1. **신용정보보호규정 신구 조문 대비표**

|  |  |  |
| --- | --- | --- |
| **현행** | **개정안** | **비고** |
| **제1장 총칙****제1조 ~ 제3조**(생략) | **제1장 총칙****제1조 ~제3조**(현행과 같음) |   |
| **제2장 신용정보 일반규정****제4조 ~ 제9조**(생략) | **제2장 신용정보 일반규정****제4조 ~ 제9조**(현행과 같음) |  |
| **제3장 신용정보 주체의 권리보호****제10조 ~ 제18조**(생략) | **제3장 신용정보 주체의 권리보호****제10조 ~ 제18조**(현행과 같음)  |  |
| **제4장 내부통제 강화****제19조 ~ 제21조**(생략) | **제4장 내부통제 강화****제19조 ~ 제21조**(현행과 같음) |  |
| **제5장 가명정보** <신설> | **제5장 가명정보** |  |
| **제22조 (가명정보의 정의)**<신설> | **제22조(가명정보의 정의)**1. “가명정보”란 가명처리한 개인신용정보를 말한다.
2. “추가정보”란 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 가명 처리하는데 사용된 정보로서 가명정보를 원래의 상태로 복원하기 위한 값을 말한다.
 | 신용정보법 제40조의2 가명처리 익명처리에 관한 행동규칙 신설에 따라 개정함 |
| **제23조 (가명정보의 범위 및 활용)**<신설> | **제23조 (가명정보의 범위 및 활용)**1. 특정 신용정보주체를 식별할 수 없는 경우에는 가명정보로 볼 수 있다. 또한, 별도의 매핑테이블 등 추가정보가 존재하는 경우에도 가명 처리한 정보는 가명정보로 볼 수 있다.
2. “가명정보”는 다음의 목적으로 사용될 경우 신용정보주체의 동의 없이 활용할 수 있다.
3. 통계작업(상업적 목적을 포함)
4. 연구(산업적 연구를 포함)
5. 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우
 | 신용정보법 제40조의2 가명처리 익명처리에 관한 행동규칙 신설에 따라 개정함 |
| **제24조 (가명처리 절차)**<신설> | **제24조 (가명처리 절차)**1. 가명처리 시에는 다음의 절차에 따라 처리되어야 한다.
2. 사전준비 단계

가. 각 사업본부는 가명정보가 필요한 경우 제23조 제②항에서 정한 목적에 부합하는 구체적 목적을 명시하여야 한다.나. 구체적 목적이 확정되면 해당 목적을 위한 필요, 최소한의 항목으로 가명처리 대상 정보집합물을 추출 하도록 하여야 한다.다. 가명정보를 활용하는 각 사업본부는 가명정보 및 추가정보에 대한 접근관리 등 본 규정에서 정하고 있는 관리, 보호 절차를 준수하여야 한다.2. 가명처리 단계가. CISO, CIO 및 신용정보관리 보호인은 가명처리 목적, 처리 및 이용 환경, 가명처리 대상 데이터의 특성 등에 따른 위험도를 분석하여야 한다. 나. 위험도를 고려하여 적절한 가명처리 방법, 수준을 결정하고 가명정보 및 추가정보의 보유기간을 설정하여 관리 한다.다. 정보시스템본부는 가명처리 방법 및 수준에 따라 식별자 삭제 또는 대체, 재식별 위험도가 높은 개인 식별가능 정보에 대한 가명처리 등을 수행한다.3. 활용 및 사후관리가. 추가정보의 분리 보관 또는 삭제 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제하여야 한다. 나. 가명처리 한 개인신용정보는 “첨부 4)”에서 정한 기술적, 물리적, 관리적 보안대책을 준수하여야 한다.다. 가명정보는 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 처리하여서는 아니 된다.라. 각 사업본부 담당자는 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제하여야 한다.마. 정보시스템본부는 가명처리 한 경우 1) 가명처리한 날짜 2) 가명처리한 정보의 항목 3) 가명처리한 사유와 근거에 대하여 3년간 보존하여야 한다.바. 각 사업본부 담당자는 가명정보 활용과 관련하여1) 처리하는 가명정보의 종류 및 이용목적 2) 가명정보의 보유 또는 이용기간 3) 가명정보 파기의 절차 및 방법 4) 처리하는 가명정보의 항목 등에 대하여 홈페이지에 공시하여야 한다.  | 신용정보법 제40조의2 가명처리 익명처리에 관한 행동규칙 신설에 따라 개정함 |
| **[별표 8] 가명정보에 관한 보호조치 기준**<신설> | **[별표 8] 가명정보에 관한 보호조치 기준**1. 기술적, 물리적 보호조치

① 추가정보에 대한 보호조치가. 정보시스템본부는 가명조치 후 추가정보를 삭제하지 아니하고 보존하여야 하는 경우 추가정보를 가명정보와 분리된 저장소에 암호화하여 저장하여야 한다.※ 반드시 추가정보를 보존하여야 하는 경우를 제외하고 원칙적으로 추가정보는 삭제나. 추가정보에 접근할 수 있는 권한은 정보시스템본부 가명처리 담당자 이외 부여하지 않는다. 다만, 추가정보 접근이 불가피한 경우 CISO의 승인을 득하여 CIO가 일시적으로 부여할 수 있으며, 관련 기록을 보관하고 업무 목적 달성 후 즉시 권한을 삭제하여야 한다.다. 전 나. 항에서 보관하여야 하는 기록은 1)접근자의 신원, 2)승인권자 3)접근일시 4)대상정보 5)조회가 불가피한 사유 및 용도 등이며 해당 기록은 3년간 보관하여야 한다.라. 추가정보를 보관하는 경우 정보시스템본부는 월 1회 이상 재 식별하는데 사용되는지 등에 대한 점검을 하여야 한다.1. 가명정보에 대한 보호조치
2. 정보시스템 본부는 가명처리 전 개인신용정보와 가명처리 한 개인 신용정보를 분리하여 저장하여야 한다.
3. 각 사업본부는 가명정보를 취급하는 담당자를 별도로 지정, 관리하고 가명처리 전 개인신용정보를 취급하는 담당자와 접근권한을 구분하여 운영하여야 한다.
4. 각 사업본부는 가명정보를 취급하는 직원이 가명처리 전 개인신용정보에 접근할 수 있는 권한을 부여하지 않아야 하며, 원본정보 접근이 불가피한 경우 CISO, 신용정보관리 보호인의 사전 승인을 득하여 일시적으로 부여하고 관련 기록을 보관하여야 한다.
5. 전 다. 항에서 보관하여야 하는 기록은 1)접근자의 신원 2)승인권자 3)접근일시 4)대상정보 5)접근이 불가피한 사유 및 용도 등이며 해당 기록은 3년 이상 보관하여야 한다.
6. 각 사업본부는 가명정보 처리 시 1)가명정보의 구체적인 처리 목적 2)처리방법 3)처리일시를 기록하여 가명정보가 파기된 이후 4)파기 담당자 5)파기 일자 6)파기방법 7)파기책임자 확인 등을 함께 기록하여 3년 이상 보관하고, 처리 기록에 대해 월1회 이상 주기적을 확인, 감독하여야 한다.
7. 가명정보를 가명처리 목적 이외 활용하거나(오용), 권한 없는 자에게 배포, 재 식별 시도 등 남용할 경우 CISO 또는 신용정보관리 보호인은 인사위원회에 제재 심의 요청을 한다. 제재 기준은 당행 인사 규정에 따른다.
8. 관리적 보호조치

가명처리한 개인신용정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경, 훼손 및 파괴, 그 밖의 위험으로부터 가명 정보를 보호하기 위해 다음 각 호의 사항을 준수하여야 한다.1. 가명정보 및 추가정보에 대한 접근 권한은 형상관리 시스템을 통하여 절차에 따라 부여, 변경, 말소 처리 되어야 한다.
2. 정보보호팀은 가명정보 및 추가정보가 저장 또는 처리되는 시스템, 단말의 보호 조치를 하여야 한다.
3. 정보시스템본부는 가명정보 및 추가정보에 대한 접근기록을 필수 본 규정에서 정한 기간 동안 보관하여야 하며 이를 매월 1회 정기 점검하여야 한다.
4. 가명정보는 가명처리 시 목적에 따른 이용 기간 동안 보유 한 후 즉시 파기 되어야 한다. 추가정보는 원칙적으로 가명처리 직후 바로 파기되어야 한다. 파기는 본 규정에서 정하는 개인신용정보 파기 기준에 따른다.
5. 정보시스템본부는 가명처리 시 재 식별되지 않도록 하여야 하며, 각 사업본부 담당자는 가명정보가 권한 없는 자가 접근할 수 없도록 관리 하여야 한다.
6. 가명정보는 제3자 제공하지 않는다. 다만, 가명정보 제공이 필요한 사업을 진행 할 경우 본 규정에 가명정보 제공 및 사후관리에 관한 사항을 정하여야 한다.
 | 신용정보법 제40조의2 가명처리 익명처리에 관한 행동규칙 신설에 따라 개정함 |