클라우드 기업 이용자 개인정보보호 수칙

서비스 이용 단계

하나 모든 부서가 클라우드 서비스의 도입 여부에 대한 의사결정에 참여하기

- 클라우드 서비스를 도입하는 과정에서 기술적 문제뿐 아니라, 개인정보 취급에 대한 법적 문제, 기업의 중요자산의 저장·관리 문제, 금전적 문제 등 복잡한 사안이 발생합니다.
- 따라서, IT부서, 법률부서, 영업부서 등 전 부서의 의견을 수렴하여 클라우드 서비스가 필요한지부터 검토해야 합니다.
- 클라우드 서비스를 도입하는 것이 필요하다고 결정하였다면 어떤 클라우드 서비스 제공자를 선택할지 정한 뒤 도입하는 전 단계에서 수렴된 의견을 반영되도록 합니다.

둘 클라우드 서비스 담당자 지정하기

- 클라우드 서비스를 도입할 때 확인·조치해야 할 사항이나 도입한 이후의 개인정보 분쟁 등이 발생할 수 있습니다.
- 이와 관련하여, 클라우드 서비스 담당자를 지정하여 운영하는 것이 필요합니다.
- 클라우드 서비스 담당자는 클라우드 서비스와 관련된 개인정보보호에 관한 사항을 충분히 숙지하여야 합니다.

셋 클라우드 서비스 도입에 따른 개인정보 위험 요소 분석하기

- 클라우드 서비스를 도입하면 개인정보는 자사 서버가 아닌 클라우드 서비스 제공자 측의 서버에 저장되므로 이에 따른 개인정보의 위험 요소를 분석할 필요가 있습니다.
- 클라우드 서비스 제공자의 데이터 접근 수준, 접근 방식(읽기권한, 읽고 쓰기 권한, 쓰기 권한), 서버의 지리적 위치에 따른 위험, SLA의 협상가능성, 개인정보 관련 법령의 준수 여부 및 감사 기능 제공 여부 등을 분석해야 합니다.

도입 단계

넷 데이터의 접근제한 및 서비스 해지시 데이터 삭제 등 자사 데이터의 보호에 관한 사항을 계약서에 명시하기

- 클라우드 서비스로 관리되는 데이터에는 자사 고객의 개인정보나 지적재산권을 가지는 저작물 등이 포함될 수 있습니다.
- 따라서, 클라우드 서비스 제공자가 자사의 데이터에 임의적으로 접근·이용·가공하거나 상업적으로 활용하지 않도록 계약서에 명시해야 합니다.
- 또한, 클라우드 서비스의 이용계약을 해지할 경우에도 클라우드 서비스 제공자가 보유하고 있는 자사의 데이터를 완전 삭제하도록 명시적으로 계약서에 넣는 것이 필요합니다.

다섯 클라우드 서비스의 데이터 저장 위치와 국내 법규의 준수 여부를 확인하기

- 클라우드 서비스의 데이터 저장 위치가 해외이면 통제권을 행사하기 곤란한 상황이 발생할 수 있으며 국내법 위반에 따른 분쟁이 발생할 경우 해결이 어려울 수 있습니다.
- 따라서, 해외 클라우드 서비스를 도입하고자 한다면 국내에 지사가 설립되어 있는지, 국내법을 준수함을 명시적으로 제시하는지 등을 고려하여 신중히 선택하도록 합니다.

여섯 클라우드 서비스가 이용자에게 자원의 독립성을 제공하는지 확인하기

- 클라우드 서비스를 이용하는 다수 이용자가 하나의 물리적 서버를 공동으로 사용하게 되므로 다른 이용자가 자사의 데이터에 접근할 수 있습니다.
- 따라서, 클라우드 서비스 제공자가 자사의 데이터에 다른 이용자가 임의적으로 접근할 수 없도록 논리적 분리 등 자원의 독립성을 보장하는지 확인하셔야 합니다.

일곱 클라우드 서비스 제공자의 보안수준 및 서비스 보안옵션 등을 정확히 파악하여 선택하기

- 클라우드 서비스 제공자의 보호조치가 미흡하면 해킹에 의해 자사의 데이터가 유출될 위험성이 있으므로 신뢰할 수 있는 클라우드 서비스 제공자를 선택하는 것이 필요합니다.
- 그리고, 기본 서비스 이외에도 강화된 보안기능을 옵션으로 받을 수도 있습니다.
- 따라서, 보안옵션 내용을 정확하게 확인하고 개인정보를 취급하는 서비스 등의 경우 필요한 보안 옵션을 선택하는 것이 필요합니다.

이용 단계

여덟 클라우드 서비스 제공자에게 개인정보를 취급위탁하는 사실과 클라우드 서비스의 서버 위치, 분쟁 발생시 처리 절차 등을 이용자에게 고지하기

- 고객의 개인정보가 클라우드 서비스의 서버 상에 저장·처리될 경우 정보통신망법에 따라 다음 사항을 이용자에게 고지하여야 합니다.
  ① 이용하는 클라우드 서비스 제공자 및 클라우드 서비스에서 처리되는 내용
  ② 개인정보와 관련한 분쟁발생시 처리 절차 및 담당자 연락처
- 만약, 클라우드 서비스의 서버 위치가 국외에 있을 경우에는 서버가 위치하고 있는 국가, 해당 서버에 저장되는 개인정보의 종류 등을 명시하여 동의를 받아야 합니다.

아홉 개인정보 등 중요 데이터를 암호화하여 저장·전송하기

- 해킹으로부터 개인정보를 안전하게 보호하기 위해서는 시스템 상에 개인정보를 암호화하여 저장하고 전송 과정에서도 암호화하는 것이 중요합니다.
- 이를 위해서 클라우드 서비스 제공자가 암호화 송수신 및 저장 기능을 제공하는지 확인하고 만약 제공하지 않는다면 자체적으로 암호화 송수신 및 저장 방법을 마련하고 이용해야 합니다.

열 클라우드 서비스에 저장한 데이터에 대해 해당 클라우드 서비스 제공자나 다른 이용자가 임의로 접근하고 있지 않은지 정기적으로 확인하기

- 자사의 데이터에 대해, 해당 클라우드 서비스 제공자가 접근하지 않는다는 사실이 계약서에 명시되어 있더라도, 실제로 접근 여부에 대해 확인하여야 합니다.
- 또한, 해당 클라우드 서비스를 이용하는 다른 이용자가 자사의 데이터 접근 가능한지에 대해서도 확인해야 합니다.
- 이와 같이 자사의 데이터에 대한 부적절한 접근 여부를 확인할 수 있도록 서비스 이용전에 접근기록이 제공되는지 확인하여야 합니다.

계약 해지 단계

열하나 클라우드 서비스 계약 해지시 자사의 데이터 회수하고 완전 삭제에 대한 확인서 받기

- 클라우드 서비스에 대한 계약을 해지할 때에는, 자사의 데이터 및 보안토큰 등 물리적 장비 등을 재사용할 수 있는 형태로 회수 받아야 하며 클라우드 서비스 제공자로부터 저장된 데이터가 복구불가능한 형태로 완전 삭제했다는 확인서를 받아 두는 것이 필요합니다.