2019년 개인정보내부관리계획

2019. 1. 2.(수)

(주) 바 이 어 블 비 젼
대 표 조 원 진

1. 개인정보내부관리계획 총칙

가. 목적

○ 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행의무에 따라 제정된 것으로, ㈜바이어블비젼(이하 당사)가 취급하는 개인정보를 체계적으로 관리하고자 함

=> 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함

※ '행정자치부'에서 제시한 개인정보보호법 내부관리계획을 우리 당사 실정에 맞도록 반영

나. 적용 범위 (개인정보보호법 시행령 제2조 근거)

○ 본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(서면, 전화, 팩스 등)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 외부업체 직원에 대해 적용된다.

다. 용어 정의

○ "개인정보"라 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

○ "처리"란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

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

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

○ “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.

○ “개인정보 보호담당자”란 개인정보책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보보호 책임자가 일정 요건의 자격을 갖춘 이를 지정한다.

○ “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

○ “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

○ “영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유・무선망을 통하여 전송하는 일체의 장치를 말한다.

○ “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영・처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.

○ “영상정보처리기기 운영자”라 함은 개인정보 보호법 제25조제1항 각호에 따라 영상정보처리기기를 설치・운영하는 자를 말한다.

○ “영상정보 보호책임자”라 함은 개인영상정보의 처리에 관한 업무를 총괄해서 책임지는 자로서, 표준지침 제41조에 따라 영상정보처리기기 운영자가 지정한 자를 말한다.

2. 내부관리계획의 수립 및 시행

가. 내부관리계획 수립

○ 개인정보의 안전한 처리를 위하여 다음 사항을 포함하는 내부관리계획을 수립함

- 개인정보 보호책임자의 지정에 관한 사항
- 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보의 안전성 확보에 필요한 조치에 관한 사항
- 개인정보취급자에 대한 교육에 관한 사항
- 그 밖에 개인정보 보호를 위하여 필요한 사항

○ 내부관리계획 사항에 중요한 변경이 있을 경우 즉시 반영하고, 그 수정 이력을 관리하여야 함

나. 내부관리계획 시행

○ 개인정보처리자는 내부관리계획을 개인정보 관련 모든 직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 함

3. 개인정보 보호책임자의 의무와 책임

가. 개인정보보호 책임자 등 지정 및 임무

○ 당사의 개인정보보호법 시행령 제32조2항1호에 따라 개인정보 보호책임자를 지정함

구분	직책	성명
개인정보 보호책임자	실장	조 용 진

○ 개인정보 보호책임자의 임무

- 개인정보 보호 계획의 수립 및 시행
- 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- 개인정보 보호 교육 계획의 수립 및 시행
- 개인정보파일의 보호 및 관리 감독
- 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
- 개인정보 보호 관련 자료의 관리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

나. 개인정보취급자의 범위 및 의무와 책임

○ 개인정보취급자의 범위는 다음과 같다.

- 당사 내에서 정보주체의 개인정보를 처리하는 업무를 수행하는 자를 말하며, 정규직 이외에 임시직, 파견근로자, 시간제근로자 등 포함될 수 있다.

○ 개인정보취급자의 의무와 책임

- 내부관리계획의 준수 및 이행
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

4. 개인정보의 기술적 · 관리적 보호조치

가. 개인정보취급자 접근권한 관리 및 인증

○ 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

○ 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 서약서를 받아야 한다.

○ 개인정보처리자는 제1항, 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

○ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

○ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

나. 비밀번호 관리

○ 개인정보처리자는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.

○ 개인정보처리자는 비밀번호에 적정한 기간의 유효기간(반기별 1회 이상)을 설정하여야 한다

다. 접근통제

○ 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

- 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
- 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

○ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.

다. 개인정보의 암호화

○ 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

○ 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

○ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

○ 개인정보처리자 또는 개인정보취급자는 정보주체의 개인정보를 업무용 컴퓨터(PC)에 저장할 때에는 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

라. 접속기록의 위·변조 방지

○ 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하여야 한다.

○ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

마. 보안프로그램 설치 및 운영

○ 개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

○ 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 적용하여야 한다.

○ 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

바. 물리적 접근제한

○ 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

○ 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

○ 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

5. 개인정보보호 교육

가. 개인정보보호 교육 계획의 수립

○ 교육목적 : 개인정보보호의 오·남용 또는 유출 등을 예방하고,
임직원에게 개인정보보호 인식제고

○ 교육대상 : 당사 임직원

○ 교육내용

- 개인정보보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시사항, 위험관리 전략
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 개인정보보호 위반을 보고해야 할 필요성
- 개인정보보호업무의 절차, 책임, 작업 설명
- 개인정보보호 관련자들의 금지 항목들, 준수사항 이행 관련 절차 등

○ 교육일정 : 2019년 상반기 예정

○ 교육방법

- 직원들의 개인정보보호 인식 제고를 위해 자체 교육을 실시
- 각 부서회의를 통해 수시 교육
- 개인정보보호 전문강사 초빙하여 집체교육 실시

6. 개인정보 처리방침의 수립 및 공개

○ 개인정보 보호책임자는 개인정보처리방침을 수립하고 본사에서 운영하는 인터넷 홈페이지를 통해 인터넷 홈페이지 첫 화면 또는 첫 화면과의 연결화면에 지속적으로 게재하여야 한다.

○ 별도 업무용 홈페이지를 운영하는 분야별 보호책임자는 등록대상이 되는 개인정보파일에 대하여 개인정보처리방침을 정한다.

○ 개인정보처리방침을 게재하는 경우에는 “개인정보처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

○ 개인정보처리방침에 반드시 포함되어야 할 사항은 다음 각 호와 같다.

- 개인정보의 처리 목적
- 개인정보의 처리 및 보유 기간
- 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다.)
- 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다.)
- 정보주체의 권리·의무 및 그 행사방법에 관한 사항
- 처리하는 개인정보의 항목
- 개인정보의 파기에 관한 사항
- 개인정보 보호책임자에 관한 사항
- 개인정보처리방침의 변경에 관한 사항
- 개인정보의 안전성 확보조치에 관한 사항

○ 개인정보 보호책임자 또는 개인정보보호 분야별 책임자가 개인정보처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 인터넷 홈페이지 등에 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

7. 개인정보취급자에 대한 관리 및 감독

○ 개인정보 보호책임자는 개인정보취급자를 업무부서의 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 설정하여야 한다.

○ 개인정보 보호책임자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 개인정보취급자로 하여금 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 하여야 한다.
(개인정보보호 서약서는 붙임1을 참조한다.)

8. 개인정보 처리 업무의 위탁 제한

가. 개인정보처리자의 개인정보 처리 업무 위탁

○ 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음의 내용이 포함된 문서에 의하여야 합니다.

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁 제한에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 개인정보 처리 업무를 위탁받아 처리하는 자(이하 '수탁자'라 함)가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

나. 위탁업무 등에 대한 공개

○ 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 '위탁자'라 함)는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재해야 합니다.

다. 위탁자의 수탁자 교육 · 감독의무

○ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 수탁자를 교육해야 합니다.

○ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우 다음의 사항을 준수하는지를 감독해야 합니다.

○ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공해서는 안 됩니다.

○ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 「개인정보 보호법」을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 봅니다.

9. 관리용 단말기의 안전조치

가. 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안정조치를 하여야 한다.

○ 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

○ 본래 목적 외로 사용되지 않도록 조치

○ 악성프로그램 감염 방지 등을 위한 보안조치 적용

10. 재난 · 재해 대비 안전조치

가. 개인정보처리자는 화재, 홍수, 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

나. 개인정보처리자는 재해 · 재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

11. 개인정보 침해대응 및 피해구제

○ 당사 개인정보 침해 신고부서(정책연구팀) 지정・운영

○ 권익침해 구제방법

- 개인정보 주체는 개인정보 침해로 인한 구제를 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보 침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있음
- 기타 개인정보 침해의 신고 및 상담에 대하여는 아래의 기관에 문의
- 개인정보침해신고센터 : 국번 없이 118번(ARS 내선 2번)
- 정보보호마크인증위원회 : 02-580-0533~4
- 대검찰청 첨단범죄수사과 : 02-3480-2000
- 경찰청 사이버테러대응센터 : 02-392-0330

[붙임 1] 개인정보보호 서약서

[붙임 2] 개인정보 처리단계별 준수사항 및 위반 시 벌칙사항

[붙임 1]

개인정보보호 서약서

개인정보보호 서약서

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

또한 회사에서 수집한 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 "개인정보보호법"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 : 20　　년　　월　　일

소 속 :

성 명 :　　(인)

[붙임 2]

개인정보 처리단계별 준수사항 및 위반시 벌칙사항

구분	주요내용	벌칙 및 과태료
수집·이용	민감정보(사상·신념·정당가입·건강 등) 처리기준 위반(제23조)	5년 이하 징역 또는 5천만원 이하 벌금
	고유식별정보(주민등록·여권·운전면허 번호 등) 처리기준 위반(제24조)	
	주민등록번호 처리기준 위반(제24조의2)	3천만원 이하 과태료
	부당한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금
	개인정보의 수집기준 위반(제15조)	5천만원 이하 과태료
	만14세 미만 아동의 개인정보 수집시 법정대리인 동의획득여부 위반(제22조)	
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)	
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	3천만원 이하 과태료
	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제24조의 2)	
	동의획득방법 위반하여 동의받은 자(제22조)	1천만원 이하 과태료
제공·위탁	정보주체의 동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 목적 외 이용·제공(제18조, 제19조, 제26조, 제27조)	
	개인정보 주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18조, 제26조)	3천만원 이하 과태료
	정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지 위반(제20조)	
	업무위탁에 따른 개인정보의 처리제한 및 공개의무 위반(제26조)	1천만원 이하 과태료
개인정보 안전관리	개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조)	2년 이하 징역 또는 1천만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	3천만원 이하 과태료
	영상정보처리기기 설치·운영기준 위반(제25조)	
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	1천만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	
정보주체 권익보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조)	2년 이하 징역 또는 1천만원 이하 벌금
	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	
	개인정보 유출사실 미통지 및 조치결과 미신고(제34조)	3천만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한·거절(제35조)	
	정보주체의 정정·삭제요구에 따라 필요 조치를 취하지 아니한 자(제36조)	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	
	시정명령 불이행(제64조)	
	개인정보의 이전 사실을 알리지 아니한 자(제27조)	1천만원 이하 과태료
	정보주체의 열람, 정정·삭제, 처리정보 요구 거부 시 통지의무 불이행(제35조, 제36조, 제37조)	
	관계물품·서류 등의 미제출 또는 허위제출(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	
파기	개인정보 미파기(제21조)	3천만원 이하 과태료