개인정보보호 내부관리 규정

2018년 3월 31일

㈜핑거

목 차

개인정보 보호 내부 관리 규정

제1장 총칙

제1조(목적)

이 규정은 「개인정보 보호법」 제24조 제3항 및 제29조와 같은 법 시행령 제21조 및 제30조, 정보통신망법 제28조 에 따라 개인정보처리자가 수집, 활용, 저장, 파기 등 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(적용범위)

본 규정은 개인정보를 취급하는 회사 임직원 및 외부 협력업체의 임직원, 프리랜서에 적용한다.

제3조(용어 정의)

이 규정에서 사용하는 용어의 뜻은 다음과 같다.

① "개인정보"란 살아있는 개인에 관한 정보로서 성명, 주민등록번호, 계좌번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라고 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

② "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

③ "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

④ "개인정보보호담당부서" 개인정보를 안전하고 효과적으로 보호하기 위한 개인정보보호 업무를 주도적으로 수행하는 부서를 의미한다.

⑤ "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

⑥ "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 개인정보보호법 시행령 제32조 제2항 제1호 및 제2호에 해당하는 자를 말한다.

⑦ "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

⑧ "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

⑨ "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

⑩ "개인정보처리시스템 개발/운영부서" 개인정보의 수집, 저장 및 사용을 위한 개인정보처리시스템을 개발, 운영하는 IT부서를 의미한다.

⑪ "내부망"이라 함은 물리적 망 분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

⑫ "비밀번호"라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

⑬ "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

⑭ "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

⑮ "P2P(Peer to Peer)"라 함은 정보통신망을 통해 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

⑯ "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.

⑰ "보조저장매체"라 함은 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

⑱ "위험도 분석"이란 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출 시 정보 주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

제2장 개인정보보호책임자의 의무와 책임

제4조(개인정보보호책임자의 지정)

개인정보보호책임자는 개인정보보호담당임원 또는 개인정보와 관련하여 이용자의 고충처리를 담당 하는 부서의 장 또는 개인정보 취급부서의 장이어야 한다.

제5조(개인정보보호책임자의 의무와 책임)

① 개인정보보호책임자는 다음 각호의 업무 수행을 위하여 필요한 권한 및 의무를 가진다.

1. 개인정보 주체의 개인정보 수집·이용·제공 및 관리에 관한 업무 총괄
2. 임직원 및 외부 인력에 의한 위법·부당한 개인정보 침해 행위에 대한 점검
3. 개인정보 주체로부터 제기되는 개인정보에 대한 불만이나 의견 처리 및 감독

② 기타 개인정보 보호에 필요한 사항

제6조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급부서의 장은 업무상 필요한 최소의 인력만을 개인정보취급자로 지정하여 개인정보 관련업무를 처리하도록 하여야 하며 개인정보취급자에 변동이 발생한 경우에는 즉시 개인정보보호담당 부서로 통보하여야 한다.

② 개인정보취급자이거나 개인정보취급자이었던 자는 직무상 알게 된 개인정보를 누설 혹은 훼손, 침해해서는 안된다.

③ 개인정보취급자의 상위 관리자는 해당 업무 처리가 관련 법규, 개인정보보호정책 등을

준수하는지 관리하여야 한다.

제3장 개인정보보호위원회 운영

제7조 (개인정보보호위원회 역할)

① 개인정보보호위원회를 통하여 회사 개인정보처리방침의 이행사항 및 담당자의 준수여부를 확인하여 문제가 발견될 경우 즉시 수정하고 바로 잡을 수 있도록 한다.

② 개인정보보호위원회는 개인정보 취급 관련 안정성 확보를 위해 정기적(분기 1회)으로 자체 감사를 실시한다.

③ 개인정보의 안전한 처리를 위하여 내부관리계획을 수립하고 시행한다.

제4장 개인정보의 처리단계별 기술적·관리적 안전조치

제8조(개인정보취급자 접근 권한 관리 및 인증)

① 개인정보처리시스템에 대한 접근권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여한다.

② 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

④ 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 한다.

제9조(비밀번호 관리)

개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립한다. 안전한 비밀번호란 제3자가 쉽게 추측할 수 없으며 비밀번호 해킹 등을

통해서도 비밀번호를 얻어낼 수 없거나 얻어내는데 많은 시간이 요구되는 것을 의미한다.

세부 비밀번호 작성규칙은 다음과 같다.

① 8자리 이상 문자 숫자 조합 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 중 2종류 이상으로 구성

② 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.

③ love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.

④ 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 3개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.

⑤ 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.

제10조(접근통제)

① 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치. 운영한다.

1. 개인정보처리시스템에 대한 접속 권한을 ID와 PW 그리고 IP(Internet Protocol)주소 등으로 제한하여 인가 받지 않은 접근을 제한한다.
2. 외부에서 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지한다.
3. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 다음과 같은 조치를 한다.
4. 개인정보취급자의 컴퓨터는 원칙적으로 P2P 프로그램. 공유 폴더 사용을 금지한다. 하지만 반드시 사용해야 할 경우 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.

5. 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터의 운영체제(OS :Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

※ Windows 접근통제 사용방법 : [제어판] → [Windows 방화벽]에서 '사용(권장)' 클릭

제11조(개인정보의 암호화)

① 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 제1항에 따른 개인정보를 정보통신망을 통하여 송. 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방

③ 향 암호화하여 저장하여야 한다.

④ 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 위험도 분석에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

⑥ 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

제12조(접근기록의 보관 및 위·변조 방지)

① 개인정보취급자가 개인정보처리시스템에 접속한 기록은 6개월간 보관·관리한다.

② 개인정보취급자의 접속기록은 위·변조 및 도난, 분실되지 않도록 하며 수시로 백업을 한다.

제13조(보안프로그램의 설치 및 운영)

① 악성 프로그램 등을 방지. 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치, 운영하며, 다음 각 호의 사항을 준수한다.

1. 보안 프로그램의 업데이트 실시

2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제14조(물리적 접근제한)

① 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우 이에 대한 출입통제 절차를 수립. 운영한다.

② 개인정보가 포함된 서류, 보조저장매체 등은 잠금 장치가 있는 안전한 장소에 보관하여야 한다.

제5장 개인정보보호 교육 및 훈련

제15조(개인정보보호 교육 및 훈련의 목적)

안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키고자 함을 위해 개인정보보호 교육을 시행한다.

제16조(개인정보보호 교육 및 훈련의 세부 사항)

① 개인정보보호 교육은 정기 보안교육에 반드시 포함되도록 하여야 하며 개인정보취급자 전체를 대상으로 실시되어야 한다.

② 개인정보를 취급하는 자는 매년 개인정보보호교육을 이수하여야 한다.

③ 개인정보보호교육은 최소 년 1회 이상 실시하여야 한다.

④ 신규로 지정된 자는 지정일로부터 6개월 이내에 개인정보보호교육을 이수하여야 한다.

⑤ 교육 방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등

다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할수도 있다.

⑥ 개인정보보호 교육내용 예시

1. 개인정보보호의 중요성 설명
2. 내부관리계획의 준수 및 이행
3. 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
4. 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
5. 개인정보의 기술적. 관리적 보호조치 이행
6. 개인정보보호 위반을 보고해야 할 필요성
7. 개인정보보호업무의 절차, 책임, 작업 설명
8. 개인정보보호 관련자들의 금지 항목들
9. 개인정보보호 준수사항 이행 관련 절차 등

제6장 개인정보 침해사고 발생시 조치

제17조 (개인정보 침해사고 조치)

개인정보 유출 시 지체 없이 개인정보 보호책임자에게 유출사실을 보고하고, 24시간내에 정보주체에게 유출사실을 통지해야 하며 행정자치부장관 또는 한국인터넷진흥원에 신고한다.

① 통지방법

1. 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법

② 조치방법

1. 유출된 개인정보 확산 및 추가유출 방지를 위하여 접속경로 차단, 취약점 점검, 보완.
2. 유출된 개인정보 삭제 등 긴급한 조치 필요 시 해당 조치를 먼저 취한 후 정보주체에게 통지 가능
3. 개인정보에 관한 권리, 이익을 침해 받은 사람은 행정자치부장관에게 침해사실을 신고할 수 있으며 해당 침해 신고가 접수된 경우 처리대장을 작성하여 관리한다.

부 칙

제1조 (시행일)

이 규정은 2016년 6월 1일부터 제정, 시행한다

부 칙

제1조 (시행일)

이 규정은 2018년 3월 31일부터 개정, 시행한다

[보안서약서_직원]

개인정보보호 서약서

본인 ( )는 업무 중에 알게 된 개인정보 및 회사의 업무와 관련된 정보에 대하여 업무 수행 중이나 업무 수행 후에도 비밀을 지킬 것을 서약합니다.

또한 회사에서 수집한 개인의 정보, 고객사의 개인정보, 고객사의 고객 개인정보 등 모든 개인정보의 보호를 위해 회사에서 정하는 개인정보보호 관리 규정을 준수할 것이며, 적정한 절차 없이 개인정보를 무단으로 조회, 누출하지 않을 것을 서약합니다.

개인정보 보호와 관련한 비밀의 준수와 개인정보보호를 위한 법적 준수기준인 "정보통신망이용촉진 및 정보보호에 관한 법률"에 명시된 모든 조항과 회사의 개인정보보호 관리 규정 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

일 시: 201 년 월 일

소 속:

성 명: (인)

[보안서약서_협력업체]

보안서약서

_____(이하 "을"이라 한다)는 (주)핑거 (이하 "갑"이라 한다)의 업무수행에 따른 개인의 정보, 고객사의 개인정보, 고객사의 고객 개인정보등 모든 개인정보 및 개인정보취급시스템(DBMS), 업무상 취득한 비밀 및 제반 보안사항을 타인 또는 타 기관에 누설하지 아니하며 엄수할 것을 서약하며, 안전한 보안을 위해 아래 각 호의 사항을 준수한다.

1. "을" 은 관련 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.

2. "을" 은 개인정보 보호와 관련한 비밀의 준수와 개인정보보호를 위한 법적 준수기준인 "정보통신망이용촉진 및 정보보호에 관한 법률"에 명시된 모든 조항과 회사의 개인정보보호 관리 규정 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

3. "을" 은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반 사항에 대하여 모든 책임을 부담한다.

4. 위 1~3가지 사항은 "을" 의 소속 임직원 및 기타 비 정규직, 아르바이트, 프리랜서등 을의 소속인 자는 모두 포함 된다.

5. 만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 모든 책임을 부담하고, 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

년 월 일

을.

업체명:

주소:

대표이사: (인)

[보안서약서_프리랜서]

보안서약서

_____(이하 "을"이라 한다)는 (주)핑거 (이하 "갑"이라 한다)의 업무수행 에 따른 개인의 정보, 고객사의 개인정보, 고객사의 고객 개인정보등 모든 개인정보 및 개인정보취급시스템(DBMS), 업무상 취득한 비밀 및 제반 보안사항을 타인 또는 타 기관에 누설하지 아니하며 엄수할 것을 서약하며, 안전한 보안을 위해 아래 각 호의 사항을 준수한다.

1. "을" 은 관련 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.

2. "을" 은 개인정보 보호와 관련한 비밀의 준수와 개인정보보호를 위한 법적 준수기준인 "정보통신망이용촉진 및 정보보호에 관한 법률"에 명시된 모든 조항과 회사의 개인정보보호 관리 규정 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

3. 만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 모든 책임을 부담하고, 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

년 월 일

을.

주소:

전화번호:

성명: (인)__