대 외 비

개인정보보호 관리지침

Ver 1.2

제・개정이력

버전	내 용	제·개정일	주관부서	작성자	비고
1.0	최초 제정	2021.6. 21.	BADA 사업본부	안혜진	
1.1	개인정보 처리 및 관리에 대한 내용 추가	2023.07.31	BADA 사업본부	방현배	
1.2	주관부서/담당자 번경 및 연락처 추가	2024.09.02	경영지원팀	이상만	

목 차

제 1 장 총칙

제 1 조 (목적)

본 지침은 뱅크웨어글로벌(이하 '회사')의 고객사 개인정보(이하 '개인정보')를 안전하게 관리함으로써, 허가 받지 않은 공개, 개인정보의 오/남용, 변조 및 파괴 등으로부터 보호하기 위함을 목적으로 한다.

제 2 조 (적용범위)

본 지침은 BADA SaaS 서비스 제공을 목적으로 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보에 적용되며, 이러한 개인정보를 취급하는 모든 임직원 및 이해관계자에 적용된다. 다만 국내법상의 범위에 해당되지 않는 해외 서비스 및 해외 사용자의 개인정보에 대해서는 해당 국가의 법령을 따른다.

제 3 조 (용어의 정의)

1. "개인정보"란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보(당해 정보만으로 알아볼 수 없어도 다른 정보와 용이하게 결합하여 식별할 수 있는 것 포함)를 말한다.
2. "개인정보의 처리"란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 모든 행위를 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 사업자 및 개인 등을 말한다.
4. "개인정보처리 시스템"이란 개인정보를 처리할 수 있도록 체계적으로 구성 및 운영되는 시스템이며, 본 지침에서는 BADA 시스템을 의미한다.
5. "개인정보취급자"란 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말한다. 회사 임직원 및 외주 협력 직원 등 모두 포함한다.
6. "고객사"란 BADA SaaS 서비스를 이용하는 주체이자, 이용자를 말한다.
7. "고유식별정보"란 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 '여권번호', 운전면허의 '면허번호', '외국인등록번호' 등을 말한다.

제 2 장 개인정보보호 조직 및 지침 운영

제 4 조 (개인정보보호 관련조직 및 역할)

① 개인정보보호책임자는 경영지원팀장(이상만 전문위원)이며, BADA SaaS 서비스에 대한 개인정보보호 업무 및 조직을 총괄하여 감독하고, 다음 각 호의 역할을 수행한다.

1. 개인정보보호 조직의 구성 및 운영 총괄
2. 개인정보보호 지침의 제·개정 검토 및 공표
3. BADA 시스템 위험관리 총괄
4. 개인정보 침해사고에 대한 보안사고 대응팀 운영
5. 이 밖에 개인정보보호 활동을 위하여 업무 수행에 필요한 사항

② 개인정보보호관리자는 영업및사업관리팀장이며, 개인정보보호책임자의 위임을 받아 개인정보보호 업무를 관리하고, 다음 각 호의 역할을 수행한다.

1. 개인정보보호 조직 운영, 개인정보보호 지침의 제·개정 관리
2. 고객사의 개인정보 처리에 관한 의견 접수 및 처리
3. BADA 시스템의 관리적·기술적 보호대책 관리
4. 개인정보 유출 및 오·남용 방지를 위한 보안시스템 구축
5. 개인정보 침해사고에 대한 예방 활동 및 사고 접수 시 대응 등

③ 개인정보보호담당자는 인프라팀원이며, 개인정보보호관리자의 위임을 받아 개인정보보호 관련 실무를 수행하고, 다음 각 호의 역할을 수행한다.

1. 개인정보보호 관련 대내·외 창구역할 수행
2. BADA 시스템 관리적·기술적 보호대책 적용현황 관리
3. 보안시스템 설치 및 운영 등

④ 정보시스템관리자는 인프라팀장이며, 개인정보처리시스템의 기술적 운영업무를 관리하고, 다음 각 호의 역할을 수행한다.

1. BADA 시스템 취약점 점검 수행 및 기술적 보호대책 적용
2. BADA 시스템의 클라우드 SaaS 서비스 연속성을 보장 등

⑤ 개인정보취급자는 개인정보보호와 관련하여 다음 각 호의 역할을 수행한다.

1. 개인정보보호 활동 및 교육 참여
2. 개인정보보호지침의 관리적·기술적 보호조치 기준 준수
3. 직무상 알게 된 비밀의 누설 및 직무상 목적 외 용도로의 이용금지
4. 개인정보 관련 이슈 발생 시 개인정보보호관련 부서에 신고할 의무 등

제 5 조 (개인정보보호지침 관리)

① 본 지침은 고객사 개인정보의 안전한 보호를 위한 전반적인 사항과 관련 감독기관의 요구사항을 반영하여야 한다.

② 수립된 개인정보보호지침은 정기적으로 타당성과 개정 필요성을 검토하며, 필요한 경우 개인정보보호책임자의 승인을 득하여 개정한다.

③ 개인정보보호지침은 최신화하여 관리하며, 고객사의 제출 요구 시, 개인정보보호책임자의 승인을 거쳐 제출할 수 있다.

제 3 장 관리적 보호조치

제 6 조 (정보보호관련 인증 취득 및 유지)

① BADA 시스템의 안전성 및 신뢰성 확보를 위해 정보보호경영시스템에 대한 인증을 취득하고 유지하여야 하며, 인증 유형은 다음을 고려한다.

1. 국제공인 인증: ISO/IEC27001(정보보호경영시스템), ISO/IEC27017(클라우드 서비스 정보보안통제) 등
2. 국내인증: ISMS-P(정보보호관리체계), 클라우드 서비스 확인서 등

② 개인정보보호책임자는 제 1 항 각 호의 인증 중 대·내외 요구사항에 따라 적합한 인증을 선택하고, 해당 인증의 취득 및 유지를 위해 BADA 시스템에 대한 정보보호관리체계를 구축하고 운영한다.

③ 정보보호관리체계는 일회성이 아닌 PDCA 사이클에 의해 지속적인 계획, 이행, 개선 등 사후관리가 이뤄지도록 한다.

제 7 조 (클라우드 서비스 공급망 관리)

회사는 클라우드 컴퓨팅 서비스 공급망 제공자의 건전성 및 안전성을 확보하기 위해 다음 각 호를 고려한다

1. 클라우드 컴퓨팅 서비스 공급망이 준수해야하는 보안요구사항
2. 클라우드 컴퓨팅 서비스 공급망의 서비스 수준 요구사항(SLA)
3. 클라우드 컴퓨팅 서비스 인프라 지원 및 관리 책임 등

제 8 조 (개인정보취급자 교육)

① 회사는 개인정보취급자에 대해 개인정보 보호에 대한 인식을 제고시키고, 개인정보의 오용, 남용 또는 유출 등을 적극 예방하기 위해 개인정보보호교육을 실시한다.

② 교육방법은 오프라인교육 외 인터넷(온라인) 교육, 그룹웨어 교육 등 다양한 방법을 활용하고, 필요한 경우 외부 전문기관에 위탁할 수 있다.

③ 개인정보보호 교육실시 내역에 대한 기록은 인사총무부서에서 유지 및 관리한다.

제 9 조 (내부감사 시행)

① BADA 시스템에 대하여 기밀성, 무결성, 가용성을 확인하고, 정보보호관리체계 유지여부를 확인하기 위해 내부감사를 실시한다.

② 내부감사는 연 1 회 이상 정기적으로 실시하며, 감사 수행의 객관성 및 독립성을 확보하기 위해 외부 전문가 등을 포함하여 실시한다.

③ 내부감사는 회사 정보보호호 정책 및 지침, 정보보호관리체계 인증 기준 등의 준수여부를 확인하고, 감사수행 결과는 회사 정보보호최고책임자(CEO)에게 보고한다.

제 4 장 개인정보의 처리

제 10 조 (개인정보처리방침의 수립 및 공개)

① 회사는 고객으로부터 개인정보를 수집하여 이용하거나, 고객정보 취급업무를 위탁 또는 제 3 자에게 고객정보를 제공할 경우에는 다음 각 호의 사항이 포함된 개인정보의 처리방침(이하 "개인정보처리방침"이라 한다)을 정하여 인터넷 홈페이지 등을 통하여 게시하여야 한다.

가) 수집하는 고객정보의 항목(필수항목과 선택항목으로 구분) 및 수집방법

나) 고객정보의 수집・이용 목적

다) 고객정보의 보유 및 이용 기간과 파기절차 및 파기방법

라) 보유 및 이용 기간 만료에도 법령에 따라 고객정보를 보존해야 하는 경우 그 보존근거와 보존하는 고객정보의 항목

마) 동의 거부권 및 거부 시 불이익에 관한 사항

바) 고객정보를 취급위탁 하는 경우 고객정보 수탁업체 및 취급위탁 업무의 내용

사) 고객정보를 제 3 자에게 제공하는 경우 제공받는 자의 성명(법인인 경우 법인명)과 연락처, 제공하는 고객정보의 항목, 제공 받는 자의 이용 목적

아) 이용자 및 법정대리인의 권리와 그 행사방법

자) 정보주체의 권리・의무 및 그 행사방법에 관한 사항

차) 인터넷 접속정보파일 등 고객정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항

카) 고객정보 정책관리자 및 정책담당자의 성명, 소속부서, 직위 및 연락처 또는 고객정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

구분	개인정보보호책임자	개인정보보호 담당부서	개인정보 민원처리센터
담당	경영지원팀 이상만	경영지원팀	경영지원팀
전화번호/Fax	02-501-6415 / (FAX) 02-501-6416		

타) 다른 사업자로부터 고객정보를 제공 받는 경우 가)~다)의 내용에 제공 받는 고객정보의 항목, 목적, 보유/이용기간을 포함

파) 개인정보가 포함된 공개된 정보를 수집・이용하는 경우 공개된 정보의 수집출처, 수집・저장・조합・분석 등 처리하는 사실 및 그 목적

② 개인정보처리방침은 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결을 통하여 개인정보처리방침의 내용을 고객이 볼 수 있도록 하는 방법으로 공개해야 한다. 이 때, 고객이 개인정보처리방침을 쉽게 확인할 수 있도록 글자 크기, 색상 등을 통해 강조해야 한다.

③ 개인정보보호책임자는 이전 개인정보처리방침, 변경 내역을 전자적인 파일 형태로 보관해야 한다.

④ 개인정보보호책임자는 개인정보처리방침을 변경하는 경우에는 인터넷 홈페이지 등을 통하여 변경 이유 및 내용을 정보주체에게 공지하여야 한다.

제 11 조 (개인정보의 수집)

① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 회사는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

가) 정보주체로부터 사전에 동의를 받은 경우

나) 법률에서 개인정보를 수집・이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우

다) 법령에서 회사에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집・이용하지 않고는 법령에서 부과하는 구체적인 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

라) 개인정보를 수집・이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

마) 정보주체 또는 제 3 자(정보주체를 제외한 그 밖의 모든 자를 말한다.)의 생명, 신체, 재산에 대한 피해를 방지해야 할 급박한 상황이어서 개인정보를 수집・이용해야 할 필요성이 명백히 인정됨에도 불구하고 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 연락을 취할 수 없는 상황이어서 사전에 동의를 받을 수 없는 경우

바) 회사가 법령 또는 정보주체와의 계약에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 개인정보의 수집・이용에 관한 동의 여부 및 동의 범위 등을 선택하고 결정할 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집・이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위로 한정된다.

③ 회사 또는 임직원이 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함 등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의의사를

명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 회사가 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지 등"이라 함)에서 개인정보를 수집하는 경우, 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지 등에 게시하거나 게시하도록 허용한 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지 등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 회사는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인으로부터 또는 의사표시를 하는 경우 대리인의 개인정보를 수집・이용할 수 있다.

⑥ 회사는 근로자와 근로계약을 체결하는 경우「근로기준법」제 2 조제 5 호의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집・이용할 수 있다.

제 12 조 (개인정보의 제공)

① 개인정보의 "제공"이란 개인정보의 저장매체 또는 개인정보가 담긴 출력물이나 책자 등의 물리적 이전, 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제 3 자의 접근권한 부여, 개인정보처리자와 제 3 자의 개인정보 공유 등 개인정보의 이전과 공동으로 이용할 수 있는 상태를 초래하는 모든 행위를 말한다.

② 법 제 17 조의 "제 3 자"란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적・직접적으로 수집・보유한 개인정보처리자를 제외한 모든 자를 의미하며, 법 제 26 조제 2 항에 따른 수탁자는 제외한다.

③ 회사가 법 제 17 조제 2 항제 1 호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

④ 정보주체의 개인정보를 제 3 자에게 제공(공유를 포함한다. 이하 같다)할 경우에는 반드시 다음 각 호의 사항을 정보주체에게 알린 후 그 동의를 받아야 한다.

가) 개인정보를 제공받는 자

나) 개인정보를 제공받는 자의 개인정보 이용 목적

다) 제공하는 개인정보의 항목

라) 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

마) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

⑤ 개인정보를 국외의 제 3 자에게 제공할 때에는 제 4 항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 개인정보보호 관련 법규 등을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다

제 13 조 (개인정보의 이용・제공 제한)

① 개인정보 이용 및 제공에 관한 제한 사항은 다음 각 호와 같다.

가) 개인정보를 정보주체에게 미리 고지한 범위 또는 해당 서비스 이용약관에 명시한 범위를 넘어 이용하거나 제 3 자에게 제공하여서는 아니 된다.

나) 개인정보를 제공받은 목적 외의 용도로 이용하거나 제 3 자에게 제공하여서는 아니 된다.

다) 위탁업체와의 계약 시 관련법규 및 동 규정에 위반하는 내용이 포함되어서는 아니 된다.

② 개인정보는 정확하고 최신의 상태로 관리될 수 있도록 적절한 기술적 조치를 취하여야 한다.

③ 영업의 전부 또는 일부를 양도/양수하거나 합병, 상속 등으로 그 권리 및 의무를 이전/승계하는 경우 고객에게 다음의 각 호와 관련된 사항들을 통지하여야 한다.

가) 개인정보를 이전/승계 하려는 사실

나) 개인정보를 이전/승계 받는 자(영업양수자등)의 성명(법인의 경우 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처

다) 정보주체가 개인정보의 이전/승계를 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

제 14 조 (개인정보 수집 출처 등 공지)

① 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

가) 개인정보의 수집 출처

나) 개인정보의 처리 목적

다) 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 제 1 항은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.

가) 고지를 요구하는 대상이 되는 개인정보가 범죄의 수사 등을 위하여 개인정보보호법에서 비공개로 설정한 개인정보인 경우

나) 고지로 인하여 다른 사람의 생명・신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

제 15 조 (개인정보 이용 내역 통지)

① 개인정보 이용내역을 연 1 회 이상 전자우편・서면・모사전송・전화 또는 이와 유사한 방법을 통하여 통지하여야 한다.

② 이용내역 통지시 다음 각 호의 사항을 포함해야 한다.

가) 개인정보의 수집・이용 목적 및 수집한 개인정보의 항목
나) 개인정보를 제공받은 자, 그 제공 목적 및 제공한 개인정보의 항목
다) 개인정보를 취급위탁 받은 자 및 그 취급위탁을 하는 업무의 내용

제 16 조 (개인정보의 파기)

① 개인정보 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다.

② 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 제 1 항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장・관리하여야 한다.

④ 개인정보의 파기방법 및 절차는 다음의 각 호에 따른다

가) 회사는 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5 일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5 일 이내에 그 개인정보를 파기하여야 한다. 단, 이용목적 및 관련된 금융사고 조사, 분쟁해결, 민원처리, 법령상 의무이행을 위하여 최대 6 개월간 보유・이용 할 수 있다.

나) 개인정보 데이터를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.

A. 전자적 파일 형태인 경우 : 사회통념상 현재의 기술수준에서 적절한 비용이 소요되는 복원이 불가능한 방법으로 영구 삭제
B. 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각
C. 개인정보를 파기하고자 하는 경우, 해당 개인정보의 관리주체(서비스 담당부서 혹은 인사부서)의 사전 확인을 득한 후, 개인정보보호 부서관리자의 책임하에 수행하여야 하며, 해당 사항을 기록・관리하여야 한다.

제 17 조 (서비스 미사용 고객의 개인정보 파기)

① 이용자가 회사가 제공하는 서비스를 1 년 동안 이용하지 아니하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기 또는 분리보관 하여야 한다.

② 다른 법령에서 정하거나, 이용자의 요청에 따라 기간을 달리 정한 경우 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 별도 DB 를 분리하여 저장・관리하여야 한다.

③ 분리 보관된 개인정보는 최소한의 관련 업무 담당자만 열람할 수 있도록 하고, 목적 외로 이용할 수 없도록 해야 한다.

제 18 조 (개인정보 수집 동의를 받는 방법)

① 정보주체로부터 개인정보 수집·이용 동의 획득 시 법정 고지사항만을 간결하게 고지하고 "쉬운 용어", "중요내용은 부호, 색채, 굵고 큰 문자 등"을 활용하여 명확하게 표시하여 정보주체가 동의 내용을 쉽게 인식할 수 있는 상태에서 동의를 얻어야 한다.

② 동의문에는 아래 각호의 사항이 포함되어야 한다.

가) 수집하는 개인정보의 항목(자동수집정보, 생성정보 포함)

나) 개인정보의 수집・이용 목적

다) 개인정보의 보유・이용기간

라) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 전화를 통해 개인정보를 수집하는 경우 "법정 고지사항"을 "일상 대화 속도"로 설명하고 이해 했는지 여부를 확인해야 한다.

④ 개인정보 수집시 필수 항목과 선택항목으로 구분하여 동의를 얻어야 하며, 선택항목에 개인정보를 기입하지 않아도 서비스 이용에 지장이 없어야 한다.

⑤ 선택동의 항목은 서비스 목적별로 나누어 "개별적으로 동의"받도록 구성하여 이용자가 개인정보 제공여부를 선별적으로 결정할 수 있도록 해야 한다.

제 19 조 (정보주체의 사전동의를 받을 수 없는 경우)

① 회사는 법 제 15 조제 1 항제 5 호 및 제 18 조제 2 항제 3 호에 따라 정보주체의 사전 동의 없이 개인정보를 수집, 이용 또는 제공한 경우, 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집 또는 이용한 사실, 그 사유와 이용내역을 홈페이지 등을 통해 즉시 알려야 한다.

제 20 조 (개인정보의 수집제한)

① 개인정보 수집 시 수집목적과 서비스유형을 고려하여 개인정보 항목, 수집・이용목적, 보유・이용기간 등을 최대한 상세하고 정확하게 기재하여야 하며, 수집목적에 비추어 합리적으로 인정될 수 있는 최소한의 범위 내에서 수집하여야 한다.

② 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 상품 또는 서비스의 제공을 거부하여서는 아니 된다.

③ 사상・신념, 노동조합・정당의 가입・탈퇴, 정치적 견해, 건강 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 정보주체로부터 별도의 동의를 받거나 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에는 예외로 한다.

④ 개인을 고유하게 구별하기 위하여 부여된 식별정보(이하 "고유식별정보"라 한다)로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호에 해당하는 정보를 처리할 수 없다. 다만, 정보주체로부터 별도의 동의를 받거나 법령에서 구체적으로

고유식별정보의 처리를 요구하거나 허용하는 경우에는 예외로 한다.

⑤ 만 19 세 미만 미성년자의 개인정보는 수집하지 않는다.

제 21 조 (고유식별정보의 처리 제한)

① 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 고유식별정보를 처리할 수 없다.

가) 정보주체에게 법 제 15 조제 2 항 각 호 또는 제 17 조제 2 항 각호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우

나) 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용한 경우

제 22 조 (주민등록번호 처리의 제한)

① 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

가) 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

나) 2. 정보주체 또는 제 3 자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요한 경우

② 정보주체가 홈페이지를 통하여 회원으로 가입하는 단계에서는, 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 대체 가입수단을 제공하여야 한다.

제 23 조 (개인정보 처리의 위탁)

① 개인정보 처리방침에서 명시된 업체와 별도로 개인정보 처리를 외부에 위탁하는 경우 서면, 전자우편, 전화 또는 홈페이지를 등을 통하여 사전에 해당 사실을 고객에게 고지하고 동의를 받아야 한다. 다만, 서비스 제공에 관한 계약의 이행을 위해 필요한 경우에는 개인정보 처리방침에 공개 또는 전자우편 등으로 통지하고 고객 동의 과정을 생략할 수 있다.

② 개인정보를 취급하는 위탁업체와 계약을 체결할 경우, 계약서에는 반드시 개인정보보호와 관련된 다음의 항목을 반영하여야 한다.

가) 개인정보 제공 또는 위탁을 하는 업무의 목적 및 범위

나) 업무상 목적 외 사용금지에 관한 사항

다) 개인정보의 제 3 자 제공 금지 및 재위탁 제한에 관한 사항

라) 개인정보에 대한 기술적, 관리적 보호조치 확보에 관한 사항

마) 개인정보 송수신 방법 및 안정성 보호조치 확보에 관한 사항

바) 개인정보의 반납 및 폐기에 관한 사항

사) 개인정보보호 관리 조치의 부실로 인한 문제발생시 손해배상 등 책임에 관한 사항

아) 개인정보의 관리현황 점검 및 수탁회사 소속직원의 교육 및 감독에 관한 사항

자) 기타 정보를 안전하게 처리하기 위하여 필요한 사항 및 법적 준수 사항

③ 위탁업체와의 업무를 수행하는 해당 부서는 위탁·수집되는 개인정보가 안전하게 관리될 수 있도록 적정한 관리・감독을 하여야 한다.

제 5 장 정보주체의 권리 보장

제 24 조 (개인정보의 열람절차 등)

① 정보주체는 자신의 개인정보에 대한 열람을 요구하려는 경우에는 다음 각 호의 사항 중 열람하려는 사항을 특정하여 요청하여야 한다.

가) 개인정보의 항목 및 내용
나) 개인정보의 수집・이용의 목적
다) 개인정보 보유 및 이용 기간
라) 개인정보의 제 3 자 제공 현황
마) 개인정보 처리에 동의한 사실 및 내용

② 제 1 항에 따른 개인정보 열람요구서를 받은 날부터 10 일 이내에 정보주체에게 해당 개인정보를 열람할 수 있도록 하는 경우와 열람 요구 사항 중 일부를 열람하게 하는 경우에는 열람할 개인정보와 열람이 가능한 날짜・시간 및 장소 등(요구 사항 중 일부만을 열람하게 하는 경우에는 그 사유와 이의제기방법을 포함한다)을 해당 정보주체에게 알려야 한다.

③ 정보주체로부터 영 제 41 조 제 1 항 제 4 호의 규정에 따른 개인정보의 제 3 자 제공현황의 열람청구를 받은 회사는, 국가안보에 긴요한 사안으로 법 제 35 조 제 4 항 제 3 호 마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제 3 자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제 25 조 (개인정보의 정정・삭제)

① 회사가 법 제 36 조제 1 항에 따른 개인정보의 정정・삭제 요구를 받았을 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정・삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정・삭제 요구가 법 제 36 조제 1 항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제 26 조 (개인정보의 처리정지)

① 회사가 정보주체로부터 법 제 37 조제 1 항에 따라 개인정보처리를 정지하도록 요구받은 때에는 법 제 37 조제 2 항단서에 해당하지 않고 다른 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 개인정보의 처리의 일부 또는 전부를 정지하여야 한다.

② 회사는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여는 정당한 사유가 없는

한 처리정지의 요구를 받은 날로부터 10 일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제 27 조 (권리행사의 방법 및 절차)

회사는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집 시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다. 이는 영 제 46 조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 수수료와 우송료의 정산에도 마찬가지로 적용된다.

제 6 장 물리적 보호조치

제 28 조 (출입통제)

① 개인정보보호책임자는 BADA 시스템 운영을 위한 SaaS Operation Room 을 별도로 마련하고, 통제구역으로 지정 및 강화된 출입통제를 적용한다.

② SaaS Operation Room 의 출입권한은 회사 인사총무 부서에서 관리하고, 권한을 부여받은 인가자에 한해 출입할 수 있으며, 시스템 유지보수 등 외부 협력업체 직원의 출입이 필요한 경우, 출입관리대장에 기록 후, 업무 담당자의 동행 하에 출입할 수 있다.

③ 개인정보보호담당자는 SaaS Operation Room 의 인가자 외 출입내역에 대해 검토하여 분기 1 회 개인정보보호책임자에게 보고하고, 인사총무 부서에 통보한다.

④ 인사총무 부서는 SaaS Operation Room 출입권한 및 출입내역에 대한 전반적인 검토를 분기 1 회 수행한다.

⑤ 이 외 출입관리 및 물리적 접근 통제에 대한 세부 사항은 '물리 보안 지침'을 따른다.

제 29 조 (업무용 단말기 보안)

① BADA 시스템 운영자 및 개인정보취급자의 업무용 단말기에는 회사 표준 보안시스템을 설치 및 유지하여야 한다.

② 표준 보안시스템의 보안정책은 다음 각 호와 같으며, 해당 보안정책을 준수한다.

1. 보조 저장매체 사용 통제
2. 업무용 단말기 외부 반출입 통제
3. 인터넷 및 네트워크 보안 통제
4. 불법 소프트웨어 통제 등

5. 이 외 업무용 단말기의 보호대책에 대한 세부 사항은 '사용자 보안관리지침'을 따른다.

제 7 장 기술적 보호조치

제 30 조 (접근통제)

① BADA 시스템 접근 시 암호화 통신하고 강화된 사용자인증(MFA 등)을 적용한다.

② 원격 접속을 위한 로그인은 5 회 이상 실패 시 자동으로 접속을 종료하도록 설정하고, 일정시간 미 작동 시에는 세션타임아웃 설정을 한다. 단, 모니터링 등 운용 상 필요성이 인정되는 경우에는 예외 처리할 수 있다.

③ BADA 시스템 접점 구간에는 보안시스템을 설치하여 비인가자 접근 및 DDoS 등을 예방하도록 한다.

제 31 조 (사용자 계정 및 접근권한 관리)

① BADA 시스템 사용자 계정은 개인정보보호책임자의 승인을 득한 후 발급 가능하고, 사용자 계정은 퇴직, 직무 변경, 장기 미사용 등 변경 발생 시에는 즉시 사용중지 등 조치를 취한다.

② 사용자 계정에 대한 접근권한은 해당 업무에 따라 차등 부여하며, 등록, 변경, 삭제 등의 내역은 다음 각 호에 따라 기록하고, 최소 5 년 보관한다.

1. 작업 수행자 정보(IP, ID, 소속 및 성명)
2. 작업 수행일자
3. 사용자 계정 정보(ID, 소속 및 성명)
4. 부여된 접근권한 내용 등

③ 사용자 계정은 1 인 1 개 부여하며, 다른 사용자와 공유되지 않도록 한다.

④ 정보시스템관리자는 시스템 운영자의 접근권한 오·남용을 예방하기 위하여 접근권한 및 접속기록에 대해 분기 1 회 검토하고, 개인정보보호관리자에게 통보한다.

⑤ 개인정보보호관리자는 BADA 시스템 응용프로그램 사용자의 접근권한 및 접속기록에 대해 분기 1 회 검토하고, 정보시스템관리자 검토내역과 함께 개인정보보호책임자에게 보고한다.

제 32 조 (비밀번호 관리)

① BADA 시스템의 접근통제를 강화하기 위하여 반드시 비밀번호를 설정해야 하며, 비밀번호 설정 시 다음 각 호를 포함한 생성 규칙을 따른다.

1. 영문, 숫자, 특수문자의 2 종류 조합일 경우 8 자리 이상 사용(3 종류 시 10 자리 이상)
2. 계정과 동일한 비밀번호나 계정이 포함된 비밀번호 사용 금지
3. 동일 숫자, 문자의 연속적인 반복 사용 금지
4. 전화번호, 생일 등 추측하기 쉬운 정보 설정 금지

② 비밀번호는 최대 3 개월 이내에 정기적으로 변경하도록 설정한다. 단, 시스템 관리자 계정의 비밀번호는 시스템간의 연계성 및 업무 영향도를 고려하여 별도의 기간을 설정할 수 있다.

③ 비밀번호를 데이터베이스에 저장 시에는 복호화 할 수 없도록 일방향 암호화를 적용하여야 하며, 알고리즘 강도는 SHA2 이상으로 한다.

제 33 조 (접속기록 관리)

① 개인정보취급자가 BADA 시스템에 접속하여 고객사 개인정보를 처리한 경우에는 접속기록을 저장하며, 최소 2 년 보관한다.

② 정보시스템관리자는 접속기록이 위·변조 및 분실되지 않도록 안전하게 보관하고, 주기적으로 백업한다.

③ 개인정보보호관리자는 개인정보취급자의 접속내역을 월 1 회 이상 정기적으로 검토하며, 개인정보보호책임자에게 보고한다.

④ 과도한 개인정보 처리 내역이나 인가되지 않은 접근 등의 이상징후가 발생한 경우, 해당 업무담당자 확인 및 원인 분석 등 조치를 취한다.

제 34 조 (서비스 연속성 관리)

① 정보시스템관리자는 BADA 시스템 SaaS 서비스의 연속성 보장을 위해 정보시스템 백업을 수행하며, 백업수행 결과는 분기 1 회 개인정보보호책임자에게 보고한다.

② 백업데이터의 정합성 및 복구 테스트를 연 1 회 실시하며, IT 재해복구 모의훈련 시 포함하여 수행한다

③ BADA 시스템의 장애 예방 및 성능의 최적화를 위해 사용현황 및 추이 분석등을 정기적으로 실시하여, 효과적인 가상자원 활용 및 최적의 용량을 확보한다.

④ BADA 시스템에 접속 불능 및 지연 등 장애 발생 시 장애등급을 판단하고, 등급별 보고대상 및 대응절차에 따라 조치한다.

장애등급	판단 기준		보고대상	이용자 통지
1급	서비스 불능	- 서비스 전체영역이 접속되지 않는 경우 - 연속해서 10 분이상 지속	대표이사 (CISO)	O
	서비스 불안정	- 서비스 전체영역이 24 시간 이내에 다회 접속되지 않는 경우 - 2 회 이상, 중단된 시간 합산 15 분 이상 지속		
2급	서비스 일부 불능	- 서비스 중 일부 메뉴가 접속되지 않거나 실행이 지연(5 분 초과)되는 경우	BADA 사업본부장	X

	서비스 일부 불안정	- 서비스 중 일부 메뉴가 24 시간 이내에 다회 접속되지 않거나 실행이 안되는 경우 - 2 회 이상, 중단된 시간 합산이 7 분 이상 지속	(CPO)	
3급	단순 오류	- 단순 기능 오류 - Link 오류 또는 출력 오류 등	개인정보 보호관리자	X

⑤ 장애등급 1 급에 해당될 시 이용자에 통지하여야 하며, 다음 각 호의 내용을 포함한다.

1. 발생 내용 및 발생원인
2. 회사의 피해 확산 방지 조치 현황
3. 회사의 담당부서 및 연락처
4. 이용자의 피해 예방 또는 확산방지 방법

제 35 조 (취약성 점검)

① 정보시스템관리자는 BADA 시스템의 기술적인 취약성 점검을 연 1 회 수행하고, 발견된 취약점에 대한 보호대책을 마련하여 적용한다.

② 취약성 점검결과 및 보호대책 계획은 개인정보보호책임자에게 보고하고, 개인정보보호책임자는 이에 대해 확인 및 감독한다.

제 36 조 (개발 보안관리)

① BADA 시스템의 개발 및 운영환경은 분리하고, 개발 및 테스트는 실 운영 시스템과 분리된 별도 개발 시스템에서 수행한다.

② 개발 및 테스트 시에는 임의의 테스트 데이터를 생성하여 활용한다.

③ BADA 시스템 개발 및 변경 시에는 소스코드 등에 존재할 수 있는 잠재적인 보안취약점을 제거하고, 안전한 시스템 개발을 위한 시큐어 코딩 기법을 적용한다.

④ 운영 시스템으로의 이관은 개인정보보호관리자의 승인을 득한 후, 이관한다.

제 37 조 (개인정보의 암호화)

① BADA 시스템 내 저장되는 개인정보의 암호 대상 및 알고리즘 강도, 적용방법 등은 고객사 규제기관의 요구사항을 따른다.

② 비밀번호 암호화는 제 14 조(비밀번호 관리)에 따른다.

③ 정보통신망을 통해 개인정보 및 인증정보를 송수신 할 경우에는 SSL 인증서 등으로 암호화 적용한다.

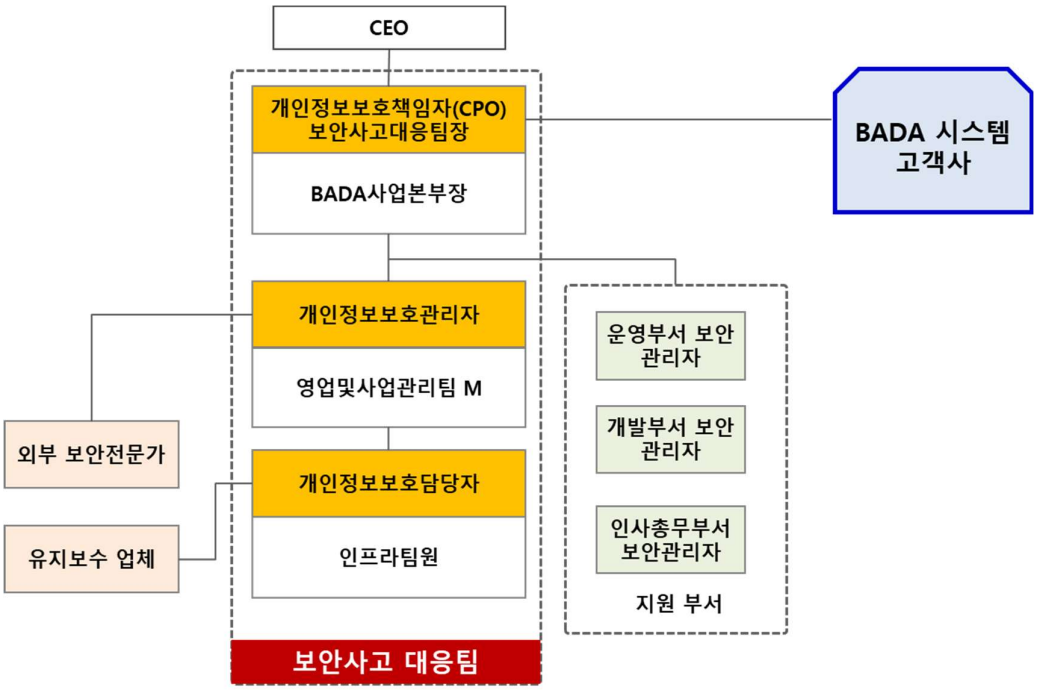
제 8 장 개인정보 침해사고 대응

제 38 조 (침해사고 대응조직 구성)

① 개인정보보호책임자는 고객사 개인정보 침해사고 발생 시 신속한 대처를 위하여 대응조직의 구성 및 책임을 부여하고, 비상연락체계가 유지될 수 있도록 관리한다.

② 개인정보보호관리자는 개인정보 침해사고 발생 시 개인정보보호책임자의 지시에 따라 '보안사고대응팀'을 소집한다.

③ 개인정보보호담당자는 비상연락망(지원부서, 외부협력 인원, 고객사 포함)을 최신화 유지한다.

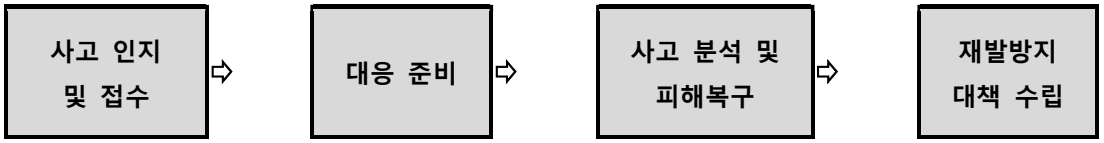


④ 보안사고대응팀장은 BADA 사업본부장이 수행하며, 운영, 개발 및 인사총무부서 등 내부 지원부서와 외부전문가와 긴밀한 협조체제를 마련한다.

제 39 조 (침해사고 대응 절차)

① 개인정보보호책임자는 개인정보 침해사고 발생 시 고객사의 업무협조 요청에 기민하게 대응하며, 사고원인분석 및 피해복구에 적극 협조한다.

② 개인정보 침해사고 발생 시 신속한 대응을 위해 다음과 같은 절차를 마련한다.



제 40 조 (사고 인지 및 접수)

① BADA 시스템 업무담당자는 다음 각 호와 같은 개인정보 침해사고 정황이 인지되는 즉시, 개인정보보호담당자에게 구두(유선) 등으로 신고한다. 고객사 업무담당자는 BADA 시스템 내 헬프센터 또는 유선 등을 통해 접수한다.

1. 다량의 개인정보가 허가 없이 전송되거나 출력되고 있는 것을 발견한 경우
2. 고객사의 동의 없이 개인정보 관련 업무가 수행된 경우
3. 기타 권한이 없는 자에게 개인정보가 노출된 경우
4. BADA 시스템에 대한 최종 로그인, 로그아웃 시간이 사실과 다르게 표시된 경우
5. 이 외 개인정보 오남용, 변조, 유출 등으로 의심이 되는 경우

② 개인정보보호담당자는 침해사고 접수 시 해당 내용을 개인정보보호관리자에게 즉시 보고하고, 고객사 업무담당자와 공유한다.

제 41 조 (대응 준비)

① 개인정보보호관리자는 사고접수 내용 등을 확인하여 개인정보 침해사고 유형, 유출 여부, 유출 규모 등 사고현황 및 추가피해 발생 가능성을 파악하고, 보안사고대응팀 소집 여부를 개인정보보호책임자에게 건의한다.

② 침해사고가 아닌 것으로 판단되거나, 오탐인 경우는 침해사고를 종료하고, 관련 사항은 기록하여 관리한다

③ 개인정보보호책임자 판단에 따라 보안사고대응팀이 소집되는 경우는 사고분석 및 피해복구, 재발방지 대책 수립 절차에 따른다.

제 42 조 (사고 분석 및 복구)

① 보안사고대응팀은 고객사 업무담당자와 협업하여 개인정보 침해사고 발생 경로 및 원인 파악을 위해 증거자료 분석 및 필요한 자료를 수집하여 분석한다.

② 개인정보 유출이 확인된 경우, 다음 각 호의 사항을 고객사에게 전달하여, 고객사가 해당 개별 이용자에게 통지할 수 있도록 안내한다.

1. 유출된 개인정보의 항목
2. 유출 시점과 그 경위
3. 피해 최소화를 위한 고객사의 조치방법
4. 회사의 대응조치 등

③ 고객사 업무담당자는 개인정보 유출에 대한 사항을 해당 이용자에게 통지할 경우, 회사는 이를 지원한다.

④ 고객사 금융당국 또는 규제기관에 대한 신고 여부는 고객사가 판단하여 이행한다.

⑤ 보안사고대응팀은 고객사와 협업하여 개인정보 침해사고 원인분석, BADA 시스템 복구 등 대응조치를 취하며, 사고대응 종료 후 개인정보보호관리자는 사고 처리에 대한 사항을 기록하여 개인정보보호책임자에게 보고하며, 관련사항은 '보안사고 대응 지침'을 따른다.

⑥ 개인정보보호책임자는 필요 시 정보보호최고책임자에게 보고할 수 있다.

제 43 조 (재발방지 대책 수립)

① 보안사고대응팀은 재발방지를 위해 사고 발생 후 대응과정 및 조치결과 등을 고객사와 공유한다.

② 개인정보보호책임자는 BADA 본부원을 대상으로 유사 사고 재발방지를 위한 교육 및 개인정보보호 점검을 수행하고, 개선이 필요한 경우 관련 보호조치를 마련하여 이행한다.

부 칙

제 1 조 (시행일)

본 지침은 2021 년 6 월 21 일부터 시행한다.

제 2 조 (준용)

BADA 시스템에 대한 개인정보보호 업무는 본 지침에 따라 수행하되, 해당 서비스 이용국가 규제기관의 요구사항이 있을 경우, 그 요구사항을 우선하여 적용한다.

관련양식

[물리 보안 지침] 內 양식 공용
[정보시스템 보안 지침] 內 양식 공용
[보안사고 대응 지침] 內 양식 공용