

[데이터 경제 시대의 도래, 기업이 대비해야 할 주요 법안서]

5차시. 개인정보 보호원칙과 정책

| 학습목표 |
|---|
| <ul style="list-style-type: none">▪ 학습내용: 해당 차시에서 학습할 학습주제(목차)를 제시해 주세요.▪ 학습목표: 해당 차시 학습을 통해 <u>학습자들이 달성해야 할 목표</u>를 학습내용과 연계하여 작성해 주세요. |

▶ 학습내용

1. 개인정보보호 원칙과 정보주체의 권리
2. 국가 및 지방자치단체의 책무와 개인정보 보호정책

▶ 학습목표

1. 개인정보 보호원칙에 대해 설명할 수 있습니다.
2. 개인정보 보호에 대한 국가 및 지방자치단체의 책무를 설명할 수 있습니다.
3. 개인정보 보호정책에 대해 설명할 수 있습니다.

| 학습내용 |
|--|
| <ul style="list-style-type: none"> ■ 학습내용의 위계 파악을 위해 일관성 있는 번호 체계로 작성해 주세요. |

I. 개인정보보호 원칙과 정보주체의 권리

1. 개인정보보호 원칙의 법적 근거

개인정보에 대한 기본법인 개인정보 보호법에서 개인정보를 규제하는 개인정보보호원칙은 무엇인가? 이러한 개인정보에 대한 보호원칙은 개인정보처리자로 하여금 개인정보 처리시 준수해야 하는 기본 원칙을 제시한 것이다. 즉 개인정보보호 원칙을 살펴봄으로써 개인정보 처리에 대한 정부의 정책적 방향성을 알 수 있으며, 법적 규제에 대한 전체적인 이해를 도모할 수 있다.

개인정보보호 원칙에 대해서는 개인정보 보호법 제3조에서 규정하고 있다. 뿐만 아니라 개인정보보호위원회가 마련한 ‘표준 개인정보 보호지침(이하 “표준지침”이라 함)¹⁾ 제4조에서도 유사한 내용의 개인정보보호 원칙을 규정하고 있는데, 표준지침에서 보다 상세한 내용을 담고 있다. 한편 표준지침이란 개인정보 보호법 제12조 제1항에 따라 개인정보의 처리기준, 개인정보 침해유형 및 예방조치 등에 관해서 개인정보보호위원회가 제정한 것이다.

| 개인정보 보호법 | 표준 개인정보 보호지침 |
|---|---|
| <p>제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.</p> <p>② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.</p> <p>③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.</p> <p>④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.</p> <p>⑤ 개인정보처리자는 개인정보 처리방침 등 개</p> | <p>표준지침 제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.</p> <p>② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.</p> <p>③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.</p> <p>④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.</p> <p>⑤ 개인정보처리자는 개인정보 처리방침 등 개</p> |

1) [시행 2020.8.11.] [개인정보보호위원회고시 제2020-1호, 2020.8.11. 제정]

| | |
|--|---|
| <p>인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.</p> <p>⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.</p> <p>⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적 달성을 할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020. 2. 4.></p> <p>⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.</p> | <p>인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.</p> <p>⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.</p> <p>⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.</p> <p>⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.</p> |
|--|---|

2. 개인정보보호 원칙의 기본 내용

개인정보 보호법 제3조와 표준지침 제4조에서는 개인정보처리자가 준수해야 하는 개인정보 보호 원칙을 8가지로 상세히 열거하고 있다. 개인정보는 개인의 사생활과 긴밀하게 관련 맺으면서도 또한 정보화사회로 불리는 오늘날 매우 중요한 산업적 가치로 급부상함에 따라 유출될 가능성이 커지고 이에 따라 오남용의 가능성도 훨씬 커지게 되었다. 이러한 시대적 상황에서 이제 개인정보 보호법에서는 개인정보 처리목적에 명확히 할 것은 물론이고 목적에 있어서도 필요한 최소한의 개인정보만을 적법하고 정당하게 수집하도록 하고 있으며(법 제3조 제1항), 목적 이외의 용도로 활용해서는 안 됨을 분명하게 밝히고 있다(법 제3조 제2항). 즉 정보수집 목적을 익명 또는 가명으로 처리해도 달성할 수 있다면, 가능한 한 익명처리에 의해 개인정보를 처리하며, 만일 익명처리로 수집목적 달성을 할 수 없는 경우에는 가명으로 개인정보를 처리하도록 의무화하고 있는 것이다(법 제3조 제7항).

나아가 개인정보처리자는 정보주체의 권리침해 가능성 등을 고려하여 개인정보를 안전하게 관리하여야 하고(법 제3조 제4항), 개인정보처리방침 등에 대해서 공개하며, 열람청구권 등과 같은 정보주체의 권리보장(법 제3조 제5항)과 함께, 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하도록 하고 있다(법 제3조 제6항).

3. 개인정보 보호원칙과 OECD 프라이버시 가이드라인의 보호원칙

1) OECD 프라이버시 가이드라인 보호원칙의 소개

개인정보 보호법 제3조에서 규정하고 있는 개인정보 보호원칙은 1980년 9월 23일에 개최한 OECD에서 채택한 ‘프라이버시와 개인정보의 초국경 이동의 보호를 규율하는 가이드라인

(Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data²⁾, 일명 “1980년 OECD 프라이버시 가이드라인”)과 밀접한 관련을 맺고 있다.

1980년 OECD 프라이버시 가이드라인에서는 제7조부터 제14조에서 ‘OECD 프라이버시보호 8대 기본원칙(Basic Principles of National Application)’³⁾을 제시하였다. 이러한 8개의 원칙에 대한 내용을 간략히 살펴보면 아래와 같다.

첫째는 제7조에서 규정하고 있는 ‘수집제한원칙(Collection Limitation Principle)’이다. 그 내용은 개인정보 수집에 있어서 가능한한 제한적으로 수집하도록 하고 있으며, 특히 합법적이고 공정한 절차에 따라 정보주체의 인지 또는 동의를 얻도록 하고 있다.

둘째는 제8조에서 규정하고 있는 ‘정보 정확성 원칙(Data Quality Principle)’이다. 개인정보는 그 이용 목적에 부합하는 것만을 수집하도록 하고 있으며, 수집목적에 필요한 범위 내에서 정확하고 완전하며, 최신의 상태를 유지하도록 정보처리자에게 요구하고 있다.

셋째는 제9조에서 규정하고 있는 ‘목적 명확성 원칙(Purpose Specification Principle)’이다. 개인정보 수집의 목적은 정보를 수집하는 시점에 명시되도록 요구하고 있으며, 그 이후의 이용은 이러한 수집목적 또는 이러한 목적과 모순됨이 없어야 하고, 만일 목적이 변경되는 경우에는 변경시 마다 이러한 목적에 명확히 충족하도록 요구하고 있다.

넷째는 제10조에서 규정하고 있는 ‘이용제한의 원칙(Use Limitation Principle)’이다. 개인정보는 수집된 목적으로만 이용하여야 하며, 목적 이외로 이용해서는 안된다고 규정하고 있다. 다만 정보주체에게 동의를 얻었거나 또는 법에 근거하여 허가된 경우는 예외로 하고 있다.

다섯째는 제11조에서 규정하고 있는 ‘안전성 보장의 원칙(Security Safeguards Principle)’이다. 개인정보는 개인정보의 분실, 무단접근, 훼손, 사용, 수정 또는 공개 등과 같은 위험에 대비하여 합리적인 보안조치에 따라 보호되도록 개인정보처리자에게 요구되고 있다.

여섯째는 제12조에서 규정하고 있는 ‘공개성의 원칙(Openness Principle)’이다. 개인정보에 관한 개발, 관행 및 정책에 대한 내용이 포함된 공개방침이 있어야 한다. 개인정보처리자(data controller)의 신원과 일상적 거주지와 함께 개인정보의 존재와 특성, 이용의 주된 목적을 쉽게 확인할 수 있도록 하여야 한다.

일곱째는 제13조에서 규정하고 있는 ‘개인참여의 원칙(Individual Participation Principle)’이다. 이 원칙에 따라 정보주체는 개인정보처리자가 자기에 관한 정보를 갖고 있는지 여부에 대하여 개인정보처리자 또는 기타의 자로부터 확인을 받을 권리, 개인에 관한 정보를 상당 기간 내에 과다하지 않은 비용으로 합리적인 방법과 알기 쉬운 형태로 본인에게 통지하도록 하는 권리, 그리고 이상의 요구가 거부당한 경우에는 그 이유를 밝히도록 하고 이와 같은 거부에 대하여 이의를 제기할 수 있는 권리, 자기에 관한 정보에 대하여 이의를 제기하고 그 이의가 인정되지 아니할 경우에는 그 정보를 삭제·개정·보완·수정하게 하는 권리를 갖고 있으며, 이러한 권리가 실현되도록 개인정보처리자는 최선을 기울여야 한다.

여덟째는 제14조에서 규정하고 있는 ‘책임의 원칙(Accountability Principle)’이다. 즉 개인정보처리자(data controller)는 위에서 제시한 원칙들이 지켜지도록 필요한 제반조치를 취하

2) <https://www.oecd.org/sti/ieconomy/>

3) <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsdatapersonal.htm#part3>

도록 하고 있다.

2) 개인정보보호법의 개인정보 보호원칙 비교

이러한 OECD 프라이버시 가이드라인에서 규정하고 있는 개인정보 보호원칙과 우리의 개인정보보호법에서 천명하고 있는 개인정보 보호원칙을 비교하면 아래와 같다.

[표 #: OECD 프라이버시 가이드라인과 개인정보 보호법상 개인정보 보호원칙 비교⁴⁾]

| OECD 프라이버시 가이드라인 | | 개인정보보호법상 개인정보 보호원칙 제3조 | |
|------------------|--|------------------------|---|
| 7조 | 수집제한 원칙 (Collection Limitation Principle) | 제1항 | 처리 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 함 |
| 8조 | 정보 정확성 원칙 (Data Quality Principle) | 제3항 | 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 |
| 9조 | 목적 명확성 원칙 (Purpose Specification Principle) | 제1항 | 개인정보의 처리 목적을 명확하게 하여야 |
| 10조 | 이용제한의 원칙 (Use Limitation Principle) | 제2항 | 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. |
| 11조 | 안전성 보장의 원칙 (Security Safeguards Principle) | 제4항 | 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 |
| 12조 | 공개성의 원칙 (Openness Principle) | 제5항 | 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 |
| 13조 | 개인참여의 원칙 (Individual Participation Principle) | 제5항 | 열람청구권 등 정보주체의 권리를 보장하여야 |
| 14조 | 책임의 원칙 (Accountability Principle) | 제8항 | 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 |
| | | 제6항 | 사생활침해의 최소화 |
| | | 제7항 | 익명처리 및 가명처리에 대한 권장 |

위의 도표를 보면 국내 개인정보 보호법은 OECD 프라이버시 가이드라인을 많이 반영하고 있음을 알 수 있다. 우리나라가 OECD 회원국이기기는 하나, 이러한 OECD 가이드라인이 회원국에 구속력이 있는 것은 아니다. 하지만 개인정보라는 것이 국경이 없으며 국가간의 자유로운 이동이 가능하고 글로벌시장에서 원활하게 개인정보를 활용할 수 있도록 하기 위해 OECD에서는 이러한 OECD 프라이버시 가이드라인의 원칙들을 회원국에서 반영하여 협력할 것을 권고하였다. 이에 따라 OECD 가이드라인이 구속력은 없지만, 자국의 개인정보보호 관련 법률에서 이러한 원칙들을 반영하였으며 우리나라도 예외는 아니어서, 2011년 3월 29일에 개인정보 보호법 제정 당시부터 OECD 가이드라인의 보호원칙을 많이 반영하였다.

4. 개인정보보호 원칙의 구체적 내용

1) 처리 목적에 대한 명확화

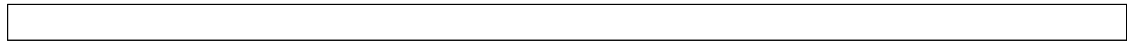
개인정보 보호법 제3조 제1항과 표준지침 제4조 제1항에서는 개인정보처리자의 가장 우선적인 원칙으로서 ‘처리 목적에 대한 명확화’를 규정하고 있다. 우선 개인정보처리자가 개인정보를 처리하기 위해서는 전제조건이 정보주체로부터 정보주체의 개인정보를 수집하여야 한다. 이때 정보주체로부터 동의를 받아야 하는데 진정한 동의를 받기 위해서는 그 처리목적이 명확해야 하는 것이다. 데이터 3법 개정에 따라 이제 개인정보는 보호의 대상만이 아니라 활용의 대상으로 변모되었다. 따라서 데이터 3법의 본래 목적이 제대로 기능을 발휘하기 위해서는 개인정보의 주체로부터 수집과 이용 등의 처리에 대한 정확한 내용이 전달되어 동의를 받아야 함은 가장 기본적인 개인정보 처리의 순서라고 할 수 있다.

2) 최소한의 수집

개인정보처리자는 처리 목적에 필요한 범위라고 하더라도 가급적 최소한의 개인정보만을 수집하여야 한다(법 제3조 제1항, 표준지침 제4조 1항).

구체적인 개인정보 수집·이용의 방법에 대해서는 개인정보 보호법 제15조 제1항(개인정보의 수집·이용)에서 상세히 규정하고 있으며, 개인정보 수집하는 경우에 있어서 수집목적에 필요한 최소한의 개인정보를 수집하도록 제16조(개인정보의 수집 제한)에서 상세히 규정하고 있다. 즉 제15조 제1항에 따라, 아래의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 수집목적에 필요한 최소한의 개인정보를 수집하도록 개인정보처리자에게 의무지우고 있다.

- 정보주체의 동의를 받은 경우(제1호),
- 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제2호),
- 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우(제3호),
- 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우(제4호),
- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제5호),
- 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우에, 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우(제6호)



이때 과연 최소한의 개인정보 수집이었는지 여부와 관련하여 정보주체와 개인정보처리자 사이에 분쟁이 발생할 수도 있다. 이를 대비하여 개인정보보호법에서는 최소한의 개인정보 수집이라는 입증책임을 개인정보처리자에게 부담지우고 있다(제16조 제1항 제2문). 이는 무엇보다 개인정보 처리가 전문적이어서 수집된 개인정보와 목적사이의 관련성을 정보주체가 파악하기 어렵다는 현실을 반영한 것이다.

3) 적법하며 정당한 수집

또한 개인정보처리자는 개인정보를 수집하는데 있어서 수집방법은 적법하고 정당하게 수집하여야 한다(법 제3조 제1항 및 표준지침 제4조 제1항). 이때 적법하고 정당한 수집방법이 무엇인지, 나아가 적법한 수집방법과 정당한 수집방법이 어떻게 다른지에 대해서 개인정보 보호법에서는 상세히 규정하고 있지는 않다.

그러나 ‘적법하다’는 의미는 법령에서 부여한 개인정보처리시 요구되는 내용들을 충족하여야 할 것을 말한다. 즉 개인정보 보호법 제3장에서 개인정보의 처리에 대한 자세한 내용을 규정하고 있는데, 그 중 개인정보의 수집·이용(제15조), 개인정보의 수집제한(제16조)을 준수했는지 여부로 판단할 수 있다.

이에 반하여 정당한 수집이란 적법한 수집보다 폭넓은 의미라고 할 수 있다. 즉 적법한 수집은 규범을 전제로 한 적법과 불법의 구분에 따른 적법수집을 의미하는 반면에, 정당한 수집이란 규범으로 한정하지 않고 규범을 넘어 조리, 사회상규, 관습 등을 포함하여 이에 어긋나지 않도록 한 수집으로 이해될 수 있다. 따라서 미처 규범에 반영되지 못하였더라도 수집의 정당성에 대해 다시 한번 심사하도록 하여 개인정보를 제한적으로 수집하도록 한 것이다.

이러한 적법 및 정당한 개인정보의 수집은 유럽연합 회원국에 공통적으로 적용되는, 2016년에 채택한 GDPR(General Data Protection Regulation; 유럽의 개인정보보호규칙)의 첫 번째 원칙, 즉 ‘합법적이고 공정하며 데이터 대상과 관련하여 투명하게 처리해야 한다’는 내용에 상응한 것으로 이해될 수 있다.

4) 개인정보의 적합한 처리

개인정보처리자는 개인정보의 처리목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 한다(법 제3조 제2항 및 표준지침 제4조 제2항). 물론 이때 개인정보의 적합한 처리는 개인정보의 수집 뿐만 아니라 개인정보와 관련되는 모든 과정의 작업을 의미하며 전체 작업이 적합해야 한다는 것을 말한다. 이러한 개인정보의 처리목적은 개인정보를 수집하는 단계에서 확정되어야 하므로, 개인정보의 적합한 처리는 처리목적에 필요한 범위가 아닌, 수집 목적에 필요한 범위에서 요구된다고 한다.

5) 처리 목적 외의 활용금지

개인정보처리자는 개인정보의 처리 목적 외의 용도로 활용하지 못하도록 법 제3조 제2항 후단 및 표준지침 제4조 제2항 후단에서 규정하고 있다. 이때 개인정보의 ‘활용’은 이용과 유

사한 개념이면서 ‘처리’에 포함되는 개념으로 이해될 수 있다. 따라서 개인정보처리자는 개인정보를 수집할 당시의 특정된 수집목적을 넘어서 다른 목적으로 개인정보를 이용하거나 제3자에게 제공하는 등의 폭넓은 처리를 해서는 안된다는 의미이다.

이는 정보주체의 동의와 긴밀한 관련이 있다. 즉 개인정보 주체는 정보수집 당시의 처리 목적을 염두에 두고 동의를 하였으므로, 만일 수집 당시의 처리 목적 외로 활용할 경우 개인정보처리자는 원칙적으로 정보주체로부터 별도의 동의 절차를 진행해야 함을 의미한다.

6) 개인정보의 정확성, 완전성 및 최신성 보장의무

개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 유지하여야 한다(법 제3조 제3항 및 표준지침 제4조 제3항 전단). 이는 개인정보에 대한 전문적 기술을 전제로 하므로 개인정보를 수집한 개인정보처리자에게 직접 요구되는 의무사항이라고 할 수 있다. 물론 이러한 개인정보에 대한 정확성, 완전성 및 최신성에 대한 유지는 개인정보처리자가 아닌 개인정보의 주체에게서도 가능함은 당연하다. 그러나 법 및 표준지침에서의 원칙은 개인정보처리자에게 직접 이러한 유지의무를 담당하게 하는 것이므로 개인정보처리자가 정보주체에게 이러한 완전성 및 최신성 등에 대해서 의무지우는 것은 안된다.

물론 개인정보는 고유한 일신전속적인 정보도 있지만 주소변경, 전화번호, 건강상태 등이 변화하는 정보도 많다. 따라서 개인정보처리자가 처리하기 어려운 정보도 많다. 이러한 경우를 대비하여 개인정보처리자는 특정 주기, 예컨대 매년, 2년, 3년 등 정기적으로 정보주체에게 개인정보를 업데이트하도록 요구할 수 있으며, 이러한 업데이트에 대한 선택도 폭넓게 정보주체에게 선택하도록 기회를 제공하여야 함을 의미한다.

더 나아가 표준지침에서는 개인정보를 처리하는 과정에서 고의 또는 과실로 이러한 개인정보가 부당하게 변경 또는 훼손되지 않도록 추가적으로 개인정보처리자에게 요구되고 있다(표준지침 제4조 제3항 후단)

7) 개인정보의 안전한 관리

개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다(법 제3조 제4항 및 표준지침 제4조 제4항) 이러한 안전관리에 대해 표준지침에서는 추가적으로 상세하게 덧붙여 설명하고 있는데, 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 하도록 규정하였다.

이러한 안전관리의무는 개인정보의 디지털 속상상 쉽게 분실, 도난, 유출, 위·변조 또는 훼손의 가능성이 있으므로 이를 차단하기 위한 것이다. 구체적인 방법에 대해서는 대통령령인 시행령 제30조에서 규정하고 있는데, 안전한 처리를 위한 내부 관리계획의 수립·시행, 개인정보에 대한 접근통제 및 접근 권한의 제한조치, 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술을 적용하는 등의 조치를 취하도록 규정하고 있다.

[표 #: 개인정보의 안전성 확보를 위한 조치방안]

| |
|---|
| 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 |
|---|

따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
 5. 개인정보에 대한 보안프로그램의 설치 및 갱신
 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치
- ② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>
- ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 8. 4.>

8) 개인정보 처리방침에 대한 공개와 정보주체의 열람청구권 보장

개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다(법 제3조 제5항 및 표준지침 제4조 제5항 전단). 이러한 개인정보 처리방침에 대한 공개방침은 두가지 의미를 갖는다. 하나는 개인정보 처리자로 하여금 수집한 개인정보의 처리가 투명함을 정보주체에게 공개적으로 알린다는 의미이며, 다른 하나는 정보주체에게 자신의 개인정보 처리 등에 대해 열람청구권이 있음을 선언하는 의미이다.

더 나아가 표준지침에서는 정보주체의 열람청구권이 보장될 수 있도록 개인정보처리자는 합리적인 절차와 방법 등을 마련하도록 덧붙이고 있다.

9) 사생활침해의 최소화

개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에 있어서도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다(법 제3조 제6항 및 표준지침 제4조 제6항).

데이터 3법 개정으로 개인정보에 대한 정부의 입장도 변화하였다. 즉 데이터 3법 개정에 따른 2020년 8월 개인정보보호법 개정전 동법은 사생활침해로부터 개인정보를 보호하는데 주목적이 있었다. 그러나 이제 데이터 3법 개정으로 개인정보를 바라보는 시선은 ‘보호’와 ‘활용’으로 목적이 병존되게 되었다. 그러나 이전과 달리 개인정보 ‘활용’이라는 목적이 새롭게 비중이 높아졌다 하더라도 이에 비례하여 개인정보 오남용의 가능성도 훨씬 더 커지게 되었고 이로부터 정보주체의 사생활 침해를 최소화하기 위한 노력을 개인정보처리자에게 더욱 강하게 요구되고 있는 상황이다. 이러한 사생활침해의 최소화는 단순히 선언적인 추상적인 원칙에 그치는 것이 아니라, 개인정보처리자에게 정보주체의 사생활침해를 최소화하기 위한 구체적인 방안으로까지 요구하고 있는 것이다.

10) 개인정보의 익명처리 및 가명처리 권장

개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할

수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다(법 제3조 제7항 및 표준지침 제4조 제7항). 현행 개인정보 보호법에서는 개인정보 수집목적의 달성을 위해 개인정보처리에 대한 단계를 마련하고 있다. 즉 개인정보 수집목적의 달성이 가능하다면 가급적 익명정보에 의해 처리하여야 하며, 익명정보로도 수집목적달성이 어렵다면 이때는 가명처리된 정보인 가명정보로 처리하도록 한 것이다. 이러한 처리 방법은 앞서 살펴본 개인정보 보호법의 주된 목적인 ‘개인정보의 사생활침해’를 최소화하기 위한 구체적인 방법이라고 할 수 있다. 한편 가명처리에 대한 권장은 데이터 3법 개정에 따른 2020년 8월의 개인정보 보호법 개정으로 추가된 부분으로서 개인정보 처리자의 입장에서는 개인정보 활용에 있어서 상당히 유리한 입장에 놓이게 된 것이라 할 수 있다.

11) 개인정보처리자에 대한 법적 책임

개인정보처리자는 개인정보 보호법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력을 하여야 한다(법 제3조 제8항 및 표준지침 제4조 제8항). 이에 따라 개인정보처리자에게 요구되는 의무사항은 크게 두 가지로 요약될 수 있다. 하나는 개인정보 보호법 및 관련 법령에서 규정하고 있는 준수해야 하는 책임과 의무를 다하여야 하고, 다른 하나는 이러한 책임과 의무의 실천으로부터 정보주체의 신뢰를 얻기 위한 다양한 방법을 강구하여야 하는 것이다.

정보주체의 신뢰를 얻기 위한 노력에 대해서는 구체적으로 제시하고 있지 않다. 그러나 개인정보처리자가 앞서 살펴본 위의 원칙들을 준수함으로써 그러한 노력을 다한 것으로 주장할 수 있으리라고 판단된다.

II. 국가 및 지방자치단체의 책무와 개인정보 보호정책

1. 국가 및 지방자치단체의 책무

한편 개인정보 보호법에서는 개인정보 처리에 있어서 앞서 살펴본 개인정보처리자에게 준수해야 할 의무를 부과함과 동시에 나아가 국가 및 지방자치단체에게도 개인정보 관련하여 일정한 역할을 담당하도록 요구하고 있다. 즉 국가와 지방자치단체는

첫째, 개인정보 목적 외의 수집, 오남용, 무분별한 감시와 추적 등에 따른 피해를 방지하기 위해 노력해야 하며(법 제5조 제1항),

둘째, 정보주체의 권리보호를 위해 법령개선 등을 강구해야 한다(법 제5조 제2항).

나아가 셋째, 개인정보처리자의 자율적인 개인정보 보호활동을 촉진·지원을 하여야 한다(제5조 제3항).

| |
|---|
| <p>법 제5조(국가 등의 책무) ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 피해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.</p> <p>② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.</p> |
|---|

- ③ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.
- ④ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 이 법의 목적에 부합되도록 하여야 한다.

2. 개인정보 보호정책 수립

개인정보 보호법 제2장(제7조 ~ 제14조)에서는 개인정보를 보호하기 위한 다양한 정책들에 대해서 규정하고 있다. 기본적으로 개인정보 보호정책을 수립하고 심의·의결하는 기구로는 '개인정보 보호위원회(이하 '보호위원회'라 함)'를 두고 있는데, 이러한 개인정보 보호위원회는 어떻게 구성되는지(제7조의2), 위원장은 어떤 역할을 수행하여야 하며(제7조의3), 위원들의 결격사유(제7조의7) 및 제척·기피·회피 사유(제7조의11) 등을 서술하고 있다. 다음 보호위원회의 소관 사무(제7조의8) 및 심의·의결사항(제7조의9)과 함께 소위원회구성(제7조의12), 운영 등(제7조의14)에 대해서도 설명하고 있다.

| 제2장 개인정보 보호정책의 수립 등 | |
|---------------------|--------------------|
| 제7조 개인정보 보호위원회 | 제7조의12 소위원회 |
| 제7조의2 보호위원회의 구성 등 | 제7조의13 사무처 |
| 제7조의3 위원장 | 제7조의14 운영 등 |
| 제7조의4 위원의 임기 | 제8조 삭제 <2020.2.4.> |
| 제7조의5 위원의 신분보장 | 제8조의2 개인정보 침해요인 평가 |
| 제7조의6 겸직금지 등 | 제9조 기본계획 |
| 제7조의7 결격사유 | 제10조 시행계획 |
| 제7조의8 보호위원회의 소관 사무 | 제11조 자료제출 요구 등 |
| 제7조의9 보호위원회의 심의·의결 | 제12조 개인정보 보호지침 |
| 제7조의10 회의 | 제13조 자율규제의 촉진 및 지원 |
| 제7조의11 위원의 제척·기피·회피 | 제14조 국제협력 |

1) 개인정보 보호위원회의 소관사무

구체적으로 보호위원회는 첫째, 개인정보보호와 관련된 법령의 개선, 둘째, 개인정보보호 관련 정책·제도·계획수립·집행에 관한 사항, 셋째, 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항, 넷째, 개인정보처리와 관련한 고충처리·권리구제 및 관련 분쟁조정에 관한 사무를 수행한다. 또한 다섯째, 개인정보보호를 위한 국제기구 및 외국의 관련 기구와의 교류 및 협력을 수행하며, 여섯째, 개인정보보호에 관한 법령·정책·제도·실태 등의 조사·연구 뿐만 아니라, 교육 및 홍보에 관한 사항도 개인정보 보호위원회가 수행한다.

[표 #: 개인정보 보호위원회의 소관 사무]

법 제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다.

1. 개인정보의 보호와 관련된 법령의 개선에 관한 사항

2. 개인정보 보호와 관련된 정책·제도·계획 수립·집행에 관한 사항
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항
4. 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력
6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보에 관한 사항
7. 개인정보 보호에 관한 기술개발의 지원·보급 및 전문인력의 양성에 관한 사항
8. 이 법 및 다른 법령에 따라 보호위원회의 사무로 규정된 사항

[본조신설 2020. 2. 4.]

2) 개인정보 보호위원회의 심의·의결사무

또한 보호위원회는 심의·의결하는 성격을 갖는데, 구체적으로는 개인정보에 대한 정책수립, 개인정보처리에 관하여 공공기관 간의 의견조정, 법령해석 및 운용, 과징금부과, 개선권고, 시정조치, 고발 및 징계권고, 과태료부과 등에 대한 다양한 사항들에 대해 심의·의결을 하는 역할을 수행한다.

[표 #: 개인정보 보호위원회의 심의·의결 사항]

법 제7조의9(보호위원회의 심의·의결 사항 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획에 관한 사항
3. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
4. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
5. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
6. 제18조 제2항 제5호에 따른 개인정보의 이용·제공에 관한 사항
7. 제33조 제3항에 따른 영향평가 결과에 관한 사항
8. 제28조의6, 제34조의2, 제39조의15에 따른 과징금 부과에 관한 사항
9. 제61조에 따른 의견제시 및 개선권고에 관한 사항
10. 제64조에 따른 시정조치 등에 관한 사항
11. 제65조에 따른 고발 및 징계권고에 관한 사항
12. 제66조에 따른 처리 결과의 공표에 관한 사항
13. 제75조에 따른 과태료 부과에 관한 사항
14. 소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
15. 개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
16. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항

② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다.

1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로 부터의 의견 청취
2. 관계 기관 등에 대한 자료제출이나 사실조회 요구

③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 있으면 이에 따라야 한다.

④ 보호위원회는 제1항제3호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다.

⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.

[본조신설 2020. 2. 4.]

3. 개인정보 보호위원회의 계획수립

보호위원회는 개인정보의 보호 및 정보주체의 권익보장을 위하여 3년마다 개인정보보호 기본계획을 관계 중앙행정기관의 장과 협의하여 수립하여야 한다(제9조). 그리고 이런 기본계획에는 개인정보 보호의 기본목표와 추진방향이 무엇인지, 개인정보 보호 관련 제도 및 법령개선을 어떻게 할 것인지, 개인정보 침해방지를 위한 대책이 무엇인지, 개인정보 보호에 대한 자율규제의 활성화방안이 무엇인지, 그리고 교육·홍보의 활성화 및 개인정보보호를 위한 전문인력 양성 등에 대한 구체적인 계획이 포함되어야 한다.

나아가 중앙행정기관의 장은 이러한 보호위원회의 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하여야 하고, 시행계획을 받은 보호위원회가 이를 심의·의결을 한 후, 시행하도록 하고 있다(제10조)

4. 보호위원회 등의 자료제출 의견진술요구권

보호위원회는 위에서 살펴봤던 기본계획을 효율적으로 수립하기 위해, 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 등에게 개인정보 처리자의 법규 준수현황과 개인정보 관리 실태 등에 관한 자료제출이나 의견진술 등을 요구할 수 있다(제11조 제1항). 또한 필요한 경우 보호위원회는 개인정보처리자 및 공공기관(관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등)을 대상으로 개인정보관리 수준 및 실태파악 등을 위해 조사를 실시할 수 있기도 하다(제11조 제2항).

뿐만 아니라 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위해 소관 분야의 개인정보처리자에게 법규준수 현황 및 개인정보 관리실태 등에 따른 자료제출도 요구할 수 있다(제11조 제3항). 그리고 이처럼 보호위원회 또는 중앙행정기관의 장으로부터 자료제출 등을 요구받은 경우에는 이를 따르도록 규정하고 있다(제11조 제4항)

법 제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.

<개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

② 보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다. <신설 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다. <개정 2015. 7. 24.>

④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다. <개정 2015. 7. 24.>

⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다. <개정 2015. 7. 24.>

5. 자율규제 촉진 및 지원 (제13조)

한편 개인정보 보호법은 개인정보 보호를 위한 노력이 보호위원회의 개인정보처리자들에 대한 하향식의 강권만이 아닌, 개인정보처리자들로 하여금 스스로 자율적으로 규제를 하게끔 유도하고 있다. 즉 보호위원회로 하여금 이들 개인정보처리자들이 자율적인 개인정보 보호활동을 하도록 촉진하고 지원하도록

첫째, 개인정보 보호에 관한 교육과 홍보,

둘째, 개인정보 보호와 관련된 기관과 단체를 육성 및 지원,

셋째, 개인정보 보호 인증마크의 도입과 시행지원,

넷째, 개인정보처리자의 자율적 규약의 제정 및 시행을 지원하고,

다섯째, 그밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위해 필요한 사항들을 마련하도록 규정하고 있다.