Korean

information and privacy commission new south wales

안내지

2023년 11월

MNDB 제도 관련 자주 묻는 질문

이 정보는 누구를 위한 것인가요?	데이터 유출 의무 알림 제도에 대한 정보를 찾고 있는 NSW 주민들
왜 이 정보가 중요한가요?	이 안내지는 주민들이 본 제도를 더 잘 이해하고, 개인 정보 관련 데이터 유출이 발생했을 때 자신들의 권리가 무엇인지 이해하는 데 도움이 됩니다.

데이터 유출 의무 알림 제도란 무엇인가요?

데이터 유출 의무 알림 제도(MNDB Scheme)는 NSW 정부 기관을 대상으로 하는 *1998년 제정 사생활 및 개인 정보 보호법* (PPIP Act)에 따라 '해당 데이터 유출' 사건 발생시 의무적으로 피해자에게 알리도록 하는 제도입니다.

MNDB 제도는 언제 시작했나요?

MNDB 제도는 2023년 11월 28일에 시작했습니다.

MNDB 제도는 누구에게 적용되나요?

MNDB 제도는 연방 개인정보 보호 법률의 적용을 받지 않는 NSW 공공 부문 기관, 장관, 대학, 지방 자치 단체 및 주정부 소유 공기업에 적용됩니다.

데이터 유출 정책이란 무엇인가요?

데이터 유출 정책(DBP)은 기관이 데이터 유출에 대응하는 방법을 명시한 문서상 정책 또는 계획입니다. 법에 따라 기관은 DBP를 보유해야 합니다. DBP는 데이터 유출 관리에 대한 해당 기관 직원의 역할과 책임, 유출 발생 시 기관이 따라야 하는 절차를 명시해야 합니다.

기관은 DBP를 공개 열람이 가능하도록 해야 하며, 그렇기 때문에 기관 웹사이트에 DBP를 게재해야 합니다.

'해당 데이터 유출'이란 무엇인가요?

MNDB 제도에 따라, 기관은 해당 데이터 유출 발생 시 피해를 본 개인과 개인정보 보호 행정청장에게 통보해야 합니다.

'해당 데이터 유출'은 다음과 같은 경우에 해당합니다.

- 기관이 보유한 개인 정보에 대한 무단 접근 또는 무단 공개가 발생하여 해당 정보와 관련된 개인에게 **심각한 피해**를 초래할 가능성이 높은 경우
- 기관이 보유한 개인 정보를 분실하고, 무단 열람 또는 공개가 발생할 가능성이 높고 해당 정보와 관련된 개인에게 **심각한 피해**를 초래할 가능성이 높은 경우.

심각한 피해란 무엇인가요?

심각한 피해는 신체적, 재정적, 물질적 피해, 정서적 또는 심리적 피해, 또는 평판의 손상을 포함할 수 있습니다. 피해의 영향은 사람마다 다를 수 있지만 다음과 같은 경우를 포함할 수 있습니다:

- 사기로 인한 재정 손실
- 가학적인 전 배우자에 의한 신체적 또는 심리적 피해의 위험
- 재정 및/또는 신용 기록에 영향을 미칠 수 있는 신원 도용
- 개인 평판에 심각한 피해.

데이터 유출은 어떻게 발생할 수 있나요?

전반적으로 데이터 유출은 인간의 오류, 시스템 실패 또는 악의적 또는 사이버 유출로 인해 발생할 수 있습니다.

데이터 유출의 예시는 무엇인가요?

데이터 유출의 몇 가지 예시는 다음과 같습니다:

사람이 저지른 실수:

- 편지나 이메일이 엉뚱한 수신인에게 발송됨.
- 승인되지 않은 사람에게 시스템 접근이 잘못 부여되거나, 비밀번호 보호가 적절하지 않음.
- 개인 정보가 포함된 물리적 자산이 분실되거나 엉뚱한 곳에 둔 경우 (예: 기록, 노트북, USB, 전화기).

시스템 오류:

- 인증 없이 시스템 접근이 가능한 코딩 오류가 있거나 자동으로 공지가 생성됨.
- 알려진 지원 대상 패치가 적용되지 않아 시스템이 유지되지 않음.

악의적 또는 범죄적 공격:

- 사이버 사건 (예: 랜섬웨어, 맬웨어, 해킹, 피싱, 브루트 포스 접근 시도).
- 사회 공학/사칭으로 인한 부적절한 개인 정보 공개.
- 내부 위협(직원)이 유효한 자격 증명을 사용하여 자신의 직무나 권한 범위를 벗어난 개인 정보에 접근하거나 이를 공개.

기관은 개인정보 보호 행정청장에게 통보해야 합니까?

데이터 유출이 해당 데이터 유출로 평가된 경우, 기관은 IPC 웹사이트에 있는 양식을 사용하여 즉시 개인정보 보호 행정청장에게 통보해야 합니다.

해당 데이터 유출로 피해를 본 경우 통보를 받을 수 있나요?

기관이 귀하의 개인 정보와 관련된 해당 데이터 유출이 발생했다고 판단한 경우, 가능한 한 빨리 그 유출에 대해 귀하에게 통지해야 합니다. 이는 기관이 귀하에게 서면으로 통지하고 해당 데이터 유출에 대한 정보를 제공해야 한다는 뜻입니다. 여기에는 다음과 같은 것이 포함됩니다:

- 기관이 귀하에게 발생한 피해를 통제하거나 완화하기 위해 취했거나 계획하고 있는 조치
- 해당 데이터 유출 이후 본인이 고려해야 할 조치
- 기관의 행동에 대한 내부 검토를 요청하거나 개인정보 보호 행정청장에게 개인정보 보호 관련 불만을 제기하는 방법에 대한 정보.

데이터 유출 후 얼마나 빨리 통지를 받을 수 있나요?

기관이 해당 데이터 유출이 발생했을 가능성이 있다고 합리적으로 의심하는 경우, 기관은 다음과 같은 일련의 조치를 취해야 합니다:

- 유출로 인한 피해 확산을 막기 위해 모든 합리적인 노력을 기한다.
- 기관이 보유한 개인 정보에 대한 무단 접근, 공개 또는 손실이 있는지 30일 이내에 평가한다.
- 피해를 본 개인에게 심각한 피해가 발생할 가능성이 있는지 30일 이내에 평가한다.
- 유출이 일어났다고 의심이 되는 경우 그로 인한 피해를 완화하기 위해 모든 합리적인 노력을 기울인다.

위 단계를 수행한 후, 기관이 귀하의 개인 정보와 관련된 해당 데이터 유출이 발생했다고 결론을 내린다면, 가능한 한 빨리 그 유출에 대해 귀하에게 통지해야 합니다.

기관이 데이터 유출에 대해 나에게 통지하려해도 더 이상 내 연락처가 없다면 어떻게 됩니까?

기관은 MNDB 제도에 따라 다른 공공 부문 기관에 관련 개인 정보를 요청할 수 있는 정보 공유 권한이 있습니다. 기관이 요청할 수 있는 정보는 데이터 유출 피해를 본 개인의 이름과 연락처를 확인하는 데 합리적으로 필요한 정보로 제한됩니다.

그러나 기관이 귀하에게 직접 통지할 수 없는 경우, 웹사이트에 통지를 게시하고 통지 사항을 알리기 위해 합리적인 조치를 취해야 합니다. 통지는 최소 12개월 동안 기관의 공공 통지 등록부에 남아 있어야 합니다.

기관이 나에게 통지하지 않을 이유가 있나요?

있습니다. 기관이 데이터 유출로 피해를 본 개인에게 통지해야 할 의무가 면제되는 특정 상황이 있습니다. 예를 들어, 기관이 신속하게 데이터 유출 피해를 완화하는 조치를 취하고 이로 인해 데이터 유출이 심각한 피해를 초래할 가능성이 없는 경우, 피해를 본 개인에게 통지할 의무가 없습니다.

통지 후 기관에서 지원하는 게 있나요?

통지 후 기관이 제공할 수 있는 지원이나 도움 유형은 데이터 유출의 구체적 상황에 따라 다릅니다. 예시는 다음과 같습니다:

- 내용이 유출된 정부 발급 신원 문서 또는 자격 증명(예: 운전 면허증) 대체 시 필요한 지원.
- 개인 정보 보호 방법 조언.
- 추가 지원 및 상담 서비스 링크 제공.

통지를 받으면 어떻게 해야 하나요?

개인 정보를 보호하고 데이터 유출로 인해 피해를 입을 위험을 줄이기 위해 취할 수 있는 실질적인 조치가 있습니다. 취할 수 있는 조치의 종류는 데이터 유출 상황 및 관련 정보의 종류에 따라 다릅니다. 통지서에는 통지서에 명시된 유출 유형에 대해 취할 수 있는 조치를 추천하는 내용이 들어있습니다.

데이터 유출 또는 개인 정보 보호 방법에 대한 추가 정보가 필요한 경우, 귀하에게 통지를 보낸 기관에 문의해야 합니다.

추가 정보는 어디에서 찾을 수 있나요?

정보 및 개인정보 행정청 (IPC) 웹사이트 에 추가 정보 및 자료가 실려 있습니다. 아니면 아래 IPC 연락처로 문의하셔도 됩니다.

추가 정보를 원하시면

정보 및 개인정보 행정청(NSW IPC) 연락처:

무료전화: 1800 472 679

이메일: ipcinfo@ipc.nsw.gov.au

웹사이트: www.ipc.nsw.gov.au

참고: *이 안내지에 담긴 정보는 참조용으로만 사용해야 합니다. 개별 상황에 대해서는 법률 자문을 받아야 합니다.*