# 개인정보 유출 사고 발생 시 기업이 지켜야 할 의무사항

안녕하세요. 한도형 변호사입니다.

최근 SK 텔레콤, YES24 등 주요 기업에서 연이어 개인정보 유출 사고가 발생하면서 사회적 우려가 다시 확산되고 있습니다. 개인정보보호위원회에 따르면 2024 년 한 해 동안 접수된 유출 신고 307 건 중 67%가 해킹에 의한 것으로 나타났습니다. 그러나 실제 사례를 보면, 개인정보 유출은 웹 취약점 악용뿐 아니라 개인정보취급자의 부주의가 원인이 된 경우도 적지 않습니다. 대표적으로 이메일 주소 오기재나 개인정보 파일을 공개 웹페이지에 업로드한 사례가 이에 해당합니다.

따라서 기업은 사전에 관리 체계를 정비해 개인정보 유출 사고를 예방하는 동시에, 발생에는 법적 대응을 신속히 이행해야 합니다. 이번 연구자료에서는 **개인정보 유출 사고가 발생했을 때 기업이 준수해야 할 통지 및 신고의무**에 대해 살펴보겠습니다.

## 개인정보 보호법상 통지 및 신고의무

개인정보의 분실, 도난, 유출(이하 '유출 등')이 발생한 경우 아래와 같이 통지 및 신고의무를 이행해야 하며, 이를 위반한 경우 3 천만 원 이하의 과태료가 부과될 수 있습니다.

- 통지의무: 개인정보처리자는 유출 등의 사실을 알게 된 때로부터 72시간 이내에 정보주체에게 유출 등을 통지해야 함
- 신고의무: 개인정보보호위원회 또는 한국인터넷진흥원(KISA)에 신고해야 함

개인정보 주체에 대한 통지의무와 개인정보보호위원회 또는 한국인터넷진흥원(KISA)에 대한 신고의무에 관한 구체적인 내용은 다음과 같습니다.

| | 통지의무 | 신고의무 |
|---|---|---|
| **의무자** | 개인정보처리자 | |
| **요건** | 1명 이상의 개인정보 유출 등 | *아래 중 어느 하나에 해당하는 경우<br>1. 1천 명 이상의 개인정보 유출 등<br>2. 민감정보, 고유식별정도 유출 등<br>3. 외부로부터 불법적인 접근에 의한 개인정보 유출 등 |
| **방법** | · 서면, 전자우편, 팩스, 전화, 문자전송 등의 방법으로 개인정보 주체에게 개별 통지(단, 정보주체의 연락처를 알 수 없는 경우 홈페이지에 30일 이상 게시) | · 개인정보 포털(privacy.go.kr)을 통해 개인정보 보호위원회 또는 한국인터넷진흥원(KISA)에 신고 |
| **항목** | 1. 유출 등이 된 개인정보의 항목 | 1. 정보주체에의 통지여부 |

| | | |
|---|---|---|
| | 2. 유출 등이 된 시점과 경위<br>3. 개인정보처리자의 대응조치 및 피해 구제절차<br>4. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차<br>5. 담당부서 및 연락처 등 | 2. 유출 등이 된 개인정보의 항목과 규모<br>3. 유출 등이 된 시점과 경위<br>4. 개인정보처리자의 유출 등에 따른 피해 최소화 대책·조치 및 결과<br>5. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차<br>6. 담당부서 및 연락처 등 |
| **이행기한** | 유출 등을 알게 된 때부터 72시간 이내 | |

## 신용정보회사 등의 신고의무

신용정보법의 이용 및 보호에 관한 법률(이하 '신용정보법')에 따른 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관, 신용정보제공·이용자(이하 '신용정보회사 등')는 아래와 같은 통지 및 신고의무를 이행해야 하며, 이를 위반한 경우에는 3천만 원 이하의 과태료가 부과될 수 있습니다.

- 통지의무: 개인신용정보가 누설되었음을 알게 된 때로부터 72시간 내에 신용정보주체에게 누출을 통지해야 함
- 신고의무: 금융위원회 또는 개인정보보호위원회에 신고해야 함

**개인신용정보가 누설된 경우에는 신용정보법이 개인정보 보호법에 우선하여 적용**되며, 구체적인 내용은 다음과 같습니다.

| | **통지의무** | **신고의무** |
|---|---|---|
| **의무자** | 신용정보회사 등 | |
| **요건** | 1명 이상의 개인신용정보 누설 | 1만 명 이상의 개인신용정보 누설 |
| **방법** | · 서면, 전자우편, 전화, 문자전송 등의 방법으로 정보주체에게 개별 통지 | · 상거래기업 및 법인(금융위원회의 감독을 받지 않는 신용정보 제공·이용자)의 경우 개인정보 포털(privacy.go.kr)을 통해 개인정보 보호위원회 또는 한국인터넷진흥원(KISA)에 신고<br><br>· 상거래기업 및 법인을 제외한 신용정보회사 등은 금융위원회에 신고 |
| **항목** | 1. 누설된 된 개인신용정보의 항목<br>2. 누설된 시점과 경위<br>3. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차<br>4. 신용정보회사 등의 대응조치 및 피해 구제절차<br>5. 담당부서 및 연락처 등 | |
| **이행기한** | 누설을 알게 된 때부터 72시간 이내 | |

## 정보통신서비스 제공자의 침해사고 신고의무

‘**정보통신서비스 제공자**’란 전기통신 사업법상의 전기통신사업자(기간통신사업자, 부가통신사업자)와 영리목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보제공을 매개하는 자를 말하므로, 그 범위가 매우 넓습니다. 일반적으로 홈페이지, 어플리케이션 등을 통해 서비스를 제공하는 사업자라면 정보통신서비스 제공자에 해당합니다.

정보통신망의 이용 및 촉진에 관한 법률(이하 ‘정보통신망법’)에 따르면 정보통신서비스 제공자는 침해사고*가 발생한 경우 과학기술정보통신부장관 또는 한국인터넷진흥원(KISA)에 신고해야 합니다. 개인정보가 유출되지 않은 경우에도 침해사고가 발생했다면, 정보통신서비스 제공자는 한국인터넷진흥원(KISA) 보호나라 홈페이지(boho.or.kr)를 통해 정보통신망법상의 신고의무를 이행해야 하며, 이를 위반한 경우 3 천만 원 이하의 과태료가 부과될 수 있습니다.

*정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 발생한 사태를 의미

**정보통신망법상의 신고의무는 개인정보 보호법, 신용정보법과 달리 침해사고 발생을 알게 된 때부터 24 시간 이내에 이행되어야 합니다**. 따라서 정보통신서비스 제공자는 개인정보의 유출 등이 침해사고로 인한 경우 그 사실을 안 때로부터 24 시간 내에 정보통신망법상의 신고절차를 이행해야 한다는 점을 유의해야 합니다.

## 결론

법령은 개인정보 유출 사고 발생 시 개인정보처리자에게 통지 및 신고 의무를 부과하고 있습니다. 따라서 기업은 사고 발생 시 즉시 대응체계를 가동하여 관련 의무를 적시에 이행해야 하며, 이를 통해 법적 리스크와 평판 피해를 최소화해야 합니다. 또한 복수의 법령이 동시에 적용될 수 있는 만큼, 초기 단계부터 전문가의 조력을 받아 체계적으로 대응하는 것이 바람직합니다.



**한도형 변호사**
*Partner*
dohyung.han@seumlaw.com