
> 2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제 1항 · 제2항에 따라 동의를 받은 개인정보의 보유 및 이용기간이 끝난 경우
> 3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집 · 이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우
> 4. 사업을 폐업하는 경우

좀 더 알아 봅시다

□ 개인정보 파기 사유

● 개인정보를 파기하여야 하는 구체적 예시는 다음과 같다.

개인정보 파기 사유 예시

파기사유	구체적 사례
개인정보 수집 · 이용 달성	• 이용자가 회원 · 멤버십에서 탈퇴한 경우 • 이용자가 참여한 이벤트가 종료된 경우 • 이용자가 동의한 홍보 · 마케팅이 종료된 경우
보유 · 이용기간 종료	• 개인정보 수집시에 동의 받은 보유 · 이용기간이 종료된 경우 • 다른 법률에 따라서 보관해야 하는 기간이 종료된 경우 • 해지고객이 이용요금을 미납한 경우, 해당 요금이 정산될 때까지
사업 폐지	• 회사의 파산 · 청산 등 사업 종료 • 해당 서비스 폐지

□ 개인정보 파기 시점

● 개인정보의 수집 · 이용목적이 달성된 경우 등에는 해당 개인정보는 “지체없이” 파기하여야 한다. 여기서의 “지체없이”는 시간상으로 “즉시”를 의미하는 것은 아니며, 개인정보 파기에 최대한의 업무 우선순위를 두어 신속히 처리하는데 소요되는 시간을 의미한다. 사업자가 개인정보를 지체없이 파기하였는지에 대해서는 개인정보의 저장매체, 파기방법 등을 종합적으로 고려하여 개별적으로 판단하여야 한다.

□ 개인정보 파기 방법

● 개인정보를 파기할 때는 다시 재생하거나 식별할 수 없도록 파기하여야 한다.

– (서면에 기재된 개인정보) 가입신청서, 이벤트 참가신청서 등 개인정보가 기재된 서면의 경우에는 소각, 분쇄 등 재생할 수 없는 방법으로 파기

– (전자적 방법으로 저장된 개인정보)

• 매체를 반복 사용할 필요가 없는 CD-ROM, DVD-ROM 등 : 물리적으로 파기 · 분쇄

• 매체를 반복 사용할 필요가 있는 하드디스크 등 : “로우 레벨 포맷(Low Level Format)” 등 데이터 복원을 방지할 수 있는 방법을 사용하거나 별도의 전용 소거 S/W를 사용하여 파기

토 막 상 식

로우 레벨 포맷(Low Level Format)

하드 디스크의 표면에 저장공간을 전자적으로 구분하는 트랙과 섹터만 표시되어 있는 상태를 말하며, 이 상태에서는 컴퓨터에서 하드디스크를 사용할 수 없다.

여기에 컴퓨터 운영체제가 하드디스크를 인식하고 기록할 수 있도록 파티션을 분할하는 것을 "하이 레벨 포맷(High Level Format)"이라 칭한다.

● 사업자가 별다른 예외사유 없이 개인정보를 파기하지 않은 경우에는 3천만원 이하의 과태료가 부과된다.

관련 Q&A

Q | 경영부진으로 사업을 폐업하고자 한다. 이 경우 고객 개인정보는 어떻게 하여야 하는가?

A | 사업자가 사업을 폐업하는 경우에는 이용자들에게 사업 폐업일시, 폐업사유, 보유 중인 개인정보의 파기 방침 등을 고지하고, 해당 개인정보를 모두 파기하여야 한다.

Q | 게시판에서 악성 댓글, 명예훼손 등을 반복하는 이른바 '불량회원'을 제재하기 위하여, 회원제명 후 일정기간 동안 재가입을 방지하는 조치를 취하려 한다. 그런데 이를 위해서는 불량회원의 개인정보를 파기하지 않고 보관하는 것이 필요하다. 어떻게 하면 가능한지 알고 싶다.

A | 악성 댓글, 명예훼손 등을 반복하는 이른바 '불량회원'의 개인정보를 파기하지 않고 보관하기 위해서는 회원 가입시 고지사항(개인정보의 수집 · 이용기간)에 게재하여 동의를 얻고, 개인정보 취급방침 및 이용약관에도 불량회원의 탈퇴 이후에 개인정보 보관 이유를 게시함으로써 불량회원 개인정보를 보관할 수 있다.

관련 위반사례

- ○○포털은 약 800만의 회원을 보유하고 있었으나, 경영 악화를 이유로 웹사이트를 폐쇄하게 되자 회원 개인정보 파기, 탈퇴절차 안내 등 필요한 조치를 전혀 취하지 않고 일방적으로 웹사이트를 폐쇄

- ○○마트 등에서 출력한 개인정보가 적법한 파기절차를 거치지 않고 외부로 유출되어 붕어빵 포장봉투 등으로 재활용되다가 적발

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보의 수집·이용목적이 달성된 경우 등에는 지체없이 개인정보를 파기 (정보통신망법 제29조)	○ 개인정보의 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 개인정보 파기 (개인정보보호법 제21조) ※ 현행 법률의 취지와 같음

8. 개인정보 파기의 예외사유는

Q | 쇼핑몰에서 탈퇴한 회원들의 개인정보를 파기하려고 하는데, 일부 회원들은 할부 요금이 아직 미납되었거나 제품 A/S 기간이 남아있다. 이러한 경우에는 어떻게 해야 하는가?

A | 사업자는 개인정보의 수집 · 이용 목적이 달성된 경우 등에는 지체없이 개인정보를 파기하여야 하나, 예외적으로 "다른 법률에 따라 개인정보를 보존하여야 하는 경우"에는 개인정보를 파기하지 않고 보존할 수 있다.

예들들어, 전자상거래 등에서의 소비자 보호에 관한 법률 및 시행령에서는 대금결제 및 재화 공급에 관한 기록을 5년간 보관하도록 하고 있으므로, 질의와 같이 요금 미납, A/S 등에 해당하는 경우에는 동법에 의거 5년간 개인정보 보관이 가능하다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제29조 (개인정보의 파기) 정보통신서비스 제공자 등은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항 · 제2항에 따라 동의를 받은 개인정보의 수집 · 이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제 1항 · 제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우
3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집 · 이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우
4. 사업을 폐업하는 경우

좀 더 알아 봅시다

□ 다른 법률에 따라 보존해야 하는 경우

● 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 다음과 같다.

개인정보 보존 근거법률(예시)

해당 법률	보관사유 및 보관기간
상법 제33조	상업장부와 영업에 관한 중요서류 : 10년 전표 또는 이와 유사한 서류 : 5년
국세기본법 제85조의3	모든 거래에 관한 장부 및 증빙서류 : 그 거래사실이 속하는 과세기간에 대한 해당 국세의 법정신고기한이 지난 날부터 5년
통신비밀보호법 제15조의2	전기통신사업자가 통신사실확인자료를 제공하는데 필요한 성명, 주민번호, 전화번호 : 1년
전자상거래 등에서의 소비자 보호에 관한 법률 시행령 제6조	표시광고에 관한 기록 : 6월 계약 또는 청약철회등에 관한 기록 : 5년 대금 결제 및 재화등의 공급에 관한 기록 : 5년 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 개인정보를 파기하지 않고 보존 (정보통신망법 제29조)	○ 다른 법령에 따라 개인정보를 보존하여야 하는 경우에는 개인정보를 파기하지 않고 보존 (개인정보보호법 제21조) ※ 현행 법률의 취지와 같음

사업자를 위한 개인정보보호 질의·응답집

제 8 장 법을 위반하면 과태료와 벌칙이 부과됩니다

1. 과태료와 벌칙을 알아보자

2. 개인정보 분쟁조정제도, 개인정보 침해신고센터를 활용해 보자

제8장 법을 위반하면 과태료와 벌칙이 부과됩니다

1. 과태료와 벌칙을 알아보자

Q | 사업자가 개인정보보호 조치를 위반하였을 경우 과태료 또는 벌칙이 부과된다고 하는데, 과태료와 벌칙의 차이점은 무엇이고 어떠한 개인정보보호 위반행위에 부과되는지 알고 싶다.

A | '과태료'란 일정한 기준이나 질서를 위반한 행위에 대해 행정관청이 직접 부과하는 '행정질서벌'을 말한다. 이는 형벌이 아니기 때문에 전과기록이 남지 않는다.

'벌칙'(형벌)은 형법이나 기타 법률에 규정된 범죄행위에 대해 법원 재판절차를 거쳐 부과하는 형사벌을 말한다. 여기에는 징역, 벌금 등이 있다.

개인정보관리책임자 미지정, 개인정보취급방침 미공개 등 일정 기준을 위반한 행위는 과태료 부과 대상이며, 동의없는 개인정보 수집 · 이용 등은 벌칙대상이다.

좀 더 알아 봅시다

□ 벌칙의 종류

- 개인정보보호 위반행위에 대해서는 징역 또는 벌금의 2가지 벌칙을 부과하도록 하고 있다.
  - (징역) 형무소 내에 구치하고, 정역(노동)에 복무하게 하는 형벌을 말한다.
  - (벌금) 일정한 금전을 박탈하는 형벌을 말한다.

토 막 상 식

과징금은 무엇인가요 ?

과징금은 법률의무를 위반한 자가 그 행위를 통해 경제적 이익을 얻을 것이 예상되는 경우에 그 부당이익을 환수할 목적으로 부과하는 행정벌을 말한다. 과징금도 관할 행정관청이 직접 부과하며, 역시 형벌이 아니므로 전과기록 등과도 관련이 없다.

개인정보 의무위반 행위에 대해서 "전기통신사업법에 의한 전기통신사업자"에게만 위반행위와 관련한 매출액의 1/100 이하의 과징금을 부과할 수 있도록 규정하고 있다.

□ 과태료 부과 절차

- 위반행위에 대한 과태료는 관할 행정관청(행정안전부장관 또는 방송통신위원회)이 해당 위반행위를 조사 · 확인하여 부과 · 징수한다.

- 관할 행정관청은 과태료 부과처분을 하기 이전에 처분대상자에게 10일 이상의 의견진술 기회를 주어야 한다. 의견진술은 구술 또는 서면으로 할 수 있으며, 이메일 등의 전자문서도 가능하다. 만약 지정된 기일까지 의견진술이 없는 때에는 과태료 부과처분에 대한 의견이 없는 것으로 본다.

- 과태료 부과처분은 관할 행정관청이 위반사실 · 이의방법 · 이의기간을 서면으로 명시하여 과태료 처분대상자에게 고지해야 한다.

- 사업자는 그 처분을 고지받은 날로부터 30일 이내에 관할 행정관청에 이의를 제기할 수 있다. 관할 행정관청은 과태료 처분에 이의가 제기되면 지체없이 관할 법원에 그 사실을 통보하여야 하며, 관할 법원은 「비송사건절차법」에 따른 과태료 재판을 한다.

토 막 상 식

「비송사건절차법」이란 무엇인가요 ?

'비송사건(非訟事件)'이란 국가가 사법질서의 유지를 위하여 후견적인 임무를 수행하는 사건을 말하며, 법인의 등기, 경매, 사채(社債), 회사의 청산, 과태료 처분 등이 비송사건에 포함된다.

비송사건절차법은 이러한 비송사건의 처리를 규정한 법률을 말하며, 과태료 사건에 대해서는 제247조~제251조에서 상세한 규정을 두고 있다.

□ 개인정보보호 위반행위에 대한 벌칙 · 과태료

● 현행 법률상의 개인정보보호 위반행위에 대한 과태료 및 벌칙의 종류는 아래 표와 같다.

개인정보보호 위반행위 과태료 · 벌칙

구분	주요내용	벌칙
개인정보 수집 · 이용	동의없는 개인정보 수집 (제22조)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
	민감한 개인정보 수집 (제23조)	
	법정대리인의 동의 없는 아동 개인정보 수집 (제31조)	
	동의 받은 목적과 다른 목적으로 개인정보 이용(제24조)	
	필요 최소한의 개인정보 이외의 정보를 제공하지 아니하였다는 이유로 서비스 제공 거부(제23조)	과태료 (3천만원 이하)
	주민등록번호외의 회원가입방법 미조치(제23조의2)	
개인정보 제공	이용자 동의 없는 개인정보 제3자 제공(제24조의2)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
개인정보 취급위탁	이용자 동의없는 개인정보 취급위탁 (제25조)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
	개인정보 취급위탁 사실 미공개 (제25조)	과태료 (2천만원 이하)
영업양수에 따른 개인정보 이전	영업양도 등 미통지(제26조제1항)	과태료 (2천만원 이하)
	영업양수자등이 당초 목적과 다른 목적으로 개인정보 이용 또는 제3자 제공(제26조제3항)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
개인정보 관리	개인정보관리책임자 미지정(제27조)	과태료 (2천만원 이하)
	개인정보취급방침 미공개 (제27조의2)	과태료 2천만원 이하)
	기술적 · 관리적 조치 미이행(제28조 제1항 제1호, 제6호)	과태료 (3천만원 이하)
	기술적 관리적 조치 미이행으로 인한 누출 (제28조 제1항 제2호~제5호)	벌칙 (2년 이하 징역 또는 1천만원 이하 벌금)
	개인정보취급자의 개인정보 훼손 · 침해 · 누설 (제28조의2)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
개인정보 파기	개인정보 미파기(제29조)	과태료 (3천만원 이하)
이용자 권리	이용자의 동의철회 · 열람 · 정정요구 미조치 (제30조제3항, 제4항)	과태료(3천만원 이하)
	개인정보 오류 정정 요청에 대한 필요조치를 하지 아니하고 개인정보 제3자 제공 · 이용(제30조제5항)	벌칙 (5년 이하 징역 또는 5천만원 이하 벌금)
	이용자의 동의철회 · 열람 · 정정요구를 개인정보 수집 방법 보다 어렵게 함(제30조제6항)	과태료 (3천만원이하)

관련 Q&A

Q | 개인정보 취급방침을 공개하지 않아서 관할 행정관청으로부터 과태료를 부과받았다. 그런데 만약 과태료를 계속해서 납부하지 않는다면 어떻게 되는가?

A | 과태료 처분을 받은 사업자는 그 처분을 고지받은 날로부터 30일 이내에 관할 행정관청(행정안전부 또는 방송통신위원회)에 이의를 제기할 수 있다. 만약 이의제기 기간에 별다른 이의를 제기하지 아니하고 과태료를 계속해서 납부하지 않으면 「국세 체납처분」의 예에 따라 과태료를 강제 징수하게 된다.

여기서 「국세 체납처분」이란 국세징수법에 의거한 국세(國稅)의 강제집행절차를 말하며, 과태료를 납부하지 않는 경우도 국세를 납부하지 않은 경우와 마찬가지로 국세징수법의 적용을 받아 강제집행한다는 의미이다.

개인정보보호법 이렇게 달라집니다

현 재	법 제정후
○ 개인정보보호 의무위반행위에 대해 과태료 및 벌칙 규정 (정보통신망법)	○ 개인정보보호 의무위반 행위에 대해 과태료 및 벌칙을 부과하되, 일부 위반행위에 대해서는 현행 정보통신망법에 비해 형량 조정 (개인정보보호법) 예) 법정대리인 동의없는 아동 개인정보 처리 : 5년 징역/5천만원 벌금 → 5천만원 이하 과태료로 조정

2. 개인정보 분쟁조정제도, 개인정보 침해신고센터를 활용해 보자

Q | 우리 회사의 홈페이지에서 고객들의 개인정보가 노출되는 사고가 발생하였다. 피해를 입은 고객들이 손해배상 소송을 제기하겠다고 하는데, 우리 회사로서는 소송 절차에 많은 시간과 비용이 들어갈 것 같아 걱정이다. 소송을 거치지 않고도 사건을 원활히 해결하는 방법은 없는가?

A | 개인정보 분쟁조정위원회에 조정신청을 하면 소송절차를 거치지 아니하고 비교적 빠른 시간 내에 분쟁을 해결할 수 있다.

개인정보 분쟁조정위원회는 위원장을 포함하여 15인 이내의 법조계 · 학계 · 소비자 및 사업자단체 전문가 등으로 구성되어 있으며, 분쟁조정 신청이 접수된 경우 사건 접수일로부터 60일 이내에 사실조사 및 양 당사자의 합의를 거쳐 조정결정을 내린다.

개인정보 침해로 인한 분쟁이면 모두 조정대상이 될 수 있으며, 이용자(정보주체)와 사업자가 모두 분쟁조정을 신청할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제33조 (개인정보 분쟁조정위원회의 설치 및 구성) ① 개인정보에 관한 분쟁을 조정하기 위하여 개인정보 분쟁조정위원회(이하"분쟁조정위원회"라 한다)를 둔다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제13조(개인정보 관리책임자의 자격요건 등) ② 분쟁조정위원회는 위원장 1명을 포함한 15명 이내의 위원으로 구성하며, 그 중 1명은 상임으로 한다.

좀 더 알아 봅시다

□ 개인정보 분쟁조정제도의 취지

● 개인정보와 관련한 분쟁을 법원의 소송절차에 의해서만 해결하려면 양 당사자 모두 많은 시간과 비용이 소요된다. 따라서 소송절차를 거치지 않고서도 분쟁을 원활히 해결할 수 있는 '대안적 분쟁해결제도(ADR: Alternative Dispute Resolution)'로서 개인정보 분쟁조정 제도가 운영되고 있다.

□ 개인정보 분쟁조정 절차

● 개인정보 분쟁조정 절차는 다음과 같다.

신청접수	사실조사	조정전 합의권고	조정결정
• 웹사이트, 이메일, 우편, 팩스 등으로 신청접수	• 접수사실 통보 • 사실조사 실시	• 당사자간 자율적 합의 유도	• 접수일로부터 60일 이내에 조정안 제시

□ 개인정보 분쟁조정 효력

● 조정안을 제시받은 날로부터 15일 이내에 양 당사자가 모두 조정안을 수락하는 경우 조정이 성립한다. 이때의 조정결정은 '민사상 합의'의 효력을 지닌다. 반면 당사자 중 일방이라도 조정안을 거부하면 조정은 성립하지 않으며, 이후에는 민사소송을 통해 분쟁해결을 시도하여야 한다.

□ 개인정보 침해신고센터

● 개인정보침해신고센터는 개인정보 침해에 대한 상담 및 고충처리를 위하여 2000년 4월 한국인터넷진흥원(KISA) 내에 설치되었다. 민간 및 공공부문에서 개인정보 침해로 피해를 입은 자는 누구든지 상담 · 고충처리를 문의할 수 있으며, 사업자의 개인정보보호 관련 질의 · 상담도 접수 · 처리하고 있다.

● 개인정보침해신고센터는 원칙적으로 상담의 경우 7일 이내, 고충처리의 경우 30일 이내 처리하고 있으며, 분쟁조정을 원하는 민원인이 있을 경우에는 개인정보분쟁조정위원회에 이관하여 처리하고 있다.

● 개인정보침해 상담 · 고충처리, 기업상담 신청 방법은 아래와 같다.

전 화	국번없이 118 (ARS 3번)
인터넷	www.kisa.or.kr
이메일	118@kisa.or.kr
팩 스	02-405-4729
우편 · 방문	• 서울시 송파구 중대로 135 IT벤처타워 서관 한국인터넷진흥원

개인정보보호법 이렇게 달라집니다

현 재

○ 개인정보 분쟁조정위원회
- 조정결정 효력 : 민사상 합의
- 구성 : 위원장 1인 포함 15인 이내 (상임위원 1인 포함)
- 위원 임기 : 3년 (연임가능)

(정보통신망법 제33조~제40조)

○ 개인정보 침해신고센터
- 소관업무: 개인정보침해 관련 고충처리
- 소속기관: 한국인터넷진흥원

(정보통신망법 제52조)

법 제정후

○ 개인정보 분쟁조정위원회
- 조정결정 효력 : 재판상 화해 (조정결과에 대해 강제집행력 인정)
- 구성 : 위원장 1인 포함 20인 이내 (상임위원 1인 포함)
- 위원 임기 : 2년 (1회 연임가능) (개인정보보호법 제40조~제50조)

○ 개인정보 침해신고센터
- 소관업무: 개인정보침해사실 신고
- 소속기관: 전문기관 (전문기관은 행정안전부장관이 지정)

(개인정보보호법 제62조)

본서를 만들기 위해 다음과 같은 분들이 수고하셨습니다.

총괄책임	행 정 안 전 부	개인정보보호과			
집 필	한국인터넷진흥원	개인정보안전관리팀	팀	장	신종회
	한국인터넷진흥원	개인정보안전관리팀	책	임	김민섭
	(주)KISSP		실	장	이재구
	(주)KISSP		선	임	박선아

사업자를 위한 개인정보보호 질의 · 응답집

발 행 처 행정안전부 (http://www.mopas.go.kr)
한국인터넷진흥원 (http://www.kisa.or.kr)

인 쇄 처 호정씨앤피(☎ 02-2277-4718)

〈 비 매 품 〉

※ 본서 내용의 무단전재를 금하며, 인용 시에는 반드시 출처를 행정안전부 · 한국인터넷진흥원 「**사업자를 위한 개인정보보호 질의 · 응답집**」이라고 밝혀주시기 바랍니다.

행정안전부

한국인터넷진흥원
Korea Internet & Security Agency