

목록

[교안] 개인정보보호_1차시	1
[교안] 개인정보보호_2차시	5
[교안] 개인정보보호_3차시	11
[교안] 개인정보보호_4차시	16
[교안] 개인정보보호_5차시	21

1차시. 개인정보, 제대로 알고 있나요?

1. 개인정보란 무엇인가?

최근 5년간 해킹 등으로 인해 5,300만개가 넘는 개인정보가 유출되었다고 합니다. 유출 규모조차 파악이 불가능한 사건까지 합치면 실제 유출된 개인정보는 이보다 더 심각할 것으로 보이는데요. 개인정보 유출 사고도 문제지만, 사후관리도 큰 문제입니다. 보이스피싱과 같은 2차 피해에 노출될 수 있기 때문입니다. 개인정보에 대한 제대로 된 이해와 인식이 필요한 때입니다.

개인정보의 개념에 대해 먼저 알아보시다.

Q. 사망했거나 실종신고 등으로 사망한 것으로 간주되는 사람의 정보는 개인정보가 맞을까요?

A. X

S. 개인정보란 살아있는 개인에 관한 정보로서, 사망했거나 실종 신고 등 법적으로 사망한 것으로 간주되는 자에 대한 정보는 해당하지 않습니다.

Q. 홈페이지에 기재된 기업의 대표자 성명도 개인정보에 해당할까요?

A. X

S. 개인정보는 개인에 관한 정보로서, 법인 및 단체에 관한 정보는 해당하지 않습니다. 법인의 자산 규모나 영업실적 등은 개인정보가 아닙니다.

Q. 'A학교 2018년도 졸업생 취업률'은 개인정보일까요?

A. X

S. 개인정보란 특정 개인을 알아볼 수 있는 성명, 주민등록번호, 영상 등의 정보를 말합니다. 'A학교 2018년도 졸업생 취업률'과 같은 가공되어 있는 정보는 개인정보에 해당하지 않습니다.

Q. 차량번호도 개인정보일까요?

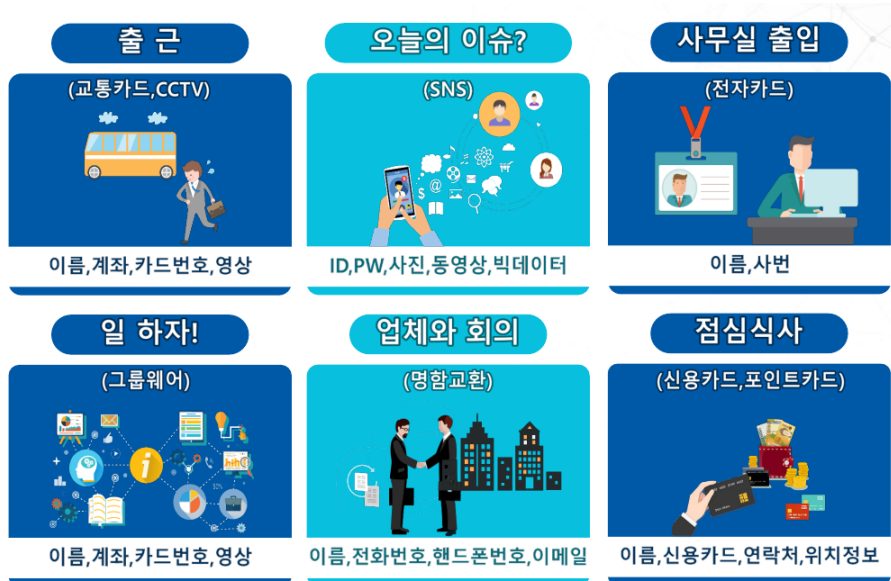
A. O

S. 개인정보에는 다른 정보와 '쉽게 결합하여' 개인을 알아볼 수 있는 정보도 해당합니다. 차량번호 하나만으로는 개인을 식별할 여지가 없더라도 자동차등록원부 등과 결합하면 쉽게 등록자 개인을 식별할 수 있으므로 개인정보입니다.

정리해보면, 개인정보란 ① 살아있는 ② 개인에 관한 정보로서 ③ 특정 개인을 알아볼 수 있는 성명, 주민등록번호, 영상 등의 정보, ④ 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보를 뜻한다는 것을 알 수 있었습니다.

개인정보는 우리의 일상생활속에서 쉽게 찾아볼 수 있습니다.

예시: 회사원A씨



2. 개인정보의 유형

일반적 정보	• 주민등록번호 • 이름, 주소, 전화번호
신체적 정보	• 신체 정보 • 의료, 건강정보
정신적 정보	• 기호, 성향 • 신념, 사상
재산적 정보	• 개인 신용정보 • 부동산, 주식
사회적 정보	• 교육정보 • 근로 정보 • 자격 정보
기타 정보	• 통신정보(통화, 로그파일, 이메일, 문자 등) • 위치정보(IP, GPS 등) • 병역정보 • 화상정보(CCTV)

3. 개인정보보호의 필요성

사례1. A항공사에서 간부급 직원이 예약 도중 말다툼을 한 여성 고객의 정보를 조건만남 사이트 등에 유출한 사고가 발생하였습니다. 이는 개인정보를 처리하는 내부직원이 피해자와 업무 도중 말다툼을 하였고, 해당 피해자의 정보를 유출한 사례입니다. 해당 고객은 이후 알 수 없는 문자와 연락에 시달려야 했다는데요. 결국 정보를 유출한 내부직원은 개인정보보호법 위반으로 처벌을 받게 되었고, A항공사는 이미지에 매우 큰 피해를 입게 되었습니다. 이처럼 개인정보 노출로 인해 피해자가 입은 개인적인 피해는 물론이거니와 A항공사도 이미지 실추라는 큰 타격을 입었습니다.

(1) 개인적 가치 및 보호의 필요성

개인은 자신에 관한 정보의 수집 · 이용 · 공개 · 제공 등을 본인이 통제할 수 있는 권리(개인정보 자기결정권)를 가지고 있음에도 불구하고, 개인정보 유출로 인해 명의를 도용당하거나, 보이스피싱과 같은 금전적 손해를 입는 등 각종 범죄에 노출될 수 있습니다.

(2) 기업적 가치 및 보호의 필요성

개인정보는 기업의 영업자산으로서 고객의 정보를 수집 활용하여 영업활동 및 수익을 창출하는 기반이 됩니다. 따라서 개인정보보호를 위한 노력은 비용이 아닌 투자라고 볼 수 있습니다. 사건에서처럼 개인정보 유출사고 발생 시 기업의 이미지가 실추되는 것은 물론이고, 소비자 단체 등의 불매운동으로 이어지며, 다수 피해자에 대한 집단적 손해배상시 기업 경영에 큰 타격을 줄 수 있습니다.

(3) 사회적 가치 및 보호의 필요성

개인정보는 사회의 핵심요소로서 공공 · 민간 서비스 · 기업경영 등 대부분의 사회활동이 개인정보를 기반으로 이루어져 있습니다. 국가적으로는 중요한 정보가 유출되었을 때, 금융·교통·에너지 등 사회적 기능이 마비되고 재난으로 발전할 가능성이 있습니다. 뿐만 아니라 IT강국이라는 대한민국의 이미지가 손상되고, 국가의 신뢰성이 하락하고, IT 산업의 수출이 어려워질 수 있습니다.

4. 개인정보 이해관계자

개인정보를 다루는 사람은 개인정보와 관련한 역할에 따르는 책임과 의무, 권리를 이해해야 합니다. 이러한 역할은 서로 중복되기도 하며, 상충하기도 합니다. 그래서 우리는 개인정보 이해관계자에 대해 이해함으로써 각 역할에 해당하는 책임과 의무, 권리를 분명하게 이해할 필요가 있습니다.

니다.

개인정보와 관련된 이해관계자는 4가지로 분류해 볼 수 있습니다. 먼저 개인정보보호법의 보호대상인 정보주체가 있습니다. 정보주체는 개인정보에 대하여 자기결정권을 가지고 있는 대상을 말하는데요. 개인정보 자기결정권이란 개인정보 주체인 개인이 해당 정보가 언제 수집되어, 어느 용도로 사용되고 있으며, 어느 범위까지 이용할 수 있는지를 스스로 통제하고 결정할 수 있는 권리를 말합니다. 정보보호의 개념은 시간에 따라 조금씩 달라지고 있는데요. 과거에는 개인의 사적인 생활을 남에게 방해 받지 않을 권리인 프라이버시가 중요한 요소였다면, 현재는 개인정보의 가치가 증가함에 따라 정보주체인 개인이 자신에 관한 정보를 적극적으로 관리하고 통제하기 위한 권리가 중요시 되고 있습니다. 여기서 중요한 것이 바로 개인정보에 대한 자기결정권이라고 하겠습니다.

이어서 개인정보 취급자가 있습니다. 개인정보 취급자는 개인정보처리자의 지휘·감독을 받아 개인정보를 실제로 처리하는 여러 종류의 직원(임직원, 파견근로자, 시간제근로자, 인턴 등)을 말합니다. 다음으로 개인정보처리자가 있습니다. 이는 업무를 목적으로 개인정보를 처리하는 개인·기관·법인·단체 등이 될 수 있습니다. 마지막으로 개인정보보호책임자가 있습니다. 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말합니다.

정보주체는 누구인지 한번에 이해가 가능하지만 개인정보취급자와 개인정보처리자는 같은 사람이라고 생각하기 쉽습니다. 개인정보 처리업무에 대한 감독의 권한을 갖는 자가 개인정보처리자와 개인정보보호책임자가 될 수 있고, 개인정보처리자의 감독을 받아 개인정보 업무를 처리하는 임직원이 개인정보취급자가 될 수 있습니다.

공공기관이나 규모가 큰 법인의 경우 개인정보처리자와 개인정보보호책임자 및 개인정보취급자를 별도로 두어 운영을 하고 있으며, 상대적으로 규모가 작은 기업에서는 동일한 직원이 처리하기도 합니다. 하지만 이들의 업무는 다르기 때문에 구분해서 이해하셔야 합니다.

2차시. 개인정보보호법, 어렵지 않아요!

1. 개인정보보호법이란?

2009 년 12 월 A 씨는 B 금융회사의 전자상거래 홈페이지에 가입하며 제 3 자 제공 동의란에 동의하지 않았음에도 불구하고 보험사의 텔레마케팅 전화를 받게 되었고, 보험사에게 문의한 결과 전산담당자의 실수로 인한 개인정보의 제공이 있었다고 답변을 하였음. 이에 대하여, A 씨는 개인정보 분쟁조정 위원회에 정신적 손해배상을 요구하는 분쟁조정을 신청함.

위와 같은 경우 정보통신망법과 전자상거래법, 전자금융거래법 등 다양한 유관법률 등이 중복적용되며 충돌할 소지가 있어 개인정보 분쟁 조정 위원회에서 분쟁 조정하는데 다양한 애로사항이 있었음.

(1) 개인정보보호법 제정배경

그동안 체계화되지 못하고 일원화되지 못했던 개인정보와 관련된 법령체계를 일원화하고 개개인의 자기정보보호 및 권익보호를 강화하기 위해 개인정보보호법이 제정되었으며 2011 년 9 월 30 일 시행되었습니다. 개인정보보호법이 제정되기 전에는 각 분야별 적용되는 개별법이 존재하였으며, 그 법의 적용 대상이 한정되어 있었으나, 개인정보보호법 제정 후 개인정보를 처리하는 모든 기업, 기관, 단체, 개인에게 적용됨으로써, 그동안의 법의 사각지대에 놓여 있던 기관과 사업자들이 새롭게 이 법의 적용 대상으로 편입되었습니다

(2) 개인정보보호법 적용 후 바뀐점

가. 보호 의무 적용대상의 확대

나. 보호 범위의 확대

다. 고유식별정보 및 민감정보 처리 제한

라. 영상정보처리기기 규제

마. 개인정보 수집 · 이용 · 제공 기준

바. 정보주체의 자기 정보결정권 및 권리행사 강화

사. 개인정보 유출 통지 및 신고제 도입

아. 위반시 처벌 및 벌칙 강화

(3) 개인정보보호 원칙(글로벌 개인정보보호 흐름(OECD)을 반영)

OECD 프라이버시 8 원칙의 영향을 받아 개인정보보호법에는 다음과 같은 원칙을 준수하여 제정되었습니다.

- 처리 목적의 명확화, 목적 내에서 적법하고 정당하게 최소 수집
- 처리 목적 내에서 처리, 목적 외 활용 금지
- 처리 목적 내에서 정확성, 완전성, 최신성 보장
- 정보주체의 권리침해 위험성 등을 고려하여 안전하게 관리
- 개인정보 처리사항 공개, 정보주체의 권리보장
- 사생활 침해 최소화 방법으로 처리
- 가능한 경우 익명 처리
- 개인정보처리자의 책임 준수, 정보주체의 신뢰성 확보

2. 개인정보 생명주기

기업이 개인정보를 효과적으로 보호하기 위해서는 개인정보 및 개인정보 보호에 대한 체계적이고 종합적인 분석이 선행되어야 합니다. 복잡한 개인정보를 가장 효율적으로 이해하는 방법 중 하나는 개인정보가 수집되어 DB에 저장·이용·파기되는 전체 프로세스를 분석하는 것인데요. 이러한 방법 중 가장 대표적인 방법이 개인정보 생명주기이며, 기업의 개인정보 보호 대책 수립, 영향평가, 인증, 컨설팅, 내부 관리 계획의 수립 등에 아주 유용하게 활용할 수 있습니다.

개인정보는 사람의 일생처럼 일련의 생명주기를 가지고 있으며, 기업, 기관 등 개인정보처리자가 개인정보 소유자의 개인정보를 수집하고 이를 저장, 관리 및 제 3 자에게 제공하며, 개인정보 보유기간이 종료된 이후 해당 개인정보를 파기하는 일련의 개인정보 관리의 단계를 개인정보 생명주기(Lifecycle)이라 한다. 개인정보생명주기는 총 4 단계를 거치게 되며, 각 단계별로 개인정보보호법에 따라 관리되어야 합니다.

(1) 수집

먼저 수집단계입니다. 개인정보의 '수집'이란 정보주체로부터 이름·주소·전화번호 등의 개인정보를 제공받는 것 뿐 만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말합니

다. 개인정보의 수집 및 이용이 가능한 경우는 동의를 받거나 법률에 의한 규정이 있는 경우를 포함하여 정보주체와의 계약의 체결과 이행을 위해 불가피한 경우에 가능합니다. 추가적으로 급박한 생명·신체·재산의 이익을 위해 필요하거나 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로 제한됩니다.

업무수행을 위해 필요한 개인정보를 수집하려면 수집근거를 명확하게 하고 수집사실이 안내되어야 하는데 그것이 바로 개인정보동의서입니다. 마트에서 이벤트를 한다거나 온라인에서 회원가입을 할 때 동의함이라는 곳에 체크하셨을 겁니다. 하지만 많은 사람들이 어떤 내용인지 읽어보지 않고, 전체 동의에 체크하는 실수를 범하게 되는데요. 여러분들은 어떠셨나요? 그동안 동의서에 체크만 하지 않으셨나요? 지금부터는 동의서에 어떤 내용이 적혀 있는지 알려드리도록 하겠습니다. 개인정보 수집 시 동의 내용은 '개인정보의 수집 이용목적, 개인정보의 항목, 보유 및 이용기간, 수집 동의 거부 권리, 필수정보와 선택정보로 나누어 수집' 이러한 내용들이 포함이 되어 있으며, 거부할 경우 발생할 수 있는 불이익도 고지합니다. 개인정보를 수집함에 있어 중요한 것은 최소 수집의 원칙입니다. 서비스 제공에 필요한 최소한의 개인정보만을 수집하여야 하며, 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보로 제한되어야 합니다. 최소 정보 외의 정보를 제공하지 않는다고 해서 서비스를 제공하지 않을 수는 없으며, 추가적인 정보를 수집할 때 선택동의 항목으로 구분해야 합니다. 개인정보동의서에 동의를 하지 않더라도 일반적인 서비스는 제공하도록 되어 있으니 참고하시구요. 만 14세 회원 가입시에는 법정대리인의 동의가 필요하다는 점도 기억해 두세요 그 외 다양한 매체 등을 이용해서 개인정보를 수집할 때는 제공받은 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정하는 범위 내에서만 수집 및 이용이 가능합니다.

<최소 수집의 원칙 위반 사례>

2014년 9월, 대형 유통업체 H사는 경품행사를 통해 다양한 개인정보를 수집한 뒤, 1mm 크기 글씨로 개인정보 이용 동의를 고지하고 보험사에 고객의 정보를 팔아 넘겨 230억이 넘는 수익을 획득한 혐의로 재판에 넘겨지는 사건 발생, 대법원에서 최종 유죄로 확정된 사례 : H회사는 경품응모권을 통해 성별, 자녀 수, 동거 여부 등 사생활 관련 정보와 주민번호 등 고유식별 정보까지 수집하면서 이를 제공하지 않으면 경품 행사에 참여하지 못한다고 한 점과 정당한 목적으로 수집하는 경우라고 해도 최소한의 정보에 그쳐야 한다는 개인정보보호법 원칙과 규정을 위반한 것이라고 판단, 또한 동의 관련 사항은 1mm 크기 글씨로 기재해 소비자가 읽기 쉽지 않게 의도하여 개인정보보호사업자가 마땅히 준수하여야 할 '고지의 의무'를 지켰다고 볼 수 없다고 보고 유죄로 판결함

참고로 주민등록번호 유출 및 오남용의 사례가 빈번함에 따라 2014 년에 개인정보보호법이 개정되었는데요. 개정의 내용으로는 주민등록번호의 수집을 제한하고 온라인 회원 가입 시

PIN 번호나 공인인증서 등의 다른 방법으로 가입을 유도하도록 되어 있습니다. 만약 온라인 회원 가입시에 주민등록번호를 요구하는 사이트가 있다면 위법이기 때문에 신고하실 수 있습니다.

(2) 이용·저장·관리

두번째로 이용·저장·관리단계입니다. 개인정보를 가지고 있는 모든 개인이나, 기관, 단체는 보유하고 있는 개인정보에 대한 안전한 관리의 의무가 있는데요. 개인정보를 관리하는 개인정보관리자를 지정되어야 하고, 목적 외 사용을 금지합니다. 업무수행을 위해서 필요한 범위안에서만 개인정보보호 파일을 보유 해야하고 개인정보를 보관하기 위해서 기술적, 관리적, 물리적으로 안전조치를 해야합니다. 정보주체가 원할 경우에는 열람·정정·삭제를 할 수 있습니다.

<저장관리단계의 위반 사례>

1. A 대학교 합격자 발표시 이름, 주민번호, 전화번호가 한꺼번에 공개되었던 사례
2. B 회사의 인사팀에서는 개인정보가 들어있는 문서를 단체 메일로 송신하는 사례

개인정보가 단 1%라도 들어있는 자료는 각각 수신인을 지정해서 발송하도록 해야하고, 개인정보가 유출되지 않도록 철저하게 관리하여야 합니다.

<목적 외 이용 위반 사례>

A 주민센터에서 민원업무를 담당하던 B 씨가 동생 배우자의 신원확인을 위해 혼인관계증명서를 임의대로 열람한 사례

(3) 제공·위탁

세번째로 제공·위탁단계입니다. 개인정보를 위탁하는 경우가 있고 제공하는 경우가 있는데요. 두 단어가 비슷하지만 누구의 이익을 위해 정보를 사용하는지에 분명한 차이가 있습니다. 개인정보 위탁은 위탁자의 이익을 위해 사용하는 것이고, 제3자 제공의 경우 제공받는 자의 이익을 위해 사용하는 것입니다.

	제 3자 제공 (법 제 17조, 제18조)	위탁 (법 제26조)
처리 목적	제공받는 자의 이익/목적	제공하는 자의 이익/목적
관리범위	제공받는 자의 책임	제공하는 자의 책임
예시	▶ 경찰에 수사자료로 제공 ▶ 감사기관 (수사 수행 목적) 등에 감사자료로 제출 ▶ 마트 이벤트 고객정보를 보험회사 마케팅에 제공	▶ 민원 처리 만족도 조사를 위해 리서치 업체에 직원 정보 제공 ▶ 직원 교육을 위해 교육 위탁업체에 직원 명단 제공 ▶ SNS를 통한 홍보를 위해 고객의 전화번호를 문자발송 업체에 전달

개인정보의 제3자 제공 및 처리위탁은 개인정보처리자가 업무수행을 위해 특정 목적으로 정보주체로부터 동의를 받고 개인정보를 이용하는 행위로 정보주체의 별도의 동의가 반드시 필요합니다. 개인정보를 제공할 경우 처음 제공할 때와 동일하게 제공받는 자에 대한 정보 · 목적 · 항목 · 기간 및 거부에 따른 불이익의 내용을 정보주체에게 고지하여야만 합니다. 참고로 제3자 정보제공 외 별도의 동의가 필요한 항목으로는 목적 외 이용 및 제공, 민감정보 수집, 주민등록번호를 제외한 고유식별번호 수집, 마케팅 및 서비스 홍보 권유가 있습니다. 과거의 경우 필수적인 내용에 대해서 동의를 받으면서 마케팅과 관련된 부분을 함께 포함해서 동의를 받는 사례가 많았습니다. 이 경우에 한번에 동의를 받는 것이 아니라 서비스 제공에 필요한 동의는 기존과 동일하게 받고, 선택사항에 대해서는 사용자가 정확하게 인지할 수 있게 표시하고 선택적으로 동의를 받아야 합니다. 개인정보를 취급함에 있어 별도 동의가 필요한 부분인지 기존 동의로 제공이 가능한지 숙지가 필요합니다.

개인정보를 제3자에게 위탁했는데 수탁자의 불법행위로 인한 손해배상의 문제가 발생이 되면 수탁자는 위탁자의 소속직원으로 간주가 됩니다. 수탁자에 대한 개인정보보호 교육과 관리감독은 위탁자의 책무이기도 합니다. 또한 위탁시에 개인정보보호 의무사항을 문서화하는데 그 내용에 손해배상 등 책임에 관한 사항을 명시하는 것이 좋습니다. 수탁자는 개인정보를 안전하게 보호하기 위한 조치를 이행 해야하고, 수탁 업무 목적 외 개인정보 이용을 금합니다.

<제 3 자 제공 위반 사례>

A 회사의 직원은 그 회사의 직원만이 이용할 수 있는 직원용 제품 할인 구매사이트의 아이디와 패스워드를 지인에게 알려주고 사용하게 하였으며, 그 지인의 지인들까지도 해당사이트의 물건을 저렴하게 구매하는 사건 발생

(4) 파기

마지막으로 정보 파기 단계입니다. 개인정보는 보유기간이 경과하거나 목적 달성 후 5 일 이내에 파기하도록 규정되어 있는데요. 개인정보보호책임자는 개인정보를 파기한 이후에 결과를 직접 확인해야 합니다. 파기 사실을 대장으로 기록관리하고 개인정보 파일을 파기할 경우 개인통보나 웹사이트로 안내되어야 합니다. 파기 후에는 개인정보가 복구나 재생이 되지 않도록 관리해야 합니다. 출력물은 파쇄나 소각으로 처리해야 하고 전자적 파일은 복원이 불가능한 방법인 포맷이나 삭제용 소프트웨어를 이용해서 삭제해야 합니다. 많은 회사에서 사용 완료된 출력물이 있을 때 이면지로 활용하는 경우가 많은데 이면지 활용은 하지 않는 것이 좋습니다. 만약 이면지에 아주 작은 개인정보라도 있을 경우에는 파기하는 것이 원칙입니다. 법령의 근거에서 파기하지 않고 보존해야 하는 경우에는 물리적 또는 기술적 방법으로 다른 개인정보와 분리하여 저장·관리하여야 합니다. 일반적으로 테이프를 백업을 하거나 별도의 네트워크로 분리된 곳에 백업을 진행합니다.

사용자가 정보통신서비스를 1년 동안 이용하지 않는 경우에는 해당기간 경과 시 개인정보를 파기하거나 분리하여 저장해야 합니다. 유효기간 만료 30일 전에는 해당 개인정보가 파기되거나 분리된다는 사실을 이용자에게 고지해야 합니다. 이 과정에서 여러 법령에 의해 특정기간 보존의무가 있는 경우에는 파기하지 말고 보존해야 합니다. 예를 들어 대금결제 및 재화 등의 공급에 관한 기록은 5년간 보존해야 합니다.

3차시. 개인정보 유출사고, 이렇게 대응하세요!

1. 개인정보 유출의 개념

개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것을 뜻합니다. 개인정보가 포함된 디바이스를 분실하거나, 접근권한이 없는 사람이 DB에 접근을 하거나, 고의 또는 과실로 개인정보가 외부로 전달되거나 하는 경우를 말합니다. 개인정보의 노출은 유출의 한 부분으로 볼 수 있습니다.

<개인정보가 포함된 디바이스 분실 사례>

C회사의 직원 A씨는 자신의 차에 고객정보가 있는 서류를 가지고 다니다가 잃어버림

<과실로 개인정보가 외부로 전달된 사례>

회사원 A가 B업체 담당에게 상품안내 메일을 보내면서 실수로 고객의 개인정보가 포함된 리스트를 상품안내 이메일에 첨부하여 발송함

2. 개인정보 유출사고의 원인

개인정보가 유출되는데에는 여러가지 이유가 있겠지만 첫번째 이유는 인터넷과 모바일 정보통신기술의 발전되었기 때문입니다. 발달된 기술때문에 오히려 중요한 정보가 쉽게 유출되고 있는 것입니다.

두번째 이유는 개인정보의 가치가 크게 증가하고 있기 때문입니다. 개인정보 수집이 관행화되어 있어 불필요한 수집이 많으며, 특히 수집된 정보 중 마케팅을 위한 개인정보는 수요가 크게 증가하여 금전적인 거래로 이어지는 경우가 빈번히 발생하고 있습니다.

세번째 이유는 우리의 불안정한 행동 때문입니다. 최첨단 기술을 이용하면서 인지하지 못했던 여러가지 불안정한 행동으로 정보가 유출되고 있는 것입니다.

<불안정한 행동 예시>

- 개인정보나 주요 비공개 자료가 포함된 공문서를 안전조치 없이 시행
- 회의 과정에서 습득한 주요 정보를 외부에 전달하고 공개하는 행위
- 홈페이지에 주민등록번호 등 주요 자료를 게재하는 행위
- 고객정보를 업무상에 협조 과정에서 다른 직원에게 무단 제공하는 행위
- 주요 자료가 담긴 파일을 부주의로 다른 기관의 담당자에게 송수신하는 행위
- PC 공유 폴더 내에 스캔 된 개인정보 등의 주요 자료를 방치하는 행위

- PC 접속 비밀번호를 모니터나 키보드 하단에 부착해서 사용
- 암호화 조치되지 않은 주요 자료가 담긴 USB 나 외장하드를 분실하는 행위

네번째 이유는 개인정보를 보호해야 하는 중요성에 대한 인식 부족입니다. 개인정보보호를 위한 투자 및 관리를 제대로 하지 못하고, 이로 인해서 기술적 · 관리적 보호조치가 미흡하여 해킹사고의 원인이 되기도 합니다.

3. 개인정보 유출사고의 유형별 예시

(1) 내/외부 인력에 의한 개인정보 유출

- 정유사 회원정보 관리를 담당하는 자회사 직원이 개인정보 판매 목적으로 고객정보 1,125 만건 유출
- A 시 공무원 2 명이 시립묘지 연고자 6,449 명의 개인정보를 장묘 업체 관계자에 유출
- 교육청 장학사가 교육의원에 출마한 후배를 위해 관내 교직원 3,000 명의 이름, 전화번호 등 유출

(2) 영리 목적을 위한 개인정보 매매

- 주민센터 직원이 심부름센터 등에 건당 만원씩 받고 개인정보 판매
- 택배회사 영업소장이 자사와 거래하던 홈쇼핑 업체의 고객정보 2 백만건을 빼돌려 텔레마케팅 업체에 판매

(3) 무분별한 개인정보 오/남용

- 차량등록시스템에 있는 차량번호, 주민번호, 이름 등 150 명의 정보를 다른 공무원으로부터 건네받아 개인적 목적으로 사용

(4) 허술한 관리에 의해 홈페이지 노출

- 민원인 수백명의 이름, 주민번호, 주소 등 개인정보가 포함된 보도자료를 인터넷 홈페이지에 공개

(5) 기업 및 담당자의 미흡한 관리 및 방치

- 모 공단 직원이 고객정보 10 만 건이 기록된 서류 미 파기 및 차량 방치
- 은행 직원의 부주의로 고객의 개인정보가 포함된 리스트를 상품안내 이메일에 첨부하여 발송

4. 개인정보 유출사고의 대응

(1) 개인의 대응방안

기업의 경우를 먼저 살펴보겠습니다. 기업이라면 가장 먼저 하셔야 되는 것이 긴급대응팀 소집을 통해서 빠른 조치를 하시도록 하는 게 중요합니다. 긴급대응팀은 소집되지 마자 왜 이 사고가 발생했는지 유출원인을 파악하고 추가적으로 혹시 개인정보가 유출이 되고 있는지를 파악을 해서 추가 유출이 되고 있는 것 같다면 이를 차단하는 작업을 해야만 하고요. 그리고 개인정보가 유출된 사실, 침해가 발생한 사실을 정보주체에게 통지해 주어야 합니다. 왜 정보주체에게 통지가 필요하냐 하면 추가적인 2 차 사고를 예방하기 위해서 빠른 통지가 되어야 하기 때문입니다. 정보가 유출이 되었습니다. 고객 정보가. 누구의 정보냐 하면 이용자의 정보죠. 그리고 그 이용자의 정보가 유출된 것이 어떤 게 유출됐는지 모르는데 혹시라도 비밀번호라든지 관련된 내용이 들어있다면 보이스피싱 피해나 계좌로부터의 인출 피해나 다른 사고로 이어질 수 있습니다. 따라서 빨리 정보주체에게 통보를 해서 혹시라도 발생할 수도 있는 2 차 피해를 정보주체가 스스로 차단할 수 있도록 하는 작업이 필요합니다.

또한 긴급대응팀은 침해된 사실을 행정안전부와 KSIA 등 정부기관에 통지해야 하고요. 왜 통지를 해야 하나면, 이러한 기관들이 발생한 침해사고에 대해서 자체적인 또는 외부적으로 이슈가 될 사항에 대응할 시간을 주기 위해서입니다. 이러한 정보기관들이 빨리 인지하고 대응하지 못하고 언론이나 외부로부터 듣고 대응하게 되면 문제가 될 수 있기 때문에 빨리 준비할 수 있도록 빨리 통지를 해주는 게 중요하고요.

그리고 혹시라도 범인을 검거하거나 범인이 유출해 간 정보를 회수할 수 있는 가능성을 극대화하기 위해서 수사 기관에 수사를 요청하는 것이 필요합니다.

이 세가지 작업을 하는데 있어서 가장 중요한 것은 이 작업들이 유출사실을 기업이 탐지하고 24 시간 이내에 수행되어야 한다는 겁니다. 의문을 가지실 수 있습니다. '개인정보보호법에서는 정보유출 사실을 탐지하고 5 일 이내에 통지하도록 되어 있는데 왜 24 시간이라고 하지?'라고 의문을 가지실 수 있습니다. 개인정보보호와 관련된 법은 개인정보보호법과 정통망법이 있습니다. 개인정보보호법에서는 5 일 이내라고 되어 있지만 정통망법에서는 24 시간 이내로 명시하고 있죠.

이 둘 중에 무엇을 지켜야 하느냐? 대부분의 많은 기업들이 개인정보보호법에도 적용이 되고 정보통신망법에도 적용이 되는 경우가 대다수입니다. 따라서 이 둘 중에 통지시간이 짧은, 24 시간 기준에 맞추어서 이 세가지 작업을 하실 수 있도록 긴급대응팀이 사전에 훈련하고 준비하는 것이 필요합니다.

또 기업의 경우에는 이 앞선 작업들을 하고 난 이후에 빠르게 정보주체가 유출여부 확인이 가능하도록 홈페이지를 구성을 해서 정보주체가 내 정보가 정말 유출된 게 맞는지, 혹시 나는 통지를 못 받았는데 정보가 유출되었다고 하니 혹시 나도 있는지, 또는 어떤 정보가 또 유출이 됐는지를 정확히 확인할 수 있도록 웹 홈페이지를 구성을 해서 제공해야 합니다. 이 과정에서 중요한 것은 정보주체가 내가 유출되었는지 확인을 하는데 주민번호를 통해서 확인하도록 하면 되지 안 된다는 겁니다. 주민번호는 법에서 정해진 경우에만 사용하도록 되어 있기 때문에 본인 여부를 확인하기 위해서 주민번호를 쓰거나 하면 또 법을 어기는 경우가 발생하기 때문에 반드시 주민번호가 아닌 다른 경로를 통해서 본인확인을 하도록 구현하셔야 합니다. 그리고 긴급대응팀이 할 가장 중요한 일 중에 하나는 사고 피해자에 대한 빠른 보상방안을 마련해서 공지하는 겁니다. 적절한 보상기준을 어떻게 마련하고 공지하느냐에 따라 정보유출 사고를 당한 정보주체들이 그 이후에 어떻게 움직이는가를 큰 영향을 줄 수 있기 때문에 빠른 보상방안을 마련해서 공지할 필요가 있고요. 그리고 긴급대응팀은 사고 처리완료 시까지 대응체계를 유지하는 것이 중요합니다.

(2) 개인의 대응방안

그러면 개인의 경우에는 '실제로 피해가 났다, 내 정보가 유출이 되었다.' 그러면 어떻게 대응해야 될까요? 개인이 기업으로부터 정보유출 통지를 받았을 때는 먼저 어떤 정보가 유출이 되었는지를 확인해야 됩니다. '얼마나 중요한 정보가 외부로 유출이 됐는지, 나와 관련된'. 그리고 이를 통해서 '혹시 이 사이트나 기업 말고, 다른 사이트에 개인정보가 추가로 유출될 가능성이 있나?' 하는 것을 확인해 보실 필요가 있습니다. 그래서 혹시라도 유출 가능성이 있다고 한다면 관련 사이트에 접속해서 비밀번호를 변경하시고 하는 작업을 하실 필요가 있고요. 그리고 기업이 이 사고와 관련해서 어떤 보상을 하는지, 어떻게 공지를 내는지를 주시하실 필요가 있습니다. 피해자들에게 기업이 '적절한 보상과 적절한 대응을 하겠다.'고 라고 공지를 하고 알려준다면 사건이 그거에 맞춰서 거기서 마무리가 될 수도 있을 것이고요. 진행사항에 따라서는 기업이 보상 여부도 알리지 않고 그냥 무대응으로 일관한다거나 할 때는 단체 소송으로 진행될 수 있기 때문에 기업의 향후 대응방안을 예의 주시하실 필요가 있습니다.

<기타>

- 개인정보 유출 확인 : e 프라이버시 클린서비스, Msafer
- 개인정보 피해구제 제도
- 개인정보 침해신고상담 : 118 번, 개인정보침해신고센터 등

- . 개인정보분쟁조정(비슷한 유형으로 다수의 피해자 발생시) : 개인정보분쟁조정위원회
- . 민사소송 : 손해배상 청구

4차시. 개인정보유출, 막을 수 있습니다!

1. 최근 발생한 개인정보 침해 사건

(1) 유명 숙박 앱 서비스 W사의 해킹 사건

다음은 유명 숙박 앱 서비스 W사의 사례입니다. W사는 XX어때 라는 앱으로 가장 유명한 업체입니다. 사건의 주요 개요는 이렇습니다. 먼저 해커가 아주 간단한, 여기서 가장 중요한 것은 간단한 해킹, 간단이라는 용어가 중요합니다. 간단한 해킹을 통해서 W사의 XX어때 서비스로부터 개인정보 99만 건, 숙박정보 340만 건 을 빼내서 유출합니다. 그리고 고객들에게 문자 메시지를 보냅니다. 4800건의 문자 메시지 입니다. 그 내용은 이렇게 들어가 있습니다. 'XXX고객님 명동의 OOO에서 일박 뜨거운 XX 하셨나요?' 라든지, 'AAA고객님 어젯밤 어디에서 뜨거운 XX 하셨나요? 즐거우셨습니까? 여기 어때?' 이렇게 되어 있습니다. 이런 문자 메시지가 4800건이나 이용자들에게 보내진 것입니다. 고객들이 얼마나 당황했을까요? 아마 W사는 고객들로부터 날아오는 항의 전화를 대응하느라 업무가 마비되었을 것입니다. 그리고 W사는 해커로 부터 수억 원 상당의 비트코인을 내 놓지 않으면 계속 이런 문자 메시지 를 보냈겠다 라고 하는 협박을 받게 됩니다. 이 사건에서 가장 중요한 것은 해킹을 당할 수 있죠. 어느 기업이나 사고를 당할 수 있습니다. 그런데 간단한 해킹, 초보적인 해킹공격에 무참히 뚫렸다는 것입니다. 해커가 사용한 기법이 일반적으로 해킹을 공부하겠다 라고 하는 초보자가 서점에서 구매해서 공부한, 교과서적인 내용의 앞장 정도에 나오는 초보적인 해킹기법만으로도 이정보를 유출해 갈 수 있었다 라는 것이 이사건의 가장 중요한 내용입니다.

교훈) 숙박 앱 서비스의 W사의 해킹사건은 지속적인 보완점검이 왜 중요한지를 알려주고 있습니다. 평상시에 W사가 보완취약 점검을 지속적으로 하고 그에 대한 조치를 잘했다면 앞서의 사고는 발생하지 않았을 것입니다. 보완이란 불을 막아주는 방화제와 같아서 유사시가 아닌 비상시에 중요한 역할을 하게 됩니다. 따라서 평상시에 보완취약점 점검을 하고 조치를 하는 것이 얼마나 중요한가를 깨달을 수 있습니다.

(2) 국내 최대 포털 사이트의 개인정보 유출 사건

다음으로 국내 최대 포털 사인 N사의 사례입니다. N사가 변호사 모집을 하겠다 라고 공고를 내고 여기에 약 100여 명이 지원을 합니다. N사는 1차 합격자 15명을 선별을 한 후 그들에게 합격통지를 보내기 위해서 메일을 보냈는데 실수로 지원한 대상자 전체의 메시지를 이 15명에게 보내게 됩니다. 즉 100여명의 정보가 15명에게 다 날라간 것입니다. 중요한 것은 그 정보에 지원했던 지원자들의 이름, 생년월일, 학교, 성적 이 상세히 기록되어 있었던 것입니다. 뒤늦게 이 사실을 깨달은 N사는 메일을 받은 담당자들과 접촉을 해서 적절한 보상조치를 하겠다 그리고

피해자들에게도 보상을 하겠다 라고 조치를 했다고 대외적으로 알리고 있습니다. 그런데 이 사건에서 가장 중요한 사실은 N사가 이 사고를 단순 인사담당자의 실수로 처리했다는 것입니다. 그냥 사람 한 명이 어찌다 실수해서 끝난 거다 라고 처리를 한 것이죠. 이게 문제가 되는 이유는 사람은 항상 실수를 할 수 있습니다. 이번 건만이 아니라도 앞으로 또 다른 회사에서라도 인사담당자가 동일한 실수를 할 수 있는데 과연 이 사고가 그냥 한번의 실수다 라고 하고 덮고 가도 되는 것인지에 대한 의문이 남는 것입니다.

교훈) 최대 포털 사인 N사의 사고 유형은 개인정보유출방지가 왜 중요한지를 보여줍니다. 단순히 사람의 잘못으로 N사는 발표를 했습니다. 그런데 사람의 잘못으로 하면 앞으로도 동일한 사건이 계속 발생할 수 있습니다. 사람은 잘못을 할 수 있으니까요. 따라서 개인정보유출방지 솔루션과 같은 방안을 통해서 사람이 잘못을 하더라도 그것까지 방어할 수 있는 보호장비가 필요하다 라는 것을 N사 사고에서 배울 수 있습니다.

(3) 웹 호스팅 업체 D사, 랜섬웨어로 매각되다!

또, D사의 사례를 들 수 있습니다. 웹 호스팅 업체인 D사가 랜섬웨어로 팔린 사례입니다. 2017년 6월에 해커의 해킹을 통해서 153개 서버가 랜섬웨어에 감염됩니다. 그리고 이 랜섬웨어가 6월 10일 일제히 동작해서 5496개의 웹 서비스가 일제히 동작을 중지하게 됩니다. D사는 이 웹 서비스를 정상화하기 위해서 해커와 지리한 협상을 하고 50억을 내놓아라 라고 하는 해커의 요구에 대응해서 13억으로 타결한 후 몸값 지불을 위해 회사를 팔고 그 돈을 해커에게 전달해준 후에 서비스를 복구하는 작업을 시작하게 됩니다. 이 사고는 지금까지 랜섬웨어 관련해서 세계 최대 몸값 사례로 기록되고 있는 사고 입니다.

그런데 이 사고가 단순히 랜섬웨어 감염으로 볼 수도 있겠지만 개인정보 관점에서는 조금 다른 해석이 가능합니다. 5496개의 서비스 안에는 쇼핑몰도 존재하고 동창회 모임도 존재하고 각종 서비스도 있습니다. 그 안에는 많은 개인정보가 있습니다. 이것들이 주인의 관리자의 의도 없이 강제로 암호화 되어 버린 것입니다. 그래서 이용자들이 접속도 못하고 그 안의 자기 정보도 못보고 자신의 정보에 접근도 못하고 택배를 신청했다면 택배가 어떻게 오는지 조회도 못하고 정보주체의 권리가 침해 당한 것입니다. 랜섬웨어 때문이에요. 그리고 이용자뿐만 아니라 이 웹 서비스의 관리자들도 접속을 하지 못해서 업무 처리가 안되어 버립니다. 즉 D사의 사고는 기존에 주로 경험을 했던 해커에 의한 개인정보 유출의 관점이 아니라 랜섬웨어 등 색다른 악성코드를 이용한 납치 형태의 침해, 개인정보의 침해 사건으로 볼 수 있습니다.

교훈) 웹 호스팅 업체인 D사의 사례는 우리에게 타산지석, 다른 기업이 당한 사례를 참고하는 것이 얼마나 중요한지를 보여줍니다. D사는 SK컴즈와 동일한 APT공격에 뚫렸습니다. 차이점은 SK컴즈는 정보를 유출해갔고 D사는 유출하는 대신 서버를 잠갔다는 것입니다. 중요 서버를

관리하는 단말기를 인터넷과 분리해서 운영하는 것이 얼마나 중요한지를 D사 사건에서 볼 수 있습니다. 또 D사 사건을 통해서 개인정보의 침해사고 영역이 기존에 개인정보를 빼내어 가는 형태의 유출에서 이제는 새로운 영역, 개인정보와 중요정보를 잠그는 영역으로 확대가 되고 있다, 그리고 D사 사건에서 해커는 13억 원의 몸값을 받은 상태이기 때문에 유사사고가 앞으로 증가할 수도 있겠구나 라는 교훈을 얻을 수 있습니다. 실제로 동일한 사고가 2017년 11월에 발생한 사례가 있습니다.

2. 개인정보 유출 방지 방안

(1) 기업의 정보유출 방지 방안

개인정보 유출을 막기위해서 기업에서 할 수 있는 일은 무엇인지 알아보시다.

먼저 보안 취약점 점검은 사전에 미리 미리 수행하시기 바랍니다. 적어도 1 년에 1 회 이상은 기업의 웹 서비스나 서버와 같은 시스템에 대한 취약점 점검을 수행하시고, 취약점에 대한 조치의 수행 하시기 바랍니다.

또한 사람은 실수할 수 있다 라는 것을 미리 염두 해 두시고 사람의 실수도 예방할 수 있도록 솔루션 구성을 검토하여야 합니다. 예를 들어 외부로 전송되는 메일에 대해서 그 안에 개인정보, 중요정보가 들어있는지를 점검하는 솔루션이 도입이 되어있었다면 포털N사와 같은 사고는 발생하지 않았을 것입니다. 따라서 사람에 의지하는 것이 아니고 보완 솔루션을 통한 보완 방안을 반드시 강구하셔야 됩니다.

그리고 중요 단말기의 인터넷 차단이 필요합니다. 서버를 관리한다든지, 데이터베이스를 관리한다든지, 계정 또는 개인정보취급자가 사용하는 단말기 등은 반드시 인터넷이 되지 않도록 차단하여야 됩니다. 인터넷 접속 차단만으로도 해커에 의한 정보유출 차단효과를 가져올 수 있기 때문입니다.

또 최근 침해사고에서 지적된 것 중 하나가 업무시간 외에 단말기 전원 차단 이슈입니다. 대부분 해커에 의한 정보유출 작업은 사용자가 컴퓨터를 사용하는 낮 시간이 아니라 사용자가 컴퓨터를 사용하지 않고 퇴근을 한 야간시간 등에 주로 발생하고 있으므로 단말기의 전원을 차단하는 것만으로 해커에 의한 정보유출 작업을 차단하는 효과를 가져올 수 있습니다.

또 기업은 사고추적을 위한 이용로그를 반드시 저장해야 합니다. 사용자가 시스템에 접속을 해서 종료하실 때까지 고객의 고객정보와 관련된 작업을 수행하는 것이 있다면 그와 관련된 모든 작업 로그를 남기셔야 합니다.

또 단말기에 개인정보를 저장할 때는 반드시 암호화하여야 됩니다. 단말기에 내려 받은

개인정보의 경우 DRM을 통해서 암호화하거나 아니면 별도의 암호화 솔루션을 이용하는 작업 등을 통해서 강제 암호화를 적용하셔야 혹시 그 파일을 그 정보를 해커가 유출해 간다고 하더라도 암호화되어서 유명무실하도록 만들 수 있습니다.

또 직원들이 사용하는 USB 등 이동식 저장매체 사용을 통제하셔야 됩니다. 최근 침해사고에서 외주업체 직원에 의해서 USB에 고객정보를 담아서 유출시킨 사례가 있듯이 반드시 내부에서는 등록된 USB만 사용토록 해서 USB나 기타 이동매체를 통해서 정보유출을 시도하는 것을 차단할 필요가 있습니다.

또 기업들은 수탁자 관리감독도 강화하셔야 됩니다. 개인정보를 제공받아서 처리하는 수탁자의 경우에 최근 침해사고와 관련된 정보유출의 주 대상이기도 합니다. 따라서 수탁자와 계약을 할 시에는 계약 시부터 파기까지 개인정보처리의 전 과정을 관리, 감독할 수 있도록 하셔야 되는데, 계약 시 위탁자의 관리, 감독 권한이 제대로 명시되어 있는지 반드시 확인하셔야 되고, 정기적으로 실제로 수탁자에 대한 점검을 시행하셔야 됩니다. 정기적으로 수탁자에 대한 점검을 수행한 것 만으로도 '위탁자가 수탁자에 대해서 개인정보를 잘 처리하는지를 실제로 감독한다'라는 주의 효과를 줘서 정보유출을 차단하는 효과를 가져올 수 있고요. '주요 처리단계, 수탁자가 위탁자로부터 개인정보를 제공받아서 처리하는 주요 처리단계, 수집이나 이용, 또는 파기까지 각각에 대해서 제대로 수행하고 있다'라는 것을 자료를 증빙을 받아서 접수해서 관리하실 필요가 있습니다.

(2) 개인의 정보유출 방지 방안

그럼 개인은 개인정보유출과 관련해서 어떤 것들을 주의해야 할까요? 최근의 사례를 통해서 보면은 약 11 가지 정도를 주의하실 필요가 있습니다. 먼저 개인의 경우, 개인정보를 기업에게 제공할 경우에 그 약관이나 수집의 목적을 꼼꼼히 점검해보실 필요가 있습니다. 혹시라도 수집의 목적에 맞지 않는 과도한 개인정보를 요구하고 있지는 않은지 보셔야 되고요. 그리고 개인의 경우 비밀번호를 생성할 때 본인의 주변정보를 사용하는 건 금지하셔야 됩니다. 많은 경우 개인들은 비밀번호를 생성을 할 때 본인의 주민번호라든지, 가족의 주민번호, 또는 가족, 본인의 생일 등 쉽게 연상할 수 있는 정보를 가지고 비밀번호를 만드는 경우가 많이 있습니다. 그리고 이러한 경우 해커에 의해서 쉽게 유추돼서 그 비밀번호가 유출될 가능성이 높기 때문에 이러한 정보는 사용하지 않으면 안 되고요. 가급적 비밀번호를 만드실 때는 유추하기 불가능한 형태로 생성을 하셔서 이 비밀번호를 여러 사이트에서 따로따로 만들기가 어려워서 하나의 비밀번호로 사용하고 계시다고 하더라도 해커가 유추하기 어려운 형태로 만들었다면 그런 형태로 만들어서 사용하시는 것이 더 적합할 것입니다.

또한 개인의 경우에는 혹시 내 개정으로 누군가가 접속한 흔적이 있는지를 반드시 살펴보실 필요가 있습니다. 많은 경우 시스템들이 온라인 시스템, 홈페이지의 경우에도 이전에 언제 접속했는지에 대한 일, 시 정도는 제공하는 경우가 많이 있습니다. 마지막 접속, 몇 월, 몇 일, 몇 시. 이렇게 제공하는 경우가 많이 있기 때문에 이전의 접속 내역을 꼭 확인하시고 '이게 내가 접속했던 것이 맞나? 이때 내가 접속하지 않았는데 접속한 내역이 있네?'라고 조금이라도 의심이 된다면 바로 비밀번호를 변경하셔서 누군가 내 비밀번호를 가지고 접속을 해서 다른 행위를 할 수 있는 가능성을 차단하는 것이 필요합니다. 또한 스마트폰이 일상화되다 보니 많은 정보가 유출이 되고 있는데 소셜 미디어에 자신이나 가족의 정보를 게시하시면 안됩니다. 특히 주민번호나 연락처 같은 경우에 절대 올리지 않도록 주의를 하실 필요가 있고요.

또 개인이라고 하더라도 중요 정보에 대해서는 분실할 경우를 대비해서 보안 USB 를 사용하시는 것이 좋습니다. 최근에는 담겨진 파일에 대해서 자동으로 암호화를 해주는 저렴한 보안 USB 가 많이 판매되고 있으므로 일반 USB 말고 이러한 보안 기능이 있는 USB 를 사용을 해서 혹시라도 USB 를 분실하더라도 정보가 유출될 가능성이 없도록 하시는 것이 필요하시고요. 또 스마트폰에 불필요한 앱 설치하는 자제하십시오. 최근에 스마트폰에 설치되는 앱들은 스마트폰에 있는 모든 내용에 대해서 사용할 수 있도록 권한을 달라고 요구하고 있습니다. 따라서 내가 꼭 설치할 필요가 있는지 그 앱에 대해서 점검하실 필요가 있고요. 개인정보와 관련된 내용이 담긴 파일을 PC 로 보관하신다 그러면 파일, 문서 솔루션에서 제공하는 암호설정 기능이라도 이용해서 꼭 암호를 설정하십시오. 또 자료를 백업하는 용도로 웹하드 등을 사용하고 계시다면 혹시 그 웹하드 등에 폴더 전체 공유가 걸려있지 않은지, 설정을 점검하실 필요가 있습니다. 중요한 정보를 PC 에 담지 않고 백업의 용도로 웹하드에 올려놓고 있는데 그 설정이 전체 공유로 돼서 다른 사용자들이 그 자료를 보고 가져갈 수 있는 경우가 드물게 발생할 수 있습니다. 따라서 본인과 관련된 설정이 어떻게 되어 있는지를 항상 점검하시는 게 필요하고요.

공공장소에서 예를 들어 PC 방 같은 곳에서 접속을 해서 사용을 하셨다면 반드시 로그아웃을 하셔야 됩니다. 로그아웃을 하지 않고 PC 를 그냥 시간이 돼서 이석을 하셨을 경우에 다른 사용자가 동일한 사이트에 들어갔을 때 로그인인 된 상태로 떠서 그냥 본인의 정보를 가지고 다른 작업을 할 가능성이 존재하기 때문입니다. 또 반드시 개인의 PC 에도 보안솔루션을 설치하셔야 됩니다. 많은 보안솔루션이 이미 알려진 위협에 대해서는 탐지하고 차단하는 기능을 제공하고 있기 때문에 보안솔루션을 설치하고 최신 엔진으로 업데이트하는 것만으로 해킹을 위한 악성코드 중에 상당부분은 차단하실 수 있습니다. 마지막으로 공유폴더는 사용하지 마십시오. 기업이든 개인이든 공유폴더를 통한 정보유출이 빈번히 발생하고 있기 때문에 공유폴더는 설정하지 않도록 하시는 습관을 들이시는 게 중요합니다.

5차시. 개인정보 안전성 확보조치, 반드시 필요해요!

1. 개인정보 안전성 확보조치의 정의

- 개인정보 처리자는 개인정보의 분실, 도난, 유출, 변조, 훼손을 방지하기 위하여 개인정보 처리 시스템의 안전성 확보에 필요한 관리적, 기술적, 물리적 조치를 취해야 합니다.

(참고: 개인정보처리시스템이란? 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말함)

- 안전성 확보에 필요한 구체적인 조치 및 기준은 시행령 및 「개인정보의 안전성 확보조치 기준 고시」에서 정하고 있습니다.

- 개인정보 안전성 확보조치 기준은 개인정보처리자의 개인정보보유량에 따라 유형1에서 유형3까지 적용대상을 분류하여 조치기준을 차등적용하고 있습니다.

유형	적용대상	조치사항 차등화
유형1 (완화)	보유량 1만명 미만 소상공인, 단체, 개인	- 과도한 규제 적용 면제 - 필수적 안전조치 의무화
유형2 (표준)	- 보유량 1만명 이상 소상공인, 단체, 개인 - 보유량 100만명 미만 중소기업 - 보유량 10만명 미만 공공기관, 대기업, 중견기업	유형1보다 안전조치 기준 강화
유형3 (강화)	- 보유량 10만명 이상 대기업, 중견기업 - 보유량 100만명 이상 중소기업, 단체	- 과도한 규제 적용 면제 - 필수적 안전조치 의무화

유형별로 안전조치를 차등하면서 추가적으로 단말기에 대한 안전조치 및 관리적 안전조치를 신설 하였으며, 불법접근에 대하여 탐지하고 차단할 수 있는 침해사고 방지를 위한 기술적 안전조치도 추가하였습니다. 기업이 어느 유형에 해당하는지의 입증책임은 개인정보처리자에 있기 때문에 우리 기업이 어느 유형인지 인지하시고 개인정보 보호 계획을 수립하시면 됩니다.

2. 개인정보 안전성 확보조치의 실천

(1) 관리적 보호조치

[개인정보 실태 점검 및 행정처분 사례집 中 160 페이지]

A 병원은 원활한 업무 처리를 위하여 환자의 개인정보를 수집하고 있는데, 현재 30 만 건 이상의 환자 개인정보를 보관하고 있다. 그리고 이를 관리하기 위하여 개인정보처리시스템을 도입하여 운용하고 있다. 한편 의료 정보와 의무 기록 등의 안전한 관리를 위하여 '개인정보보호를 위한

내부 관리계획 및 관련 문서'를 작성하여 관리하고 있다. 그러나 현장점검 결과, A 병원은 이러한 개인정보보호를 위한 내부 관리계획을 수립하여 관리는 하고 있었지만, 세부 항목을 보면 의무 업무와 관련된 내용만 담고 있어 이를 기관의 개인정보보호 내부 관리계획으로 볼 수 없었다. 즉 개인정보보호 내부 관리계획이라는 동일한 명칭을 가지고는 있었지만, 개인정보 보호법에 따른 필수 항목 (이를테면 개인정보 보호책임자 지정 등)을 반영하지 않고 다른 접근 방식을 취하고 있었던 것이다. 개인정보보호 내부 관리계획의 경우 개인정보처리자 유형[유형 1(완화)/유형 2(표준)/유형 3(강화)]에 따라 지정된 필수 사항을 모두 반영하여 계획을 수립하여야 하므로 A 병원의 경우 내부 관리계획 미수립에 해당한다.

개인정보처리자는 개인정보의 안전한 처리를 위한 '내부관리계획'을 수립·시행하여야 하는데요. 여기서 내부관리계획이란 정보주체의 개인정보를 보호하기 위한 조치를 시행하기 위해 수립된 회사 전체에서 적용되는 내부규정, 즉 정책, 지침, 가이드를 의미합니다. 이러한 내부관리계획을 근간으로 사내 개인정보처리의 기준을 마련하게 되므로 개인정보처리자는 반드시 내부관리계획을 수립 후 공표함으로써 사내에서 적용되어야 합니다.

[내부관리계획에 포함되어야 하는 사항]

- 개인정보 보호책임자의 지정에 관한 사항
- 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보취급자에 대한 교육에 관한 사항
- 개인정보의 안전성 확보에 필요한 조치에 관한 사항
- 그 밖에 개인정보 보호를 위하여 필요한 사항 등

[기타사항]

- 내부관리계획에 포함되는 사항에 중요한 변경이 있는 경우 이를 즉시 반영하여 내부관리계획을 수정하여 시행해야 함(수정 이력도 관리)
- 내부관리계획은 원칙적으로 공공기관, 기업 등 모든 개인정보처리자가 수립·시행해야 함
- 다만, 소규모 사업자에게 까지 의무화하면 사업자의 부담이 가중될 수 있어 소상공인에 한해서는 수립하지 않아도 됨

(2) 기술적 보호조치

[개인정보 실태 점검 및 행정처분 사례집 中 123 페이지]

틈틈이 어학 공부를 하고 있는 B 씨는 회사 근처 A 학원에 등록하여 일주일에 2 회씩 영어 원어민 수업을 듣고 있 다. 당시 학원에 등록하면서 자신의 주민등록번호를 비롯한 몇 가지 개인정보를 기입하였고, 해당 개인정보 수집 및 이용에 대하여 동의하였다. A 학원은 이렇게 수집한

학원생들의 개인정보 중 주민등록번호를 개인정보처리시스템에 저장하여 관리하고 있다. 그러나 현장점검 결과, A 학원의 개인정보처리시스템은 학원생들의 주민등록번호에 대하여 암호화 적용을 하지 않아 13 자리 번호가 모두 노출된 채 저장·관리되고 있는 것으로 드러났다. 주민등록번호의 경우 고유식별정보로 반드시 안전한 암호 알고리즘을 사용하여 암호화 적용을 한 후 저장·관리하여야 한다.

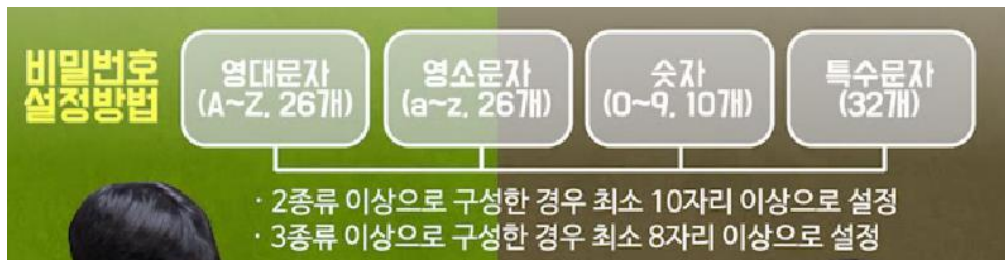
가. 접근 권한 제한 조치

다음으로 개인정보시스템에 대한 접근 통제를 실시하기 위해 접근이 가능한 권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여해야 합니다. 접근 권한에 대한 정책은 통상 내부관리계획을 통해 정의되는데 이를 기준으로 해당 직무에 적합한 임직원에게 권한이 주어져야 합니다.

또한 권한의 부여 뿐만 아니라 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경될 경우에는 해당 취급자의 시스템 접근 권한을 지체없이 변경 또는 말소해야 합니다. 이 때 해당 내역에 대해 최소 3 년간 보관해야 합니다.

특히 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며(동일한 개정으로 여러 명이 사용하면 안됨), 다른 개인정보취급자와 공유되지 않도록 조치해야 합니다.

또한 개인정보처리시스템에 접근할 수 있는 개인정보취급자와 정보주체는 안전한 비밀번호를 설정해야 합니다.



※ 가급적 연속적인 숫자나 생일, 전화번호 등 추측이 쉬운 비밀번호는 사용하지 않도록 주의해야 합니다.

나. 접근 통제 조치

개인정보처리시스템에는 승인된 권한자 이외에 불법적 접근 및 유출시도 등을 방지하기 위해 관련 시스템을 설치 운영하도록 해야 합니다. 이 때, 개인정보처리시스템에 보호 시스템은 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(방화벽(firewall))하고 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고 대응하도록 설정해야 합니다. 또한 개인정보처리시스템에 적절하게 권한이 부여되어 있더라도

외부에서 개인정보처리시스템에 접속하는 경우 개인정보취급자가 안전하게 접속할 수 있도록 가상사설망(VPN) 또는 전용선 등 안전한 접속 수단을 적용해야 합니다. 그리고 개인정보 노출 방지 조치를 취해야 합니다. 홈페이지에서 다른 법에 근거하여 정보주체의 보안확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우 정보주체의 추가적인 정보를 확인하도록 하고 인터넷 홈페이지의 취약점 방지하기 위한 조치(SQL-Injection 취약점 방지, ZeroBoard 취약점 방지 등) 등을 하여야 합니다. 개인정보가 홈페이지, P2P, 공유설정 등을 통해 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일기기에 조치를 취해야하며, 고유식별정보가 유출, 변조, 훼손되지 않도록 연 1 회 이상 취약점 점검하여야 합니다. 모바일 기기는 분실, 도난 등으로 유출되지 않도록 비밀번호 반드시 설정해야 합니다.

다. 개인정보 암호화

개인정보의 암호화는 개인정보의 전송과 저장 두 가지 측면에서 접근해야 하는데요. 먼저 개인정보처리자는 개인정보처리시스템에서 고유식별번호(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에 반드시 암호화 해야 합니다. 이 때 전송시, 암호화를 구현하는 가장 일반적인 방법으로는 웹 서버에 SSL 인증서를 설치하거나, 웹 서버에 암호화 응용프로그램을 설치하는 방법을 적용할 수 있습니다.

두번째 저장시 암호화 대상은 비밀번호 및 바이오 정보로 개인정보취급자의 단말기 모바일 기기 등에 파일로 저장할 때, 적절한 암호화 방식으로 암호화해야 합니다. 특히 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화로 저장하여야 합니다. 일방향 암호화란 해독키가 없어서 복구가 안되는 안전한 암호화를 말합니다. 또한 개인정보처리자는 인터넷 구간 및 인터넷구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화해야 합니다.

라. 접속기록의 보관 및 위조·변조 방지 조치

개인정보처리자는 개인정보취급자가 처리시스템에 접속한 기록을 보존 및 관리해야 합니다. 이는 개인정보 유출 등 사고 발생 시 책임추적성과 개인정보취급자의 위반사항을 파악하기 위한 사후적 보호조치에 해당합니다. 이에 따라 개인정보취급자의 처리활동에 따라 생성되는 개인정보처리시스템의 로그는 반드시 별도저장과 관리가 필요합니다. 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6 개월 이상 보관 및 관리하여야 하며 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템에 접속기록 등을 반기별로 1 회 이상 필수적으로 점검 하여야 합니다. 또한 개인정보취급자의 접속기록이 위 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관 해야 합니다. 이때 저장되는 개인정보취급자의 접속 기록은 회사마다 차이가 있을 수 있지만 개인정보취급자 식별정보, 접속일시, 접속지 정보, 업무수행 내역은 반드시 기록되어야 합니다.

마. 악성프로그램 방지

개인정보처리자는 악성프로그램 등을 통해 발생할 수 있는 감염을 방지하기 위해 이를 방지, 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 및 운영하여야 합니다. 이에 따라 보안프로그램의 자동 업데이트 기능을 사용하거나 일 1 회 이상 업데이트를 실시하여 최신 상태를 유지하도록 해야 합니다. 악성 프로그램 관련 경보 발령 시, 사용중인 응용 프로그램 및 운영체제 소프트웨어의 제작업체 보안업데이트 공지시 즉시 업데이트하여야 합니다.

(3) 물리적 보호조치

[개인정보 실태 점검 및 행정처분 사례집 中 72 페이지]

A 업체는 가전제품 소매업과 이동 전화 판매·개통 서비스를 제공하는 업체이다. B 씨는 최근 스마트폰을 새로 장 만하기 위하여 예전에 구매 경험이 있는 근처 A 업체를 방문하였다. 상담을 받고 마음에 드는 상품을 골라 개통하 려고 했더니 A 업체 직원이 몇 가지 조회를 해 보며 한참 만에 방문한 것 같다고 B 씨의 개인정보를 말하는 것이었 다. B 씨는 자신의 정보가 아직도 거기 있었다는 생각에 찜찜함을 감출 수 없었다. A 업체는 이동 전화 판매·개통 서비스를 위하여 고객의 이름·연락처·주소 등을 수집하여 판매 관리 시스템에 보 관하고 있었는데, 상법 등 다른 법률에 따른 개인정보 보유기간(5 년)이 지난 개인정보까지도 파기하지 않고 그대 로 가지고 있었던 것이다. 이 경우 A 업체의 판매 관리 시스템이라고 하더라도 고객으로부터 수집한 개인정보는 보유기간이 지나거나 처리 목적이 달성된 이후에는 지체 없이 파기하여야 한다.

개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에 개인정보유출에 대비하여 출입통제 절차를 수립, 운영하여야 합니다. 또한 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 하며, 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안 대책을 마련하여야 합니다. 다만 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터, 모바일 기기를 이용하여 개인정보를 처리하는 경우 이를 적용하지 아니할 수 있습니다.

가. 이용목적이 달성된 개인정보 파일을 완전 파기할 경우

- √ 완전 파괴(소각 및 파쇄 등)
- √ 전용 소자 장비를 이용하여 삭제
- √ 데이터 복원되지 않도록 초기화 또는 덮어쓰기 수행

나. 개인정보 일부만 파기하는 경우

- √ 전자적 파일 형태 : 개인정보 삭제한 후 복구/재생이 되지 않도록 관리/감독
- √ 기록물, 인쇄물, 서면, 그밖의 기록 매체 : 해당 부분 마스킹, 천공

개인정보처리자는 개인정보 유출 등 개인정보침해사고 방지를 위하여 관리용 단말기에 대한 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치하던지, 본래 목적 외로 사용되지 않도록 조치해야 합니다. 또한 화재, 홍수, 단전 등의 재해, 재난 발생시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼을 마련하고 정기적인 점검하여야 합니다.