개인정보보호 관리 규정

[헤리티지자산운용 주식회사]

제1장 총칙

제1조(목적) 개인정보보호 관리규정(이하 “규정”이라 한다)은 개인정보보호법(이하 “법”이라 한다) 제29조(안전조치의무) 규정의 수립 및 시행 의무에 따라 제정된 것으로 주식회사 [회사명](이하 “회사”)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위) 본 규정은 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.

제3조(용어 정의)본 규정에서 사용하는 용어는 다음 각 호와 같다.

1. “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.
2. “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.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등으

로 본 규정에서는 회사를 뜻한다.

5. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.
6. “개인정보 보호담당자”란 개인정보책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보 보호 책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
7. “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.
8. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
9. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
10. “모바일 기기”란 무선망을 이용할 수 있는 노트북, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
11. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
12. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk)등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 커퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
13. “영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을

통하여 전송하는 일체의 장치를 말한다.

14. “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.

제2장 규정의 수립 및 시행

제4조(규정의 수립 및 승인) ① 개인정보 보호책임자는 회사의 개인정보 보호를 위한 전반적인 사항을 포함하여 규정을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보 보호를 위한 규정의 수립 시 개인정보 보호와 관련한 법령 및 관련 규정을 준수하도록 규정을 수립하여야 한다.

제5조(규정의 공표) ① 개인정보 보호책임자는 전조에 따라 승인한 규정을 회사의 전 임직원에게 공표한다.

② 규정은 임직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 지정) ① 회사는 개인정보보호법 시행령 제32조제2항1호에 따라 각 호의 하나에 해당하는 자를 개인정보 보호책임자로 임명한다.

1. 대표이사(대표이사가 2인 이상일 경우, 경영관리부문 대표이사)
2. 개인정보 관련 임원(CPO : Chief Privacy Officer, CISO : Chief Information Security Officer, CIO : Chief Information Officer 등)

3. 개인정보의 처리를 담당하는 부서의 장(단, 제2호에 해당하는 임원이 없는 경우에 한한다.)

② 회사는 개인정보 보호책임자의 지정 시에는 인사발령 등을 통해 공식적으로 책임과 역할을 부여해야 하나, 전항 제1호에 해당하는 자를 개인정보 보호책임자로 지정시에는 지정절차를 생략할 수 있다.

제7조(개인정보 보호책임자의 의무와 책임) ① 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 규정의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 규정의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독
7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보 보호책임자는 개인정보 보호와 관련하여 이법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

④ 개인정보 보호책임자는 제1항의 개인정보 보호 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보 보호담당자로 임명할 수 있다.

⑤ 개인정보 보호담당자는 개인정보 보호책임자를 보좌하여 개인정보 보호업무에 대한 실무를 총괄하고 관리한다.

제8조(개인정보취급자의 범위 및 의무와 책임) ① 개인정보취급자는 회사 내에서 정보주체의 개인정보를 처리하는 업무를 수행하는 모든 임직원을 뜻하며, 정규직 이외에 임시직, 파견근로자, 시간제근로자 등도 포함될 수 있다.

② 개인정보취급자의 의무와 책임은 다음 각 호와 같다.

1. 규정의 준수 및 이행
2. 개인정보의 기술적·관리적 보호조치 기준 이행
3. 업무상 알게 된 개인정보를 제3자에게 제공하지 않음
4. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
5. 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행

제4장 개인정보 보호조직 구성

제9조(개인정보 보호조직) 회사의 개인정보 보호 정책을 수행하고 유사 시 신속하고 효율적인 대응을 도모할 개인정보 보호조직을 구성해야 한다.

제5장 개인정보의 기술적·관리적 보호조치

제10조(개인정보취급자 접근권한 관리 및 인증) ① 회사는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 회사는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우

지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지 의무 등에 대한 서약서를 받아야 한다.

③ 회사는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제11조(비밀번호 관리) ① 회사는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 하여야 한다.

② 회사는 비밀번호에 적정한 기간의 유효기간을 설정하여야 한다.

제12조(접근통제) ① 회사는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

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

② 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.

③ 회사는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

제13조(개인정보의 암호화) ① 회사는 주민등록번호, 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

② 회사는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 회사는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 회사가 내부망에 고유식별정보를 저장하는 경우에는 암호화 미적용시 위험도 분석 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

제14조(접속기록의 위·변조 방지) ① 회사는 개인정보 취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하여야 한다.

② 회사는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 회사는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제15조(악성프로그램 등 방지) 회사는 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태를 유지.
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제16조(관리용 단말기의 안전조치) 회사는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제17조(물리적 안전조치) ① 회사는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 회사는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 회사는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리스시템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제18조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄)
2. 전용 소각장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리

및 감독

2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

제19조(영상정보처리기기 운영·관리 방침) ① 회사가 영상정보처리기기를 설치 및 운영 관리할 경우, 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

② 회사는 전항에 따라 마련한 영상정보처리기기 운영·관리 방침을 회사의 홈페이지에 지속적으로 게재해야 한다.

제6장 개인정보 보호 교육

제20조(개인정보 보호 교육 규정의 수립) ① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보 보호 교육규정을 매년 수립한다.

1. 교육목적 및 대상
2. 교육내용

3. 교육 일정 및 방법

② 개인정보 보호책임자는 수립한 개인정보 보호 교육 규정을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육규정 수립에 반영하여야 한다.

제21조(개인정보 보호 교육의 실시) ① 개인정보 보호책임자(또는 개인정보 보호담당자)는 정보주체 정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 연1회 이상의 개인정보 보호 교육을 실시한다.

② 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

제7장 개인정보 침해대응 및 피해구제

제22조(자체감사 주기 및 절차) ① 개인정보 보호책임자는 개인정보 보호와 개인정보 유출을 방지하기 위하여 규정 및 관련 법령에서 정하는 개인정보 보호 규정을 성실히 이행하는지를 주기적으로 감사 또는 점검하여야 한다.

② 개인정보 보호책임자는 전항의 감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 별도의 규정을 수립할 수 있다.

③ 개인정보보호 자체감사는 최소 연 1회 이상 실시한다.

제23조(자체감사 결과 반영) ① 개인정보 보호책임자는 제22조의 감사 결과 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 규정의 내용을 위반한 사실을 적발한 경우에는 시정·개선 등 필요한 조치를 취하여야 한다.

② 개인정보 보호책임자는 전항의 시정·개선 등 필요한 조치가 이행되지 않거나 개인정

보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우, 인사발령 등의 필요한 추가 조치를 취할 수 있다.

제24조(개인정보 유출 등의 통지) ① 회사는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 회사의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 회사는 개인정보가 유출된 경우 그 피해를 최소화하기 위하여 침해사고 대응팀을 구성하고 필요한 조치를 할 수 있다.

제25조 (개인정보 유출 등의 신고) ① 회사는 1만명 이상의 개인정보가 유출된 경우. 제24조에 따른 통지 및 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관(한국정보화진흥원, 한국인터넷진흥원 등)에 신고하여야 한다. 이 경우 행정자치부장관 또는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

② 개인정보 유출에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 아래와 같다.

1. 회사는 개인정보가 유출되었음을 알게 되었을 때에는 서면 등의 방법으로 지체 없이 제24조 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없

이 정보주체에게 알릴 수 있다.

2. 회사는 구체적인 유출 내용(시점 및 경위)을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

3. 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 다음 각 목의 정보를 7일 이상 게재하여야 한다.

가. 유출된 개인정보의 항목

나. 유출된 시점과 그 경위

다. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

라. 회사의 대응조치 및 피해 구제절차

마. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

부 칙

제1조(시행일) 이 규정은 2019년 2월 일부터 제정 시행한다.