방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011. 7.18.(월)

보도자료

2011년 7월 18일(월) 배포시점부터 보도하여 주시기 바랍니다.

문의 : 네트워크정책국 개인정보보호윤리과 김광수 과장(☎750-2770)
개인정보보호윤리과 김지원 사무관(☎750-2775) aquarius@kcc.go.kr

방통위, 클라우드 개인정보보호 수칙(안) 마련

- 7.31까지 개인정보보호 포탈(i-privacy.kr)을 통해 공개 의견수렴 진행 -

방송통신위원회와 한국인터넷진흥원은 클라우드 서비스의 확산에 대비하여 개인정보 침해에 선제적으로 대응하기 위해 “클라우드 서비스 개인정보보호수칙(안)”을 마련하고 18일부터 개인정보보호 포탈(www.i-privacy.kr)을 통해 이에 대한 의견 수렴을 진행한다고 밝혔다.

클라우드 개인정보보호 수칙은 정부·학계·업계 등 관계 전문가로 구성된 연구반을 통해 만들어졌으며, 클라우드 서비스와 관련한 주체별로(기업 이용자, 개인 이용자, 클라우드 서비스 제공자) 약 10여개의 필요한 보호수칙을 포함하고 있다.

주요 내용을 살펴보면, ▲기업 이용자 수칙은 클라우드 도입에 따른 위험요소 사전분석, 서비스 계약시 데이터 접근제한 명시, 서비스 해지시 데이터 회수 및 삭제 등 클라우드 서비스의 도입부터 해지까지 단계별로 기업에서 고려해야 할 사항을 담았다. ▲개인 이용자 수칙은 클라우드 서비스의 데이터 처리방침 확인, 개인정보가 포함된 파일의 공유 주의 등 이용자의 주의사항을 담고 있다. 마지막으로, ▲클라우드 서비스 제공자 수칙은 데이터 저장 위치 등의 명확한 고지, 제3자로부터 주기적인 점검, 해지 고객 데이터의 완전 삭제 등을 안내하고 있다.

방송통신위원회와 한국인터넷진흥원은 7월 18일부터 7월 31일까지 동 수칙(안)에 대한 관련 사업자, 이용자들의 의견을 수렴하고 내달 초에 최종안을 확정·배포할 계획이다.

방송통신위원회와 한국인터넷진흥원은 “클라우드 서비스 개인정보 보호수칙”을 통해 클라우드 서비스에 대한 사업자 및 개인의 주의를 환기하고 클라우드 서비스의 건전한 발전에 기여할 것임을 밝혔다.

붙임 : 1. 클라우드 기업 이용자 개인정보보호 수칙(안) 1부
2. 클라우드 개인 이용자 개인정보보호 수칙(안) 1부
3. 클라우드 서비스 제공자 개인정보보호 수칙(안) 1부. 끝.

[붙임1]

클라우드 기업 이용자 개인정보보호 수칙(안)

□ 사전준비 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 의견이 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.

[붙임2]

클라우드 개인 이용자 개인정보보호 수칙(안)

□ 서비스 가입 단계

하나, 클라우드 서비스를 이용하고자 할 경우, 서비스 제공자가 해외 사업자인지 국내 사업자인지 확인하고 선택하기

- 해외 클라우드 사업자는 클라우드 서비스를 제공함에 있어 개인정보보호 등 국내관련 법규를 따르지 않을 수 있습니다.
- 이 경우 국내법에 따라 개인정보가 보호받지 못 할 수 있으므로 클라우드 서비스를 선택 할 때에 이 점을 주의해야 합니다.

둘, 클라우드 서비스 제공자의 데이터 처리 방침 확인하기

- 클라우드 서비스 제공자가 이용자 데이터를 접근, 이용, 또는 가공하는지를 확인하여 이용자 데이터를 임의적으로 처리하지 않는 클라우드 서비스를 이용하셔야 자신의 데이터가 보호받을 수 있습니다.
- 또한, 이용자 데이터의 소유권도 반드시 확인하여야 합니다.

셋, 클라우드 서비스 제공자의 개인정보취급방침 확인하기

- 사업자가 회원가입 등의 과정에 개인정보를 수집하고자 할 경우, 개인정보 정책과 개인정보 담당자의 연락처 등을 개인정보취급방침 상에 공개해야 합니다.
- 따라서, 이용자는 클라우드 서비스를 이용하기 전에 자신의 개인정보가 어떻게 보호되는지 개인정보취급방침으로 확인하고 서비스를 이용해야 합니다.
- 특히, 국내법을 따르지 않는 글로벌 사업자의 클라우드 서비스를 이용할 때는 개인정보가 무분별하게 이용되지 않도록 개인정보의 관리·이용 방법을 사전에 확인하도록 합니다.

□ 서비스 이용 단계

넷, 클라우드 서비스에서 공유 기능을 제공할 경우 개인정보가 들어있는 파일 등이 공유되지 않도록 조심하기

- 클라우드 서비스는 이용자의 편의를 위해서 데이터를 다른 이용자와 공유하는 기능을 제공하는 경우도 있습니다.
- 공유 기능이 제공되는 클라우드 서비스를 이용할 경우 개인정보가 들어있는 파일이나 중요 사생활 정보 등이 공유되지 않도록 주의를 기울여야 합니다.

다섯, 클라우드 서비스에 개인정보가 들어 있는 파일을 올릴 경우에는 암호화하기

- 개인정보나 중요한 문서를 클라우드 서비스로 관리할 경우 데이터의 안전한 보호를 위해 파일 암호화 등의 기능을 제공하는 클라우드 서비스를 선택하는 것이 좋습니다.
- 만약, 클라우드 서비스에서 암호화 기능을 제공하지 않는다면 문서 편집기 등에서 제공하는 암호화 기능을 활용하도록 합니다.

여섯, 비밀번호는 영문/숫자/특수문자 등을 조합하여 8자리 이상으로 설정하고 주기적으로 비밀번호 변경하기

- 클라우드 서비스 상에 중요 문서 또는 개인정보가 저장될 수 있으므로 비밀번호를 안전하게 관리하는 것이 중요합니다.
- 따라서 제3자가 쉽게 추측할 수 없도록 안전한 비밀번호를 사용하고 자주 변경해 주어야 하며 제3자가 쉽게 비밀번호를 획득하지 못하도록 합니다.

□ 서비스 탈퇴 단계

일곱, 서비스 탈퇴시 자신의 데이터를 삭제하는 방법을 확인하고 완전히 삭제한 후 탈퇴하기

- 클라우드 서비스를 해지할 때에는 그간에 보관·처리되어온 자신의 데이터가 타 용도로 사용되지 않도록 삭제하고 탈퇴하셔야 합니다.
- 이를 위해 서비스 탈퇴시 자신의 데이터가 자동 삭제되는지 자신이 일일이 삭제하고 탈퇴해야 하는지 데이터 취급방침을 확인한 후 데이터를 완전히 삭제하도록 합니다.

□ 피해 구제 및 기타

여덟, 클라우드 서비스 상에서 내 개인정보를 지키기 위한 권리를 적극적으로 행사하기

- 이용자는 클라우드 서비스 제공자에게 개인정보의 열람·정정·삭제 등을 요구할 수 있으며, 필요시 그 권리를 적극적으로 행사하도록 합니다.

아홉, 클라우드 서비스 이용 시 내 개인정보가 유·노출 또는 오·남용된 사실을 알게 된 때에는 e콜센터 ☎118에 도움을 요청하기

- 이용자는 클라우드 서비스 이용 중 개인정보 침해를 당한 경우 개인정보침해신고센터에서 운영하는 e콜센터 ☎118 등을 통해 신고하고 도움을 요청합니다.
- 아울러, 추가적인 개인정보 오남용 방지를 위해 비밀번호를 자주 변경하도록 합니다.

[붙임3]

클라우드 서비스 제공자 개인정보보호 수칙(안)

□ 정보 공개 원칙

하나, 데이터가 저장되는 서버의 국가 위치를 명확히 고지하기

- 클라우드 서비스 제공자의 서버는 물리적으로 여러 나라에 분산되어 있을 수 있고 이때 적용되는 개인정보보호 관련 법이 국내법과 상이할 수 있으므로 이용자가 정보통제권을 행사하기 어려울 수 있습니다.
- 따라서, 이용자 그 사실을 정확히 알 수 있도록 데이터 저장위치를 이용자에게 명확히 고지해야 합니다.

둘, 클라우드 서비스 제공자는 적용받는 개인정보 관련 법규를 고지하기

- 클라우드 서비스 제공자는 데이터 저장 위치나 사업자 등록 위치에 따라 국내법과 상이한 개인정보보호 법규를 따를 수도 있습니다.
- 따라서, 이용자에게 클라우드 서비스 제공자가 준수하는 개인정보 관련 법규를 명확히 안내해야 합니다.

셋, 고객이 저장한 데이터에 대한 처리 방침을 명확히 고지하기

- 클라우드 서비스 이용 고객의 데이터에는 저작물 등 지적재산권의 보호 대상이나 이용자의 개인정보가 포함되어 있을 수도 있습니다.
- 따라서, 원칙적으로 이용 고객이 클라우드 서버에 올린 데이터는 고객의 것으로 상업적 또는 별도의 목적으로 이용해서는 안 됩니다.
- 또한 서비스 해지 시에 데이터를 사용가능한 형태로 제공하고 서버상의 데이터는 완전 삭제하여야 합니다.
- 이와 관련하여 클라우드 서비스 제공자의 데이터 처리 방침을 고객에게 명확히 알려줘야 합니다.

□ 안전 확보의 원칙

넷, 명확하게 정의된 접근제어 기능 구비하기

- 시스템에는 내부 직원, 외부위탁 업체 직원, 서비스 이용 고객 등 다양한 사용자가 접근할 수 있습니다.
- 따라서, 클라우드 서비스의 접근제어는 중요한 사안으로 잘 정의된 방침과 자동화된 인증, 인가, 접근제어를 지원하여 부적절한 접근을 방지 하도록 합니다.
- 또한, 방화벽 등 네트워크 접근제어 및 접근 탐지 시설 등도 갖추어야 합니다.

다섯, 신뢰할 수 있는 제3자로부터 주기적으로 개인정보보호 기본 정책 및 표준의 이행 여부를 점검을 받고 고객에게 결과 제공하기

- 외부 감사를 통하여 개인정보보호 정책이 성실히 잘 이행되고 있음을 확인하고 그 증거를 고객에게 제공하여 클라우드 서비스의 신뢰성을 높이도록 합니다.

여섯, 고객 데이터에 임의적으로 접근하지 않고 불가피하게 접근해야 할 경우 접근 사유 등을 제시하기

- 고객의 데이터에는 개인정보 또는 지적재산권인 있는 정보 등이 있을 수 있으므로 원칙적으로 고객 데이터에 접근해서는 아니 됩니다.
- 부득이하게 고객 정보에 접근한 경우 접속 사유 및 접속기록 등을 고객에게 제공하여야 합니다.

일곱, 개인정보 및 고객 데이터를 보호하는 조직을 운영하고 내부관리계획을 수립·시행하기

- 내부 직원이 개인정보 및 고객 데이터에 대한 접근 권한을 가질 수 있으므로 내부 직원이 개인정보와 고객 데이터를 적절하게 취급하고 임의적으로 접근하지 못하도록 내부통제 장치를 갖추어야 합니다.
- 이를 위해 클라우드 서비스 제공자는 개인정보 및 고객 데이터 보호를 위한 조직을 운영하고 회사의 방침을 담은 내부관리계획을 수립하도록 합니다.
- 또한, 내부 직원의 교육도 주기적으로 시행하여 내부 직원의 개인정보보호 인식을 함양해야 합니다.

□ 이용 제한의 원칙

여덟, 고객이 저장한 개인정보 관련 자료를 임의적으로 이용, 변조, 훼손하지 않기

- 클라우드 서비스 이용 고객이 올린 개인정보 파일 또는 자료는 클라우드 서비스 제공자가 개인정보 주체의 소유로서 임의적으로 이용·변조·훼손해서는 안 됩니다.

아홉, 고객이 서비스를 해지할 때 고객 데이터 완전 삭제하기

- 고객이 서비스를 해지 할 때는 고객이 저장한 모든 데이터는 완전하게 삭제하는 것을 원칙으로 하고 해지고객의 데이터를 보관, 이용하지 않아야 합니다.

□ 이용자 권리 보호 원칙

열, 개인정보 분쟁이 발생할 때 문의할 수 있는 문의처 및 처리 절차를 알기 쉽게 알리고, 개인정보 분쟁 발생시 신속하게 피해구제하기

- 개인정보 분쟁 발생시 문의할 수 있는 문의처 및 처리 절차를 고객에게 알기 쉽게 고지하고 피해 발생시 신속하게 대처해야 합니다.