연계정보 처리 및 **안전조치** 등에 관한 안내서

2025. 6.

방송통신위원회
Korea Communications Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

연계정보 처리 및 **안전조치** 등에 관한 안내서

주의 사항

- 이 안내서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 연계정보의 생성·처리에 관한 규정의 취지와 해석, 규정 준수 여부의 판단 기준 등을 제시하여 연계정보를 이용하고자 하는 기관 및 사업자 등의 이해를 높이고 법적 의무 이행을 돕기 위한 목적으로 발간되었습니다.
-

CONTENTS

I 연계정보 제도

1. 연계정보의 정의

- 연계정보(Connecting Information, CI)는 주민등록번호를 일방향으로 암호화하여 복원할 수 없도록 만든 88바이트(Byte) 길이로 구성되어 있다.

- 연계정보는 정보통신서비스 제공자가 주민등록번호를 직접 처리하지 않으면서도 이용자를 식별하여 개인별 서비스를 제공할 수 있도록 하는 정보로, 신설된 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 규정에서도 연계정보를 "정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보"로 정의하고 있다.

- 연계정보는 고유식별정보인 주민등록번호를 기반으로 생성되어 개인과 밀접하게 연관된 정보라는 점에서 그 중요성이 매우 높다. 특히 암호화된 연계정보가 개인에 관한 다른 정보와 결합할 가능성이 차단되어 있다면 연계정보는 그 자체로서는 개인을 식별해 낼 수 없어 개인정보에 해당하지 않는다고 볼 수 있을 것이나, 다른 정보와의 결합 가능성이 있다면 이를 개인정보로 보고 관리하는 것이 타당하다. 연계정보를 처리하는 주체가 연계정보와 결합 가능성이 있는 이용자의 신원에 대한 정보(성명 등)를 보유하고 있거나 이를 적법하게 입수할 수 있다면 연계정보는 개인정보에 해당하므로, 이를 처리하는 주체는 그 처리 과정에서 연계정보의 유출 내지 노출, 다른 정보와 불법적인 결합, 필요한 목적 외 이용 등 오·남용이 일어나지 않도록 안전성을 확보하여야 하며, 연계정보 정보주체의 권리를 보장하고 합리적이고 안전한 서비스를 제공하기 위해 노력할 필요가 있다.

2. 법률 개정 취지 및 개정 법률의 내용

가. 법률 개정의 필요성

- 온라인·모바일·비대면 중심의 디지털화가 점차 가속화되면서 모바일 전자고지, 금융 마이데이터와 같은 정보 집적 서비스 등 각종 서비스 제공을 위하여 정보통신서비스 제공자가 온라인상에서 개인을 확인하고 식별할 필요성이 점차 높아졌다.

- 그러나 개인정보 보호법에서는 법령상 근거가 있는 경우, 정보주체 등의 급박한 생명·신체· 재산의 이익을 위해 명백히 필요한 경우 등을 제외하면 개인정보처리자가 정보주체의 주민등록번호를 처리할 수 없다고 규정하고 있고(개인정보 보호법 제24조의2 제1항), 정보통신망법 제23조의2 역시 정보통신서비스 제공자는 원칙적으로 이용자의 주민등록번호를 수집 및 이용할 수 없다고 규정하고 있어 주민등록번호를 이용하여 본인을 확인하는 것에는 명백한 한계가 존재한다.

- 기존 정보통신망법(2024. 7. 24. 법률 제20069호로 개정되기 전의 법)은 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법, 즉 대체수단을 개발·제공·관리하는 업무를 수행하는 자를 “본인확인기관”으로 정의하는 한편, 그 지정 및 지정취소에 관한 조항을 두어 본인확인기관을 통한 본인확인업무 수행 및 서비스 제공 가능성을 명문화하였다. 다만, 연계정보의 개념을 비롯하여 본인확인기관이 연계정보를 생성·처리하기 위한 요건, 연계정보를 생성·처리하는 과정의 안전조치 의무 등 준수사항, 본인확인기관으로부터 연계정보를 제공받은 자의 연계정보 처리 제한 등 구체적인 사항에 관하여는 규정하지 않아, 실제 본인확인기관이 연계정보를 생성·처리하거나 정보통신서비스 제공자가 본인확인기관으로부터 연계정보를 제공받아 활용하는 과정에서 그 법률상 근거 및 안전한 처리를 위한 준수사항 등은 다소 불분명한 상태였다.

나. 규제 샌드박스 운영

- 연계정보 활용에 관한 명확한 법적 근거가 부재하는 상황에서 실무상 높은 수요 및 필요성을 제도적으로 뒷받침하기 위하여 과학기술정보통신부와 금융위원회는 방송통신위원회와 협의하여 규제 샌드박스 제도를 활용하여 연계정보 활용에 관한 임시허가(정보통신 진흥 및 융합 활성화 등에 관한 특별법 제37조, 이하 “정보통신융합법”, 금융혁신지원 특별법 제16조 및 제16조, 이하 “금융혁신법”)를 2020년부터 부여하고 있다. 이에 따라 연계정보를 이용하여 모바일 전자고지 및 금융 마이데이터 서비스를 제공하고자 하는 기관(민간, 공공)은 보유하고 있는

주민등록번호를 연계정보로 일괄 변환하기 위해 규제 샌드박스를 통하여 임시허가를 신청하며, 과학기술정보통신부와 금융위원회는 신청기관이 추진하고자 하는 서비스가 연계정보의 처리를 필요로 하는 타당한 서비스인지를 방송통신위원회를 통해 확인하고 임시허가를 부여한다.

- 이후 모바일 전자고지 및 금융 마이데이터 서비스를 이용하고자 하나 주민등록번호만을 보유하고 있는 기관 및 민간 사업자 등은 방송통신위원회 및 한국인터넷진흥원에 연계정보의 일괄 변환을 신청할 수 있고, 신청을 받은 방송통신위원회 및 한국인터넷진흥원은 변환 적합성 여부를 심사하여 그 결과를 회신한다.

- 위 심사 과정에서는 (i) 개별 법령에 따른 주민등록번호 처리 근거가 존재하는지, (ii) 개별 법령의 주민등록번호 처리 목적에 연계정보 변환 목적이 포함되어 있는지, (iii) 주민등록번호 처리 근거와 연계정보 변환 목적이 일치하는지를 기준으로 변환 적합성 여부를 판단한다.

- 다만, 정보통신융합법에 따른 임시허가의 유효기간은 최장 4년인바(정보통신융합법 제37조 제5항), ICT 규제 샌드박스 제도 하에서 연계정보의 변환을 위하여 부여된 임시허가 유효기간의 만료가 다가옴에 따라, 그 만료 전에 연계정보 일괄변환 제도를 공식적인 법제로 포섭하여야 한다는 목소리가 높아졌다.

- 이에 따라 2024년 1월 23일 정보통신망법 개정으로 연계정보의 생성·처리에 관한 근거 조항, 안전한 생성·처리를 위한 안전조치 의무에 관한 조항 등이 신설되었다(정보통신망법 제23조의5, 제23조의6).

다. 개정 사항

- 신설된 정보통신망법 제23조의5는 본인확인기관이 정보통신서비스 제공자의 서비스 연계를 위하여 연계정보 생성·처리를 하는 것을 원칙적으로 금지하는 한편, 예외적으로 제1항 각 호에 해당하는 경우에만 연계정보를 생성·처리할 수 있도록 규정하고 있다. 구체적으로, 이용자가 입력한 정보를 이용하여 이용자를 안전하게 식별·인증하기 위한 서비스를 제공하는 경우(제1호), 「개인정보 보호법」 제24조에 따른 고유식별정보를 보유한 행정기관 및 공공기관(이하 “행정기관 등”)이 연계정보를 활용하여 「전자정부법」 제2조제5호에 따른 전자정부 서비스를 제공하기 위한 경우(제2호), 고유식별정보를 보유한 자가 「개인정보 보호법」 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성·처리를

요청한 경우(제3호), 「개인정보 보호법」 제24조의2제1항 각 호에 따라 주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 아니하고 연계정보 생성·처리가 불가피한 대통령령으로 정하는 정보통신서비스를 제공하기 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받은 경우(제4호)에는 연계정보를 생성·처리할 수 있다고 규정하고 있다. 그 밖에 위 제4호에 따른 방송통신위원회의 연계정보 생성·처리 승인과 관련하여 승인심사 기준 및 승인 취소 사유를 정하고 있으며, 본인확인기관으로부터 연계정보를 제공받은 자(이하 “연계정보 이용기관”)의 연계정보 처리 제한에 대하여도 정하고 있다.

- 또한 정보통신망법 제23조의6은 본인확인기관 및 연계정보 이용기관이 연계정보의 생성·처리 과정에서 취하여야 하는 안전조치 의무를 규정하고 있다.

II 연계정보의 생성·처리

1. 정보통신망법 제23조의5 제1항

정보통신망법

제23조의5(연계정보의 생성·처리 등) ① 본인확인기관은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보(이하 "연계정보"라 한다)를 생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 없다.

1. 이용자가 입력한 정보를 이용하여 이용자를 안전하게 식별·인증하기 위한 서비스를 제공하는 경우
2. 「개인정보 보호법」 제24조에 따른 고유식별정보(이하 이 조에서 "고유식별정보"라 한다)를 보유한 행정기관 및 공공기관(이하 "행정기관 등"이라 한다)이 연계정보를 활용하여 「전자정부법」 제2조제5호에 따른 전자정부 서비스를 제공하기 위한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
   가. 「전자정부법」 제2조제4호에 따른 중앙사무관장기관의 장이 행정기관 등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성·처리를 요청한 경우
   나. 행정기관 등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성·처리를 요청한 경우
3. 고유식별정보를 보유한 자가 「개인정보 보호법」 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성·처리를 요청한 경우
4. 「개인정보 보호법」 제24조의2제1항 각 호에 따라 주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 아니하고 연계정보 생성·처리가 불가피한 대통령령으로 정하는 정보통신서비스를 제공하기 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받은 경우

가. 규정 취지

- 정보통신망법 제23조의5 제1항은 본인확인기관이 연계정보를 생성 또는 처리할 수 있는 경우를 한정적으로 나열하여 규정하고 있다. 이는 본인확인기관의 연계정보 생성·처리의 법적 근거를 신설하는 한편, 그 범위를 연계정보 활용의 필요성이 분명하게 인정되는 경우로 제한함으로써 연계정보가 무분별하게 활용되는 것을 막기 위함이다.

2. 연계정보의 정의

- 제23조의5 제1항은 "연계정보"를 "정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보"로 규정하고 있다.

가. 정보통신서비스 제공자 및 이용자

- 정보통신서비스 제공자는 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무(전기통신설비를 이용하여 다른 사람의 통신을 매개하거나 전기통신설비를 다른 사람의 통신용으로 제공하는 것)를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 의미하므로(정보통신망법 제2조 제3호), 인터넷을 이용하여 온라인상에서 서비스 등을 제공하거나 매개하는 자는 "정보통신서비스 제공자"에 포함된다.

- 한편, 주민등록번호를 연계정보로 처리할 때의 정보주체인 "이용자"는 이러한 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 의미한다(정보통신망법 제2조 제4호).

나. 주민등록번호의 비가역적 암호화

- 이용자의 주민등록번호를 연계정보로 만들어 처리하기 위하여는 해당 정보를 "비가역적으로 암호화"하여야 한다. 이는 고유식별정보인 주민등록번호가 그 자체로 활용되지는 않도록 하면서, 서비스를 제공하고자 하는 대상(개인)을 안전하게 특정·식별할 수 있도록 하기 위한 조치이다. 이때 비가역적 암호화는 일방향 암호화를 의미하는 것으로, 당해 정보만으로는 개인을 식별해 낼 수 없는 수준으로 수행되어야 하며, 나아가 해당 정보를 다시 주민등록번호로 복원해 내는 것 역시 차단할 수 있어야 한다.

다. 연계정보 이용기관

- 연계정보 이용기관이란 본인확인기관으로부터 연계정보를 제공받은 자로서, 일반적으로 본인확인서비스를 이용하는 정보통신서비스 제공자가 연계정보 이용기관에 해당한다. 이 밖에도 본인확인기관으로부터 연계정보를 제공받아 활용하는 국가, 중앙행정기관, 지방자치단체, 그 밖의 국가기관 및 공공단체, 금융기관 등도 역시 연계정보 이용기관에 해당할 수 있다.

3. 연계정보의 생성·처리

- 정보통신망법 제23조의5 제1항은 동조에 따라 본인확인기관이 연계정보를 취급할 수 있는 구체적 방식으로 "생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위(이하 "처리")"를 규정하고 있다.

가. 연계정보의 생성

- 연계정보의 "생성"이란 본인확인기관이 주민등록번호를 비가역적으로 암호화하여 주민등록번호에 일대일 대응되는 암호화된 식별값, 즉 연계정보를 만들어 내는 것을 의미한다. 연계정보의 생성은 정보통신망법 제23조의3 및 본인확인기관 지정 등에 관한 기준 제12조의2 등에 의거하여 방송통신위원회가 지정한 본인확인기관이 수행할 수 있다.

나. 연계정보의 처리

- 연계정보의 "처리"란 연계정보를 본인확인기관 및 연계정보 이용기관이 활용하는 과정 전반을 포함하는 개념이다. 정보통신망법 제23조의5 제1항은 처리의 예시적 형식으로 제공·이용·대조·연계를 제시하고 있다. "제공"이란 본인확인기관이 연계정보 이용기관에 연계정보를 전달하는 행위나 연계정보 이용기관 사이에 연계정보를 대조하기 위하여 연계정보를 전달하는 행위를 의미하며, "이용"이란 본인확인기관 및 연계정보 이용기관이 연계정보를 내부적으로 활용하는 행위 전반을, "대조"는 연계정보 이용기관이 보유하고 있는 연계정보를 비교하여 동일인 여부를 식별하는 행위, "연계"란 동일인 여부 식별을 통하여 연계정보 이용기관 제공 서비스의 통합적 이용을 가능하게 하는 행위를 개념화한 것으로 이해할 수 있다. 한편, "처리"에는 이 같은 행위

외에도 “그 밖에 이와 유사한 모든 행위”가 포함되는데, 개인정보 보호법상 “처리” 정의 규정 등을 고려하여 볼 때, 이러한 행위에는 연계정보의 연동·기록·저장· 보유·가공·편집·검색·출력·정정·복구·공개·파기 등의 행위도 포함될 수 있다.

- 정보통신망법 제23조의5 제4항에 따라 본인확인기관으로부터 연계정보를 제공받은 연계정보 이용기관은 원칙적으로 제공받은 목적 범위에서 연계정보를 처리하여야 한다. 본인확인기관으로부터 제공받은 목적상 연계정보의 저장이 필요한 경우, 연계정보를 저장하는 것이 가능할 수 있다. 예컨대 주민등록번호 정보를 보유한 연계정보 이용기관이 전자고지 업무를 수행하기 위하여 본인확인기관으로부터 연계정보를 제공받아 저장하는 것은 가능하다. 그러나 본인확인기관으로부터 제공받은 목적상 필요하지 않다면, 연계정보의 저장은 허용되지 않는다. 특히 본인확인서비스 제공에 따라 연계정보 이용기관에 제공된 연계정보는, 서비스의 통합적 이용을 가능하게 하기 위하여 다른 연계정보 이용기관에 일시적인 대조·연계 목적으로의 전달이 허용될 뿐이므로, 본인확인기관이 아닌 연계정보 이용기관으로부터 연계정보를 전달받은 이용기관은 목적 달성 시 다른 법률에 별도 근거가 있는 경우 등을 제외하면 해당 연계정보를 바로 파기하여야 하고, 저장 및 보관하여서는 안 된다.

4. 연계정보의 처리가 허용되는 경우

가. 본인확인서비스를 제공하는 경우

- 정보통신망법 제23조의5 제1항 제1호에 따라 본인확인기관은 이용자가 입력한 정보를 활용하여 이용자를 안전하게 식별·인증하고자 하는 경우에는 연계정보를 생성·처리할 수 있다. 이는 정보통신망법 및 같은 법 시행령에 따라 본인확인기관 지정 등에 관한 기준(방송통신위원회 고시 제2022-1호)에서 정의하고 있는 “본인확인서비스”의 정의를 바탕으로 한 규정으로, 본인확인기관이 이용자의 본인확인입력정보를 바탕으로 본인확인서비스를 수행하는 경우를 의미한다.

본인확인기관 지정 등에 관한 기준(방송통신위원회 고시 제2022-1호)

제2조(정의) 이 기준에서 사용하는 용어의 정의는 다음과 같다.

10. “본인확인서비스”라 함은 본인확인입력정보를 이용하여 이용자를 안전하게 식별·인증하기 위해 본인확인기관이 제공하는 서비스를 말한다.

나. 고유식별정보를 보유한 행정기관 등이 전자정부 서비스를 제공하는 경우

- 정보통신망법 제23조의5 제1항 제2호는 개인정보 보호법 제24조에 따른 고유식별정보를 보유한 행정기관 및 공공기관(이하 “행정기관 등”)이 연계정보를 활용하여 전자정부법 제2조 제5호에 따른 전자정부 서비스를 제공하기 위한 경우로 (i) 전자정부법 제2조 제4호에 따른 중앙사무관장기관의 장이 행정기관 등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성·처리를 요청한 경우, (ii) 행정기관 등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성·처리를 요청한 경우에 본인확인기관이 연계정보를 생성하거나 처리할 수 있다고 규정하고 있다.

행정기관, 공공기관, 중앙사무관장기관의 의미(전자정부법 제2조 제2호 내지 제4호)

행정기관: 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함) 및 그 소속 기관, 지방자치단체

공공기관: 공공기관의 운영에 관한 법률 제4조에 따른 법인·단체 또는 기관, 지방공기업법에 따른 지방공사 및 지방공단, 특별법에 따라 설립된 특수법인, 초·중등교육법, 고등교육법 및 그 밖의 다른 법률에 따라 설치된 각급 학교, 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률 제8조제1항에 따른 연구기관, 과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률 제8조제1항에 따른 연구기관

중앙사무관장기관: 국회 소속 기관에 대하여는 국회사무처, 법원 소속 기관에 대하여는 법원행정처, 헌법재판소 소속 기관에 대하여는 헌법재판소사무처, 중앙선거관리위원회 소속 기관에 대하여는 중앙선거관리위원회 사무처, 중앙행정기관 및 그 소속 기관과 지방자치단체에 대하여는 행정안전부

- 정보통신망법 제23조의5 제1항 제2호는 행정기관 등의 요청에 의한 연계정보 생성·처리도 제한적으로만 허용하고 있다. 행정기관 등이 개인정보 보호법 제24조에 따른 고유식별정보를 보유하고 있고, 전자정부법 제2조 제5호에 따른 전자정부 서비스를 제공하기 위하여 연계정보의 활용이 필요한 경우로, 각 목(아래 ①, ②) 중 어느 하나에 해당하여야 본인확인기관이 해당 행정기관 등의 요청에 응하여 연계정보를 생성·처리할 수 있도록 하고 있다. 이때 행정기관 등이 고유식별정보를 개인정보 보호법에 따라 ‘적법하게’ 보유할 것이 요구된다고 해석하는 것이 타당하다. 적법한 보유로 판단되려면, 주민등록번호는 개인정보 보호법 제24조의2 제1항 각 호 중 어느 하나의 경우에 해당하여야 하고, 그 밖의 고유식별정보는 같은 법 제24조 제1항 각 호 중 어느 하나의 경우에 해당하여야 한다.

① 「전자정부법」 제2조제4호에 따른 중앙사무관장기관의 장이 행정기관 등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성·처리를 요청한 경우

- 전자정부법은 행정기관 등이 전자정부(정보기술을 활용하여 행정기관 등의 업무를 전자화하여 행정기관 등의 상호간 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부)를 통하여 다른 행정기관등 및 국민·기업 등에 제공하는 행정서비스를 "전자정부 서비스"로 정의하고 있다(전자정부법 제2조 제5호).

- 중앙사무관장기관의 장은 행정전자서명에 대한 인증업무를 수행하고(전자정부법 제29조) 행정정보의 공동이용에 관한 사항을 관장하는 주체로서(전자정부법 제4장), 전자정부 서비스의 제공과 관련하여 중추적인 역할을 수행한다. 따라서 정보통신망법은 중앙사무관장기관이 각 행정기관 등의 전자정부 서비스 제공을 위하여 이용자 식별 과정을 통합적으로 수행하면서 이를 위한 연계정보의 생성·처리를 요청하는 경우에는 본인확인기관이 연계정보를 생성·처리할 수 있도록 허용하고 있다(정보통신망법 제23조의5 제1항 제2호 가목).

② 행정기관 등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성·처리를 요청한 경우

- 본인확인기관은 행정기관 등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성·처리를 요청한 경우에도 연계정보를 생성하거나 처리할 수 있다(정보통신망법 제23조의5 제1항 제2호 나목).

- 앞서 살펴본 바와 같이, 주민등록번호와 그 밖의 고유식별정보는 개인정보 보호법 제24조 및 제24조의2에 따라 처리가 이루어져야 한다. 정보통신망법은 고유식별정보의 처리 목적 범위 내인 경우에도 이용자의 동의를 받지 않고 연계정보를 생성·처리하는 것이 불가피한 경우에 한하여 연계정보의 생성·처리를 허용함으로써 이용자의 권리침해 가능성을 최소화하고 있다. 이때 이용자의 동의를 받지 않고 연계정보를 생성·처리하는 것이 "불가피한 경우"란, 이와 같이 연계정보를 생성·처리하지 않고는 행정기관 등이 전자정부 서비스를 제공하는 것이 불가능하거나 현저히 곤란한 경우를 의미한다. 행정기관 등이 연계정보를 생성·처리하지 않더라도 전자정부 서비스를 제공할 수 있거나, 연계정보 생성·처리에 대한 이용자의 동의를 받는 것이 가능함에도 단순히 업무상 편의나 효율성만을 위하여 이용자의 동의 없이 연계정보 생성·처리를 요청한다면, 이는 '불가피한 경우'라고 보기 어렵다.

다. 고유식별정보를 보유한 자가 개인정보 전송의무를 수행하기 위하여 연계정보 생성·처리를 요청한 경우

- 정보통신망법 제23조의5 제1항 제3호에 따라 본인확인기관은 고유식별정보를 보유한 자가 개인정보 보호법 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성·처리를 요청한 경우에는 연계정보를 생성·처리할 수 있다.

- 개인정보 보호법은 2023년 3월 14일 법 개정으로 개인정보의 전송 요구권을 신설하였다(개인정보 보호법 제35조의2). 신설된 전송 요구권을 통하여 정보주체는 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 개인정보를 정보주체 자신 또는 개인정보관리 전문기관이나 일반 수신자에게 전송할 것을 요구할 수 있다(개인정보 보호법 제35조의2 제2항).

- 개인정보의 전송 요구가 있는 경우 개인정보처리자로서는 정보주체의 본인 여부를 확인하는 한편, 전송 요구의 상대(정보주체 자신 또는 개인정보관리 전문기관이나 일반 수신자) 역시 식별하여 당해 개인정보를 전송하여야 한다. 이때 정보주체의 본인 여부가 확인되지 않는 경우 등에는 전송 요구를 거절하거나 중단할 수 있다(개인정보 보호법 제35조의2 제6항). 즉 개인정보처리자로서는 전송 요구를 이행하고 정보주체의 전송 요구권을 보장하기 위하여 정보주체를 정확히 특정할 필요성이 발생하고, 이 같은 식별 과정을 보다 안전하게 수행하기 위하여는 연계정보를 생성·처리할 필요성이 인정된다고 할 수 있다. 따라서 본인확인기관은 개인정보처리자가 정보주체의 전송 요구권 보장을 위한 전송 의무 수행 과정에서 정보주체의 식별을 필요로 하여 요청하는 경우에는 정보통신망법 제23조의5 제1항 제3호에 따라 연계정보를 생성·처리할 수 있다.

개인정보 보호법

제35조의2(개인정보의 전송 요구) ① 정보주체는 개인정보 처리 능력 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 다음 각 호의 요건을 모두 충족하는 개인정보를 자신에게로 전송할 것을 요구할 수 있다.

1. 정보주체가 전송을 요구하는 개인정보가 정보주체 본인에 관한 개인정보로서 다음 각 목의 어느 하나에 해당하는 정보일 것
   가. 제15조제1항제1호, 제23조제1항제1호 또는 제24조제1항제1호에 따른 동의를 받아 처리되는 개인정보
   나. 제15조제1항제4호에 따라 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 처리되는 개인정보
   다. 제15조제1항제2호·제3호, 제23조제1항제2호 또는 제24조제1항제2호에 따라 처리되는 개인정보

중 정보주체의 이익이나 공익적 목적을 위하여 관계 중앙행정기관의 장의 요청에 따라 보호위원회가 심의·의결하여 전송 요구의 대상으로 지정한 개인정보

2. 전송을 요구하는 개인정보가 개인정보처리자가 수집한 개인정보를 기초로 분석·가공하여 별도로 생성한 정보가 아닐 것
3. 전송을 요구하는 개인정보가 컴퓨터 등 정보처리장치로 처리되는 개인정보일 것

② 정보주체는 매출액, 개인정보의 보유 규모, 개인정보 처리 능력, 산업별 특성 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 제1항에 따른 전송 요구 대상인 개인정보를 기술적으로 허용되는 합리적인 범위에서 다음 각 호의 자에게 전송할 것을 요구할 수 있다.

1. 제35조의3제1항에 따른 개인정보관리 전문기관
2. 제29조에 따른 안전조치의무를 이행하고 대통령령으로 정하는 시설 및 기술 기준을 충족하는 자

③ 개인정보처리자는 제1항 및 제2항에 따른 전송 요구를 받은 경우에는 시간, 비용, 기술적으로 허용되는 합리적인 범위에서 해당 정보를 컴퓨터 등 정보처리장치로 처리 가능한 형태로 전송하여야 한다.

④ 제1항 및 제2항에 따른 전송 요구를 받은 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 법률의 관련 규정에도 불구하고 정보주체에 관한 개인정보를 전송하여야 한다.

1. 「국세기본법」 제81조의13
2. 「지방세기본법」 제86조
3. 그 밖에 제1호 및 제2호와 유사한 규정으로서 대통령령으로 정하는 법률의 규정

⑤ 정보주체는 제1항 및 제2항에 따른 전송 요구를 철회할 수 있다.

⑥ 개인정보처리자는 정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 제1항 및 제2항에 따른 전송 요구를 거절하거나 전송을 중단할 수 있다.

⑦ 정보주체는 제1항 및 제2항에 따른 전송 요구로 인하여 타인의 권리나 정당한 이익을 침해하여서는 아니 된다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 전송 요구의 대상이 되는 정보의 범위, 전송 요구의 방법, 전송의 기한 및 방법, 전송 요구 철회의 방법, 전송 요구의 거절 및 전송 중단의 방법 등 필요한 사항은 대통령령으로 정한다.

라. 개인정보 보호법에 따라 주민등록번호의 처리가 허용된 경우로서 이용자의 동의 없는 연계정보 생성·처리가 불가피한 정보통신서비스를 제공하기 위하여 방송통신위원회의 승인을 받은 경우

- 정보통신망법 제23조의5 제1항 제4호는 개인정보 보호법 제24조의2 제1항 각 호에 따라 주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 않고 연계정보 생성·처리가 불가피한 대통령령으로 정하는 정보통신서비스를 제공하기 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받은 경우에는 본인확인기관이 연계정보를 생성·처리할 수 있다고 규정하고 있다.

● 즉, 법 제23조의5 제1항 제4호에 따라 연계정보를 생성·처리하기 위하여는 ① 연계정보 이용기관이 제공하고자 하는 정보통신서비스를 위한 주민등록번호의 처리가 개인정보 보호법에 근거하여 허용되어야 하며, ② 해당 서비스 제공을 위하여 이용자의 동의를 받지 않고 연계정보를 생성·처리하는 것이 불가피하여야 하고, ③ 나아가 본인확인기관과 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받아야 한다.

※ 이 호에서 "개인정보 보호법 제24조의2 제1항 각 호에 따라 주민등록번호 처리가 허용"될 것을 요구하는 것은 연계정보 이용기관이 제공하고자 하는 '정보통신서비스'에 대한 것인바, 본인확인기관과 함께 방송통신위원회 승인을 신청하는 정보통신서비스 제공자가 법령에 따른 주민등록번호 처리 근거를 보유하여야 하는 것은 아니다. 정보통신망법 시행령 제10조는 위 법 제23조의5 제1항 제4호에 따른 "대통령령으로 정하는 정보통신서비스"를 다음과 같이 구체화하고 있다.

정보통신망법 시행령

제10조(연계정보 생성·처리가 불가피한 정보통신서비스) ① 법 제23조의5제1항제4호에서 "대통령령으로 정하는 정보통신서비스"란 다음 각 호의 어느 하나에 해당하는 정보통신서비스를 말한다.

1. 법령에 따라 이용자에게 고지하는 사항을 「전자문서 및 전자거래 기본법」 제2조제10호에 따른 공인전자문서중계자를 통해 고지하는 서비스
2. 「신용정보의 이용 및 보호에 관한 법률」 제33조의2제1항에 따른 전송 요구에 따라 개인신용정보를 같은 법 제2조제9호의3에 따른 본인신용정보관리회사를 통해 해당 신용정보주체 본인에게 전송하는 서비스
3. 제1호 또는 제2호와 유사한 서비스로서 방송통신위원회가 법 제23조의5제1항 각 호 외의 부분에 따른 연계정보(이하 "연계정보"라 한다)의 생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위(이하 "처리"라 한다)가 불가피하다고 인정하여 고시하는 서비스

② 방송통신위원회는 제1항제3호에 따른 서비스를 고시하려는 경우에는 개인정보보호위원회와 합의해야 한다.

① 법령에 따라 이용자에게 고지하는 사항을 「전자문서 및 전자거래 기본법」 제2조제10호에 따른 공인전자문서중계자를 통해 고지하는 서비스

- 법령에 따라 이용자에게 고지하여야 하는 사항을 전자문서 및 전자거래 기본법 제2조 제10호에 따른 공인전자문서중계자를 통하여 고지하는 서비스는 이른바 "전자고지 서비스"를 의미한다.

전자문서 및 전자거래 기본법

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

10. "공인전자문서중계자"란 타인을 위하여 전자문서의 송신·수신 또는 중계(이하 "전자문서유통"이라 한다)를 하는 자로서 제31조의18에 따른 인증을 받은 자를 말한다.

- 개별 법령상 주민등록번호 처리 근거가 존재하여 개인정보 보호법 제24조의2 제1항에 따라 개인정보를 처리할 수 있는 자가 전자고지를 이행하고자 하는 경우, 우선 공인전자문서중계자의 이용자와 고지대상이 동일인임을 식별하여야 하며, 대상 식별을 위해서는 주민등록번호 또는 연계정보가 필요하다. 그러나 전자고지를 하려는 자는 근거 법령에 따라 주민등록번호를 적법하게 보유하고 있는 반면, 공인전자문서중계자는 주민등록번호 처리 근거를 보유하고 있지 않다.

- 결과적으로 전자고지를 하려는 자가 자신이 보유한 주민등록번호를 연계정보로 변환하여 공인전자문서중계자에게 제공하면, 공인전자문서중계자가 기존에 보유한 연계정보와 제공받은 연계정보를 대조하여 이용자를 특정하는 과정이 불가피하다. 이에 따라 정보통신망법은 전자고지 서비스를 제공하기 위하여 필요한 경우로 본인확인기관과 정보통신서비스 제공자(예컨대 공인전자문서중계자)가 방송통신위원회의 승인을 받은 경우에는 연계정보의 생성·처리를 허용하고 있다. 다만, 이때 연계정보 생성의 기초가 되는 주민등록번호의 처리는 개인정보 보호법 제24조의2 제1항 각 호에 따른 적법한 주민등록번호 처리 근거에 기초하므로, 그 처리 근거에 이행하고자 하는 전자고지에 관한 사항도 포함되었다고 볼 수 있는 경우에 한하여 연계정보 생성·처리가 가능하다고 보아야 한다.

② 「신용정보의 이용 및 보호에 관한 법률」 제33조의2 제1항에 따른 전송 요구에 따라 개인신용정보를 같은 법 제2조제9호의3에 따른 본인신용정보관리회사를 통해 해당 신용정보주체 본인에게 전송하는 서비스

- 신용정보의 이용 및 보호에 관한 법률(이하 “신용정보법”) 제33조의2 제1항에 따른 전송 요구에 따라 개인신용정보를 같은 법 제2조 제9호의3에 따른 본인신용정보관리회사를 통해 해당 신용정보주체 본인에게 전송하는 서비스는 본인신용정보관리 서비스, 이른바 “금융 마이데이터 서비스”를 의미한다.

신용정보의 이용 및 보호에 관한 법률

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

9의2. “본인신용정보관리업”이란 개인인 신용정보주체의 신용관리를 지원하기 위하여 다음 각 목의 전부 또는 일부의 신용정보를 대통령령으로 정하는 방식으로 통합하여 그 신용정보주체에게 제공하는 행위를 영업으로 하는 것을 말한다.

9의3. “본인신용정보관리회사”란 본인신용정보관리업에 대하여 금융위원회로부터 허가를 받은 자를 말한다.

- 신용정보법은 개인인 신용정보주체는 신용정보제공·이용자 등(신용정보법 제22조의9 제3항 제1호 참고;. 대통령령으로 정하는 신용정보제공·이용자나 「개인정보 보호법」에 따른

공공기관으로서 대통령령으로 정하는 공공기관 또는 본인신용정보관리회사)에 대하여 자신의 개인신용정보를 신용정보주체 본인, 본인신용정보관리회사, 대통령령으로 정하는 신용정보제공·이용자, 개인신용평가회사, 기타 법령으로 정하는 자에게 전송할 것을 요구할 수 있다고 규정하고 있다(신용정보법 제33조의2 제1항).

- 금융 마이데이터 서비스에서 개인신용정보의 안전한 전송 및 활용을 위해 주민등록번호 대신 연계정보를 공통 식별자로 사용하기로 결정됨에 따라 신용정보제공·이용자 등으로서는 전송의무를 이행하기 위하여 자신이 보유한 주민등록번호를 바탕으로 연계정보를 생성하고, 이를 본인신용정보관리회사에 제공하여 개인신용정보를 전송받을 신용정보주체를 특정하도록 할 필요가 있다.

- 따라서 본인확인기관은 정보통신망법 제23조의5 제1항 제4호 및 같은 법 시행령 제10조 제1항 제2호에 따라 금융 마이데이터 서비스를 통하여 본인에게 개인신용정보를 전송하고자 하는 정보통신서비스 제공자(신용정보제공·이용자 등)와 함께 방송통신위원회의 승인을 받는 경우 연계정보를 생성·처리할 수 있다. 다만, 이 경우에도 전자고지 서비스 제공을 위한 경우(정보통신망법 시행령 제10조 제1호)와 동일하게 개인신용정보를 전송하고자 하는 신용정보제공·이용자 등에게 주민등록번호를 보유할 법령상 근거가 존재하여야 한다.

③ 제1호 또는 제2호와 유사한 경우로서 방송통신위원회가 개인정보 보호위원회와 협의하여 법 제23조의5 제1항 각 호 외의 부분에 따른 연계정보의 생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위가 불가피하다고 인정하여 고시하는 서비스

- 정보통신망법 시행령 제10조 제1항 제3호에서는 같은 항 제1호, 제2호와 유사한 경우로서 방송통신위원회가 개인정보보호위원회와 협의하여 연계정보의 생성 또는 처리가 불가피하다고 인정하여 고시하는 서비스를 규정하고 있다. 이에 따라 이러한 서비스에 대하여도 본인확인기관과 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받은 경우 연계정보를 생성·처리할 수 있다.

5. 벌칙 규정

위반 행위	벌칙	조문
정보통신망법 제23조5 제1항을 위반하여 연계정보를 생성·처리한 자	5년 이하의 징역 또는 5천만 원 이하의 벌금	제71조 제1항 제9호

Ⅲ 연계정보의 생성·처리 승인

1. 정보통신망법 제23조의5 제2항

정보통신망법

제23조의5(연계정보의 생성·처리 등) ② 방송통신위원회는 제1항제4호에 따라 연계정보의 생성·처리를 승인하려는 경우 다음 각 호의 사항을 종합적으로 심사하여야 한다.

1. 제공 서비스 구현의 적절성 및 혁신성
2. 연계정보 생성·처리 절차의 적절성
3. 연계정보 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치 계획
4. 이용자 권리 보호 방안의 적절성
5. 관련 시장과 이용자 편익에 미치는 영향 및 효과

가. 규정 취지

- 앞서 살펴본 바와 같이 정보통신망법 제23조의5 제1항 제4호 및 같은 법 시행령 제10조 제1항에 따라 특정 정보통신서비스를 제공하기 위하여 이용자의 동의 없이 연계정보의 생성·처리가 불가피한 경우, 연계정보 생성·처리 과정의 적절성 및 안전성 확보를 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송통신위원회의 사전 승인을 받도록 규정하고 있으며, 이를 위하여 대통령령 및 고시를 통하여 연계정보 생성·처리 승인심사 절차 및 기준을 상세히 마련하여 공정성과 투명성을 제고하였다.

2. 연계정보 생성·처리에 대한 승인신청

가. 본인확인서비스를 제공하는 경우

- 방송통신위원회의 승인을 받아야 하는 서비스는 “연계정보 생성·처리가 불가피한 정보통신서비스”를 수행하려는 경우로 정보통신망법 제23조의5 제1항제4호 및 정보통신망법 시행령 제10조가 이를 세 가지로 구분하여 구체적으로 나열하고 있는데, 다음과 같다. 이에 관해서는 이 안내서 Ⅱ. 4. 라.에서 자세히 설명하였다.

  ① 법령에 따라 이용자에게 고지하는 사항을 「전자문서 및 전자거래 기본법」 제2조제10호에 따른 공인전자문서중계자를 통해 고지하는 서비스(전자고지 서비스, 정보통신망법 시행령 제10조제1항제1호)

  ② 「신용정보의 이용 및 보호에 관한 법률」 제33조의2제1항에 따른 전송 요구에 따라 개인신용정보를 같은 법 제2조제9호의3에 따른 본인신용정보관리회사를 통해 해당 신용정보 주체 본인에게 전송하는 서비스(금융 마이데이터 서비스, 정보통신망법 시행령 제10조제1항제2호)

  ③ 정보통신망법 시행령 제10조제1항제1호 또는 제2호와 유사한 서비스로서 방송통신위원회가 법 제23조의5제1항 각 호 외의 부분에 따른 연계정보의 생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위가 불가피하다고 인정하여 고시하는 서비스(정보통신망법 시행령 제10조제1항제3호).

나. 승인신청 기관

- 정보통신망법 시행령 제10조제1항 각 호가 정한 서비스를 수행하려는 본인확인기관 및 정보통신서비스 제공자가 공동으로 승인을 신청하여야 한다. 이는 정보통신망법 시행령 제10조 제1항 각 호가 정한 서비스의 경우, 이용자의 동의 없이 연계정보가 일괄적으로 생성·처리된다는 점을 고려하여 연계정보를 생성·처리하는 주체인 본인확인기관과 정보통신서비스 제공자 모두에 대하여 연계정보 생성·처리 과정의 적절성 및 안전성 확보 등에 관한 심사기준을 충족하고 있는지를 심사하기 위함이다.

다. 승인신청 방법

- 정보통신망법 시행령 제10조제1항 각 호가 정한 서비스를 수행하려는 본인확인기관 및 정보통신서비스 제공자는 「연계정보 생성·처리 승인신청서」(고시 별지 제1호 서식)를 방송통신위원회에 제출하여야 하며, 신청서를 제출할 때에는 다음 서류(원본 1부, 사본 각 7부 및 이동식 저장매체 1벌)를 함께 첨부하여야 한다(정보통신망법 시행령 제11조제1항, 고시 제3조)

- 승인신청을 하고자 하는 본인확인기관 및 정보통신서비스 제공자는 고시 [별표 1]의 사업계획서 작성요령에 따라 사업계획서를 작성하되, 고시 [별표 2] 심사사항별 세부 평가기준 및 평가항목의 목차에 따라 작성하여야 하며, 작성내용의 증빙을 위하여 부속서류 및 관련 증빙자료를 첨부하여야 한다.

[승인신청 시 구비서류(시행령 제11조 제1항, 고시 제3조 및 별표 1)]

1. 본인확인기관 및 정보통신서비스 제공자의 조직·인력 및 설비 등의 현황을 기재한 사업계획서 : 고시 [별표 1]의 사업계획서 작성요령에 따라 작성
2. 시행령 제12조에 따른 승인심사 사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류
3. 본인확인기관 및 정보통신서비스 제공자의 정관 또는 단체의 규약(법인 또는 단체인 경우에만 해당)
4. 본인확인기관 및 정보통신서비스 제공자의 과거 3개년간 재무제표(법인 또는 단체인 경우에만 해당)

라. 승인신청 서류의 추가 및 수정

- 승인신청기관은 서류의 수정이 필요한 경우 「연계정보 생성·처리 승인신청서」 및 구비서류를 승인심사 전일까지 수정할 수 있으며, 방송통신위원회는 필요시 승인신청기관에게 자료의 제출을 요구할 수 있다. 이 경우 서류 및 자료 제출 보완에 필요한 기간은 심사 기간에 포함되지 않는다(고시 제5조).

3. 승인심사 기준

- 방송통신위원회는 승인심사 기준에 따라 심사를 진행하여 승인 여부를 결정하며, 승인심사 사항

및 심사사항별 세부 평가기준 및 평가항목은 다음과 같다(정보통신망법 시행령 제12조, 고시 제6조 및 [별표 2]).

[심사사항별 세부심사기준의 평가기준 및 평가방법]

1. 제공 서비스 구현의 적절성 및 혁신성
   가. 제공 서비스 구현을 위한 연계정보 생성·처리의 필요성
   나. 기존 유사 서비스와의 차별성
2. 연계정보 생성·처리 절차의 적절성
   가. 관련 법령 및 내부 규정에 따른 연계정보 생성·처리 절차의 적절성
3. 연계정보 생성·처리의 안전성 확보를 위한 영 제13조제1항 각 호의 조치에 관한 계획의 적절성
   가. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치
   나. 물리적·기술적·관리적 조치를 총괄하는 책임자 지정 등 연계정보 생성·제공을 위한 내부 규정의 수립 및 시행
   다. 연계정보 생성 소프트웨어에 대한 보안 통제
   라. 연계정보의 위조·변조 방지 조치
   마. 연계정보 생성·처리 사실 확인자료의 기록·보관
4. 이용자 권리 보호 방안의 적절성
   가. 연계정보 생성·처리의 정지 및 생성된 연계정보의 삭제 등 이용자 권리 보호 방안
   나. 이용자 불만 등의 접수 및 처리에 관한 절차
   다. 이용자 피해 예방 및 안전성 확보 조치 방안
5. 관련 시장과 이용자 편익에 미치는 영향 및 효과
   가. 관련 산업의 활성화 및 비용 절감 등 제공 서비스가 관련 시장에 미치는 영향 및 효과
   나. 이용 편의성 및 경제적 이익 등 제공 서비스가 이용자 편익에 미치는 영향 및 효과

가. 제공 서비스 구현의 적절성 및 혁신성

- 제공하려고 하는 서비스의 내용 및 구조상 연계정보의 생성·처리가 필수적으로 필요한 경우이어야 하고, 기존 유사 서비스보다 혁신적이거나 높은 편의성을 갖는 등 차별성 있는 서비스 구현을 위하여 연계정보를 생성·처리하는 경우이어야 한다.

- 전자고지 서비스, 금융 마이데이터 서비스를 위하여 연계정보를 생성·처리하고자 하는 승인신청기관은 사실상 이 요건을 충족한 것으로 평가된다. 다만, 정보통신망법 시행령 제10조제1항 제3호의 “제1호 또는 제2호와 유사한 서비스로서 방송통신위원회가 법 제23조의5제1항 각 호 외의 부분에 따른 연계정보의 생성 또는 제공·이용·대조·연계 등 그 밖에 이와 유사한 행위가

불가피하다고 인정하여 고시하는 서비스"에 해당하는 경우에는 사업계획서 기재 내용을 기초로 제공 서비스 구현을 위하여 연계정보의 생성·처리가 필수적으로 필요한지와 기존 유사 서비스와 차별성이 있는 새로운 서비스에 해당하는지에 대하여 실질적으로 판단하여야 한다.

나. 연계정보 생성·처리 절차의 적절성

- 본인확인기관이 연계정보를 생성하여 정보통신서비스 제공자에게 제공하고, 이후 정보통신서비스 제공자가 이용·대조·연계, 그 밖에 이와 유사한 모든 행위(저장·보유·파기 포함)를 하는 일련의 처리 절차 전반에 걸쳐 개인정보 보호법 및 정보통신망법을 포함한 관련 법률의 위반 사항은 없는지 그 적절성을 종합적으로 심사하는 항목이다.

- 연계정보 생성·처리 절차의 적절성(사전 심사이므로 연계정보의 생성·제공 계획을 포함) 심사를 위해서는 본인확인기관 및 정보통신서비스 제공자 상호간 연계정보 생성·처리를 위한 관련 계약서 및 연계정보 흐름도, 서비스 구조도 등을 기초로 이를 평가한다.

다. 연계정보 생성·처리의 안전성 확보를 위한 시행령 제13조제1항 각 호의 조치에 관한 계획의 적절성

① 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치(시행령 제13조 제1항 제1호)

- 연계정보를 생성·제공하는 본인확인기관에 대하여 본인확인기관 지정 심사기준인 정보통신망법 시행령 제9조의3 제1항 제1호 각 목에서 정한 세부 심사기준 사항의 준수 여부를 심사한다. 다만, 본인확인기관의 경우 지정심사 및 정기심사를 통하여 본인확인업무의 안정성 확보를 위한 물리적·기술적·관리적 조치 여부를 수시로 평가하고 있기 때문에 해당 평가 결과를 원용하는 형태의 서류심사로 갈음할 수 있다.

② 물리적·기술적·관리적 조치를 총괄하는 책임자 지정 등 연계정보 생성·제공을 위한 내부규정 수립 및 시행(시행령 제13조 제1항 제2호)

- 본인확인기관에 대하여 고시 제10조 및 고시 [별표 3] 본인확인기관의 물리적·기술적·관리적 조치상의 하위 항목 '1. 연계정보 생성·처리를 위한 연계정보 내부관리계획 수립 및 시행에 관한 사항' 준수와 동일한 내용을 심사한다. 이에 관해서는 이 안내서 [부록]의 Ⅰ. 1.에서 자세히 설명하고 있다.

③ 연계정보 생성 소프트웨어에 대한 보안 통제 및 연계정보의 위조·변조 확인 등의 보호조치 (시행령 제13조 제1항 제3호, 제4호)

- 본인확인기관에 대하여 고시 제10조 및 고시 [별표 3] 본인확인기관의 물리적·기술적·관리적 조치상의 하위 항목 '2. 연계정보 생성 소프트웨어에 대한 보안 통제에 관한 사항' 및 '3. 연계정보의 위조·변조 방지 조치에 관한 사항'과 동일한 내용을 심사한다. 이에 관해서는 이 안내서 [부록]의 Ⅰ. 2. 및 3.에서 자세히 설명하고 있다.

④ 연계정보 생성·처리 사실 확인자료의 기록·보관(시행령 제13조 제1항 제5호)

- 본인확인기관에 대하여 고시 제10조 및 고시 [별표 3] 본인확인기관의 물리적·기술적·관리적 조치상의 하위 항목 '4. 연계정보 생성·처리 사실 확인자료의 기록·보관에 대한 조치 사항'과 동일한 내용을 심사한다. 이에 관해서는 이 안내서 [부록]의 Ⅰ. 4.에서 자세히 설명하고 있다.

라. 이용자 권리 보호 방안의 적절성

① 연계정보 생성·처리의 정지 및 생성된 연계정보의 삭제 등 이용자 권리 보호 방안

- 이용자는 연계정보 생성·처리의 정지 및 삭제 등을 요구할 수 있고, 본인확인기관 및 정보통신서비스 제공자는 이용자가 해당 권리를 행사할 수 있도록 권리 행사 방법 및 절차를 마련하여야 하며, 이용자의 권리 행사에 따른 조치 결과를 회신하여야 한다. 또한 연계정보 생성·처리의 정지 및 삭제 등을 요구받은 경우 본인확인기관 및 정보통신서비스 제공자는 연계정보를 지체 없이 파기하는 등 필요한 조치를 취하여야 한다.

② 이용자 불만 등의 접수 및 처리에 관한 절차

- 본인확인기관 및 정보통신서비스 제공자는 연계정보의 생성·처리 등과 관련한 불만을 접수하고 처리할 수 있는 상담창구(예시 : 전화·ARS·이메일·게시판 등)를 마련하여야 한다. 이 경우 이용자 불만 접수 및 처리에 관한 기록을 남기고, 법적 요건 등을 고려하여 보유기간을 설정하여야 하며, 보유기간 경과 시 이용자 불만 관련 자료를 파기하는 절차를 마련하여야 한다,

③ 이용자 피해 예방 및 안전성 확보 조치 방안

- 본인확인기관 및 정보통신서비스 제공자는 연계정보의 분실·훼손·도난·유출을 방지하기 위하여 고시 제10조 및 고시 [별표 3] 본인확인기관의 물리적·기술적·관리적 조치를 포함한

정보통신망법, 개인정보 보호법 등에 따른 안전성 확보 조치 방안을 마련하여야 한다. 또한 이용자의 피해를 예방하기 위하여 이용자가 연계정보의 분실·훼손·도난·유출을 신고할 수 있는 기능을 제공하여야 한다.

마. 관련 시장과 이용자 편익에 미치는 영향 및 효과

- 제공하려고 하는 서비스의 내용 및 특성, 예상 이용자 규모 및 사용 빈도, 사용 편의성 등을 고려하여 제공 서비스의 승인이 관련 산업의 활성화 및 비용 절감 등 관련 시장에 긍정적인 영향과 효과를 가져와야 하고, 이용자에게도 편리성 및 경제적 이익 등 편익을 제공하여야 한다.

4. 승인심사 절차

- 방송통신위원회는 승인신청기관의 승인 신청을 접수하면 연계정보 생성·처리 승인심사를 위한 계획을 수립·시행한다. 승인심사 계획에는 ① 승인심사 일정, 장소 및 절차, ② 승인심사위원회의 구성 및 운영에 관한 사항, ③ 기타 승인심사를 위하여 필요한 사항을 포함한다(고시 제4조).

- 승인심사위원은 ①「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 부교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 정보보호 또는 법학 연구경력이 10년 이상인 자, ② 정부·공공기관 또는 정보보호 관련 업체 또는 단체(협회, 조합)에서 10년 이상 정보보호 분야에 근무한 자, ③ 정보보호 관련 심사제도의 인증심사원 자격이 있는 자, ④ 정보보호 관련 분야 기술사 또는 변호사나 공인회계사의 자격이 있는 자, ⑤ 그 밖에 정보보호에 관한 학식과 경험이 풍부한 자 중 10명 이내로 구성되며, 위촉된 승인심사위원 중 승인신청기관과 이해관계가 있는 경우에는 위촉을 거부하거나, 승인심사 업무 수행이 불가한 사실을 즉시 방송통신위원회에 알려야 한다(고시 제8조).

- 승인심사는 서류심사를 원칙으로 하며, 제출된 사업계획서 및 구비서류, 증빙서류를 기초로 심사한다. 다만, 심사과정에서 필요한 경우 별도 현장실사를 실시할 수 있으며, 현장실사는 승인신청기관에 대한 청문 및 담당자 인터뷰를 포함한다. 승인심사를 위하여 필요한 경우 서류심사 및 현장실사 단계에서 승인신청기관에게 자료의 제출을 요청하거나 그 의견을 들을 수 있다(정보통신망법 시행령 제11조 제3항, 고시 제7조 제1항, 제3항).

5. 승인결정 및 통보 기간

- 방송통신위원회는 심의·의결을 거쳐 연계정보 생성·처리 승인 여부를 결정한다(고시 제9조 제1항).

- 방송통신위원회는 심사사항별 세부 심사기준에 대해서는 절대 평가방식으로 적합 또는 부적합으로 평가하며, 승인신청기관이 각 세부심사 기준에서 모두 적합 판정을 받은 경우 연계정보 생성·처리를 승인한다. 다만, 일부 항목에 대한 개선이 필요하다고 판단되는 경우에는 일정 기간 내에 해당 사항에 대한 개선 등의 조건을 붙여 승인할 수 있다(고시 제7조 제2항). 조건부 승인의 경우에는 조건 이행 여부를 확인한 후 승인서를 교부한다.

- 방송통신위원회는 승인신청을 받은 경우 신청을 받은 날로부터 90일 이내에 세부심사기준의 적합 여부를 심사하여 승인심사 결과를 승인신청기관에게 통보하여야 한다. 다만, 부득이한 사유가 있을 때에는 그 사유를 알리고 30일의 범위에서 그 기간을 연장할 수 있다(시행령 제11조 제4항, 고시 제9조 제2항). 이때 앞서 언급한 바와 같이 서류 및 자료 제출 보완에 필요한 기간은 심사 기간에 포함되지 않는다(고시 제5조).

Ⅳ 연계정보 생성·처리 승인의 취소

1. 정보통신망법 제23조의5 제3항

정보통신망법

제23조의5(연계정보의 생성·처리 등) ③ 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에 제1항제4호에 따른 연계정보 생성·처리 승인을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 그 승인을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 제1항 제4호에 따른 연계정보 생성·처리 승인을 받은 경우
2. 제2항 각 호에 따른 심사사항에 부적합하게 된 경우
3. 제23조의6제1항에 따른 물리적·기술적·관리적 조치 의무를 위반한 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

가. 규정 취지

- 정보통신망법 제23조의5 제3항에 따라 연계정보의 생성·처리 승인은 일정한 사유가 있는 경우 취소될 수 있다. 연계정보 생성·처리 승인 취소 사유는 승인 이전에 발생한 사유(거짓이나 그 밖의 부정한 방법으로 연계정보 생성·처리 승인을 받은 경우; 정보통신망법 제23조의5 제3항 제1호) 및 연계정보 생성·처리 승인 이후 발생한 사유(사후에 연계정보 심사사항에 부적합하게 된 경우, 물리적·기술적·관리적 조치 의무를 위반한 경우, 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우; 동조 제2호 내지 제4호)로 구분된다.

- 연계정보 생성·처리 승인의 취소는 제도의 실효성 및 이용자를 보호하기 위하여 이루어진다. 구체적으로, 부정한 방법으로 인한 승인이 이루어진 경우 등 연계정보의 생성·처리가 이용자의 권리를 침해할 우려가 있는 경우 승인이 취소될 수 있다. 이로써 연계정보의 생성·처리에 대한 관리·감독이 이루어진다.

- 승인 취소 처분에 대한 불복 방법은 정보통신망법상 규정되어 있지 않다. 다만, 승인이 취소된 본인확인기관 또는 정보통신서비스 제공자는 행정소송 및 행정심판을 통하여 해당 처분에 대해 불복할 수 있다.

2. 연계정보 생성·처리 승인의 취소 사유

가. 개관

- 정보통신망법 제23조의5 제1항에 따라 연계정보는 특정한 경우에만 생성·처리될 수 있다. 방송통신위원회의 승인이 있는 경우도 연계정보의 생성·처리가 가능한 경우에 포함된다(정보통신망법 제23조의5 제1항 제4호). 이러한 승인은 이용자의 권리 보호 및 안전성 확보가 보장된 경우에만 이루어진다. 다만, 연계정보의 생성·처리 과정에서 이용자의 권리 보호 등이 원활히 이루어지지 못할 사유가 발견된 경우 승인이 취소될 수 있다.

- 연계정보의 생성·처리 승인에 대한 취소 사유는 정보통신망법 제23조의5 제3항 각 호에 나열되어 있다. 각 사유는 발생 시기를 기준으로 승인 이전에 발생한 사유 및 승인 이후에 발생한 사유로 구분할 수 있다.

나. 부정한 방법에 의한 승인

- 정보통신망법 제23조의5 제3항 제1호에 따라 “거짓이나 그 밖의 부정한 방법”으로 연계정보 생성·처리에 관한 승인을 받은 경우 승인이 취소될 수 있다. 특히 다른 사유들과는 달리 부정한 방법으로 연계정보 생성·처리 승인을 받은 사실이 확인된 경우에는 방송통신위원회는 승인을 취소하여야 한다(정보통신망법 제23조의5 제3항 단서).

- 즉, 다른 사유들과는 달리 이러한 사유가 확인된 경우 기존의 승인 처분은 반드시 취소되어야 한다. 거짓 등 부정한 방법으로 승인을 받은 경우 본인확인기관 및 정보통신서비스 제공자의 귀책이 크기 때문에 다른 사정에도 불구하고 기존의 승인 처분은 취소된다.

다. 연계정보 생성·처리에 대한 승인 관련 심사사항에 부적합하게 된 경우

- 정보통신망법 제23조의5 제3항 제2호에 따라 연계정보 생성·처리에 대한 승인 관련 심사사항에 부적합하게 된 경우에는 승인이 취소될 수 있다. 즉, 연계정보 생성·처리에 대한 승인이 이루어진 시점에는 모든 요건이 구비되었으나, 이후 승인을 받기에 부적합한 수준으로 변경된 경우 승인이 취소될 수 있다. 여기에서 말하는 심사사항에는 정보통신망법 제23조의 제2항 각 호에 규정된 사항뿐 아니라 같은 법 시행령 제12조에 규정된 승인심사 사항별 세부 심사기준에 해당하는 사항이 변경된 경우도 포함된다.

- 이는 부정한 방법 등으로 승인을 받은 경우(정보통신망법 제23조의5 제3항 제1호)와는 달리 기존에는 승인을 받을 수 있는 상태였으나 승인 이후 심사사항 중 일부와 관련된 상태가 변경된 경우를 의미한다. 이러한 경우, 부정한 방법으로 승인을 받은 때와는 달리 다른 사정 등을 종합적으로 고려하여 승인의 취소 여부가 결정된다.

- 이때 이러한 사유에 해당하기 위해서는 각 심사사항에 해당하는 항목의 상태가 변경되었다는 것만으로는 부족하며, 변경된 상태가 본래 연계정보 생성·처리에 대한 승인을 받기에 부적합한 경우에까지 이르러야 한다. 즉, 제공 서비스 구현의 적절성 및 혁신성(정보통신망법 제23조의5 제2항 제1호) 등 심사사항과 관련된 일부 상태가 변경되었을 뿐 아니라, 이로 인하여 본래 해당 연계정보의 생성·처리가 승인될 수 없는 상태가 되어야 한다.

- 이러한 사유가 발생한 경우, 방송통신위원회는 현재 발생한 상태 변경이 어느 정도 수준으로 이용자 보호 등에 부정적 영향을 미치는지 등을 평가하여 승인의 취소 여부를 판단한다.

라. 물리적·기술적·관리적 조치 의무를 위반한 경우

- 연계정보를 생성·처리하는 본인확인기관은 연계정보의 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치를 하여야 한다(정보통신망법 제23조의6 제1항). 본인확인기관의 물리적·기술적·관리적 조치가 전제되어야 본인확인기관으로부터 연계정보를 제공받은 이용기관 역시

연계정보를 안전하게 처리할 수 있으며, 또한 연계정보의 안전한 처리에 대한 감독도 이루어질 수 있다.

- 연계정보의 안전한 처리 의무는 이용자를 보호하기 위하여 특히 준수되어야 한다. 연계정보 생성·처리에 대한 승인 과정에서도 심사사항 중 하나로서 "연계정보 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치 계획"을 두고 있다.

- 정보통신망법 제23조의6 제1항은 연계정보의 생성·처리 과정에서 적용되는 안전성 확보조치 기준을 상세히 규정하고 있다. 구체적으로, 정보통신망법 시행령 제13조 제1항 각 호에는 안전성 확보조치 책임자 지정, 연계정보 생성 소프트웨어에 대한 보안 통제, 연계정보의 위조·변조 방지 조치, 연계정보의 생성·처리 사실 확인자료의 기록 보관이 규정되어 있다.

- 연계정보 생성·처리에 대한 승인을 받는 과정에서 본인확인기관 및 정보통신서비스 제공자는 안전성 확보조치에 대한 계획을 작성하여 제출하여야 하며, 이후 해당 조치를 준수하여야 한다. 이러한 의무를 위반한 경우 승인이 취소됨으로써 이용자 보호를 보장하는 동시에 안전성 확보조치를 위반한 본인확인기관 및 정보통신서비스 제공자에 대하여 제재가 이루어질 수 있다(정보통신망법 제23조의5 제3항 제3호). 방송통신위원회는 승인의 취소 여부를 판단하는 과정에서 위반 행위의 중대성과 경위 등을 고려한다.

마. 개인정보 보호 관련 법령을 중대하게 위반한 경우

- 연계정보의 생성·처리 승인을 받은 자가 ① 개인정보 보호 관련 법령을 위반하고, ② 그 위반사유가 중대한 경우에도 방송통신위원회는 연계정보의 생성·처리 승인을 취소할 수 있다(정보통신망법 제23조의5 제3항 제4호). 본인확인기관 또는 정보통신서비스 제공자가 개인정보를 적법하게 관리하지 못할 경우, 연계정보의 생성·처리 역시 안정적으로 이루어지지 못할 가능성이 높으므로 개인정보 보호 관련 법령의 중대한 위반이 발생한 경우 승인을 취소할 필요가 있다.

- 정보통신망법 제23조의5 제3항 제4호에 규정된 "개인정보 보호 관련 법령"은 "개인정보(개인정보 보호법 제2조 제1호)"의 처리 등을 규제하는 법률을 의미하는 것으로 볼 수 있다. 이러한 취지에서 개인정보 보호법만이 아니라, 넓게는 신용정보의 이용 및 보호에 관한 법률(이하 "신용정보법") 및 위치정보의 보호 및 이용 등에 관한 법률(이하 "위치정보법")까지 포괄할 수 있다.

- 다만, 연계정보의 처리 과정에서 개인정보 보호법 외에 신용정보법 및 위치정보법이 "개인정보 보호 관련 법규"로 적용될 가능성은 낮다. 신용정보법의 경우 "특정 신용정보주체를 식별할 수 있는 정보"를 신용정보로 정의하고 있으나, 신용정보법 제2조 제1호 나목부터 마목까지의 정보[1] 중 특정 정보와 결합되어야 한다는 제한을 두고 있다(신용정보법 제2조 제1호 가목). 연계정보의 경우 개인을 식별할 수 있는 정보로서 신용정보법 제2조 제1호 가목에서 규정된 정보에 해당하지만, 특별한 사정이 없는 한 본인확인기관이나 정보통신서비스 제공자가 해당 정보를 다른 신용정보와 결합하여 처리할 가능성은 낮다. 또한, 연계정보는 위치정보법에서 규율하는 개인위치정보, 즉 특정 개인을 식별할 수 있는 위치정보(물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보; 위치정보법 제2조 제1호)에 해당하지도 않는다(위치정보법 제2조 제2호). 따라서 본인확인기관 및 정보통신서비스 제공자가 연계정보를 처리하는 과정에서 신용정보법 또는 위치정보법의 규율을 받을 가능성은 낮으며, "개인정보 보호법" 위반 문제가 주로 제기될 것이다.

- 정보통신망법 제23조의5 제3항 제4호에 따라 "개인정보 보호 관련 법령"을 중대하게 위반한 경우에도 연계정보 생성·처리에 대한 승인이 취소될 수 있으며, 해당 법령 위반 행위가 본인확인기관 및 정보통신서비스 제공자의 연계정보 처리와 관련되어 있다면 연계정보 생성·처리 승인 취소사유에 해당할 가능성은 더 높아질 수 있다.

- 이때 "위반사유가 중대한 경우"에 해당하는지와 관련하여 ① 해당 위반행위와 관련된 개인정보의 규모(정보주체의 수 등), ② 해당 위반행위에 대한 개인정보 보호 관련 법령상 제재의 수준 등이 기준이 된다. 또한, 개인정보 보호 관련 법령의 중대한 위반이 있는 경우에도 이를 근거로 승인을 취소할지에 대해서는 해당 위반행위와 연계정보 관리의 관계 등이 고려된다.

---

1) 신용정보주체의 거래내용을 판단할 수 있는 정보, 신용정보주체의 신용도를 판단할 수 있는 정보, 신용정보주체의 신용거래능력을 판단할 수 있는 정보, 그 밖에 신용정보주체의 신용을 판단할 때 필요한 정보

V 연계정보의 목적 범위 내 처리

1. 정보통신망법 제23조의5 제4항

정보통신망법

제23조의5(연계정보의 생성·처리 등) ④ 제1항 각 호에 따른 서비스를 위하여 본인확인기관으로부터 연계정보를 제공받은 자(이하 "연계정보 이용기관"이라 한다)는 제공받은 목적 범위에서 연계정보를 처리할 수 있다. 다만, 정보주체에게 별도로 동의받은 경우에는 동의받은 목적 범위에서 연계정보를 처리할 수 있다.

가. 규정 취지

- 「정보통신망법」 제23조의5 제4항에 따르면 본인확인기관으로부터 연계정보를 제공받은 자는 제공받은 목적 범위에서 연계정보를 처리할 수 있다. 이는 주민등록번호와 일대일 대응되는 연계정보가 무분별하게 이용되거나 제3자에게 제공되는 것을 방지하기 위함이다. 다만, 연계정보 이용기관은 정보주체에게 별도로 동의를 받은 경우에는 동의받은 목적 범위에서 연계정보를 처리할 수 있다.

- 정보통신망법은 연계정보의 생성·처리에 관하여 규율하는 법률로, 연계정보의 안전한 활용을 유도하기 위하여 정보통신망법에 연계정보의 목적 외 이용 제한 등의 규정을 둘 필요성이 인정된다. 이와 유사하게 「위치정보의 보호 및 이용 등에 관한 법률」 제21조는 위치정보 사업자가 이용약관에 명시 또는 고지한 범위를 넘어 위치정보를 이용하거나 제3자에게 제공하면 안 된다고 규정하면서도 예외 사유로 개인위치정보주체의 동의가 있을 경우를 두고 있다.

위치정보의 보호 및 이용 등에 관한 법률

제21조(개인위치정보 등의 이용·제공의 제한 등) 위치정보사업자등은 개인위치정보주체의 동의가 있거나 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인위치정보 또는 위치정보 수집·이용·제공사실 확인자료를 제18조제1항 및 제19조제1항·제2항에 의하여 이용약관에 명시 또는 고지한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니된다.

1. 위치정보 및 위치기반서비스 등의 제공에 따른 요금정산을 위하여 위치정보 수집·이용·제공사실 확인자료가 필요한 경우
2. 통계작성, 학술연구 또는 시장조사를 위하여 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우

2. 제공 또는 동의 받은 목적 범위 내에서 처리

- 연계정보 이용기관은 연계정보를 제공받은 목적 범위 내에서 처리할 수 있고, 정보주체로부터 동의를 받은 경우에도 그 동의받은 목적 범위 내에서 처리할 수 있다(정보통신망법 제23조의5 제4항). 처리 행위가 목적 범위 내에 해당하는지 여부는 그 행위로 정보통신서비스 이용자의 개인정보자기결정권이 침해되어 개인정보가 보호되지 않는 결과가 초래되는지, 그 행위로 인하여 정보통신서비스 이용자에게 불이익이 발생하는지 등의 사정을 종합하여 판단하여야 한다.

판례 동의받은 목적 외 이용에 해당하는지 여부

헌법상 기본권인 개인정보자기결정권의 보장, 정보통신망법의 입법목적 등을 고려하면, 피고인 회사와 같은 정보통신서비스 제공자가 정보통신서비스 이용자의 개인정보를 이용하는 행위가 수집 당시 동의받은 목적 외 이용에 해당하는지 여부는 그 행위로 정보통신서비스 이용자의 개인정보자기결정권이 침해되어 개인정보가 보호되지 않는 결과가 초래되는지, 그 행위로 인하여 정보통신서비스 이용자에게 불이익이 발생하는지 등의 사정을 종합하여 판단하여야 한다.(대구고등법원 2016. 6. 23. 선고 2015노551 판결)

- 주민등록번호와 일대일 대응되는 연계정보를 무분별하게 처리하는 경우 이용자의 개인정보자기결정권이 중대하게 침해될 것이므로 연계정보 이용기관은 제공 및 동의 받은 목적의 범위를 더욱 엄격하게 해석하여 연계정보를 목적 범위 외에 처리하지 않도록 유의하여야 할 것이다.

- 한편, 정보통신망법 제23조의5 제1항에서 오로지 본인확인기관만이 본인확인업무를 수행할 수 있도록 규정하고 있고, 이를 위반할 경우 정보통신망법 제76조 제3항 제2호의2에 따라 본인확인

기관의 지정을 받지 아니하고 본인확인업무를 한 자에 대하여 1천만 원 이하의 과태료를 부과하고 있으므로, 설령 정보주체로부터 동의를 받은 경우라도 연계정보 이용기관이 본인확인 기관처럼 연계정보를 제공하는 등의 방식으로 실질적으로 본인확인업무를 수행하여서는 안 된다.
예컨대, 개인정보 보호법상 개인정보관리 전문기관이나 가명정보 결합 전문기관의 경우에도 개인정보 또는 가명정보의 처리 자체는 정보주체의 동의나 법령에 따라 가능하더라도 해당 전문기관으로서의 기능을 수행하기 위해서는 별도의 지정이나 인허가가 요구된다는 점에서, 연계정보 제공이 본인확인기관의 고유 기능과 결부되는 경우에는 본인확인기관만이 수행할 수 있는 본인확인업무에 해당하는지에 대한 면밀한 검토가 필요할 것이다.

3. 동의를 받는 방법

- 정보주체로부터 동의를 받으면 연계정보를 처리할 수 있으나 개정법은 아직 이러한 동의를 받는 방법에 대하여는 구체적으로 정하고 있지 않았다. 다만, 관계 법령인 개인정보 보호법 및 그 시행령에서 정보주체로부터 동의를 받는 방법에 대하여 정하고 있으므로 처리에 필요한 동의를 받는 방법에 관하여 개인정보 보호법을 참고할 필요가 있다.

- 개인정보 보호법 시행령 제17조 제1항에 따라 개인정보처리자는 정보주체의 동의를 받을 때 ① 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것, ② 동의를 받으려는 내용이 구체적이고 명확할 것, ③ 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것, ④ 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것이라는 요건을 모두 충족하여야 한다. 또한, 동조 제2항에 따라 개인정보처리자는 전화·우편·팩스 등의 방법을 통하여 정보주체로부터 동의를 받아야 한다.

- 특히 신설된 개인정보 보호법 시행령 제17조 제1항 제1호에서 정하는 바와 같이 동의를 받을 때에는 정보주체의 자유로운 의사에 따르도록 하는 것이 중요하다. 개인정보보호위원회는 개인정보처리자가 동의를 요청하는 과정에서 동의를 거부할 경우 서비스 계약체결 자체를 거부하는 등의 방법으로 동의를 강제하여서는 안 된다고 보고 있다.

- 연계정보의 중요성 및 개인정보자기결정권 침해 위험 등을 고려하면 연계정보 이용기관이 연계정보를 제공받은 목적 이외의 범위에서 연계정보를 처리하고자 할 때에는 정보주체의 “자유로운 의사에 반하지 않는” 방식으로 동의를 받아야 할 것이다.

Q) 동의를 받을 때에는 정보주체의 자유로운 의사에 따르도록 하였는데, 앞으로는 개인정보를 수집하는 과정에서 필수적으로 동의를 요구해서는 안 되는 것인지?

A) 동의를 받을 때에는 정보주체의 자유로운 의사에 따라 동의 여부를 결정할 수 있도록 하여야 함. 따라서, 정보주체에게 동의를 요청하는 과정에서 동의를 거부할 경우 서비스 계약체결 자체를 거부하는 등의 방법으로 동의를 강제하여서는 안 됨. 시행령 제17조제1항의 해당 규정은 2024년 9월 15일부터 시행 예정이므로 정보주체의 자유로운 의사가 반영되도록 동의 절차를 개편하는 준비를 진행하여야 함

[출처] 개인정보보호위원회, 개인정보 보호법 및 시행령 개정사항 안내, 2023, 제11면

4. 벌칙 규정

위반 행위	벌칙	조문
정보통신망법 제23조의5제4항에 따른 목적 범위를 넘어서 연계정보를 처리한 자	5년 이하의 징역 또는 5천만 원 이하의 벌금	제71조 제1항 제10호

VI 연계정보 실태 점검

1. 정보통신망법 제23조의6 제3항

정보통신망법

제23조의6(연계정보의 안전조치 의무 등) ③ 방송통신위원회는 생성·처리하는 연계정보의 규모, 매출액 등이 대통령령으로 정하는 기준에 해당하는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치에 대한 운영·관리 실태를 점검할 수 있다.

가. 규정 취지

- 방송통신위원회는 연계정보의 생성·처리와 관련하여 본인확인기관이 방송통신위원회로부터 승인을 받은 후 승인 시 본인확인기관이 행한 조치가 지속적으로 유지되고 있는지를 확인하여야 한다.

- 또한, 정보통신망법 제23조의6제3항에 따라 방송통신위원회는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치에 대한 운영·관리를 적절히 취하고 있는지를 공무원이 점검하도록 하여 연계정보 유출 및 오·남용을 사전에 방지하기 위한 제도적 장치를 마련하고 있다.

2. 연계정보의 운영·관리 실태 점검

가. 본인확인기관의 물리적·기술적·관리적 조치 의무 및 연계정보 이용기관의 안전조치 의무

- 정보통신망법은 연계정보 생성·처리의 안전성 확보를 위하여 본인확인기관에 물리적·기술적·관리적 조치 의무를 부여하고 있고, 연계정보가 분실·도난·유출·위조·변조·훼손되지 않도록 연계정보 이용기관에 안전조치 의무를 부여하고 있다.

- 한편, 같은 법 시행령 제13조(본인확인기관의 물리적·기술적·관리적 보호조치 등)에 본인확인기관 및 연계정보 이용기관이 준수하여야 할 물리적·기술적·관리적 조치와 안전조치 등 세부 기준을 마련함으로써 이를 구체화하고 있다.

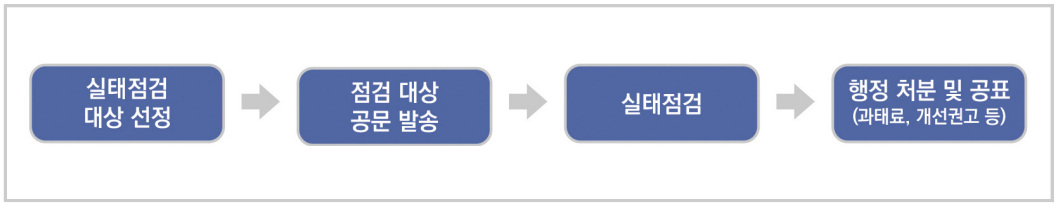
- 본인확인기관이 준수하여야 할 물리적·기술적·관리적 조치와 연계정보 이용기관의 안전조치는 부록에서 상세히 살펴본다.

나. 실태 점검 절차

- 본인확인기관의 물리적·기술적·관리적 조치의 내용과 연계정보 이용기관의 안전조치 실태를 점검하는 공무원은 ① 점검의 근거 및 목적, ② 점검 일시, ③ 점검자의 인적사항, ④ 점검 내용을 점검 7일 전까지 본인확인기관에 통보하여야 한다.

- 다만, 연계정보의 침해 사고 등이 발생하거나 연계정보의 침해에 대한 구체적인 민원이 제기되어 긴급히 점검할 필요가 있는 경우에는 통보하지 않을 수 있다.

[실태점검 절차]



다. 자료제출 요구

- 방송통신위원회는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치를 이행을 확인할 수 있는 업무상황, 물품·서류, 시설·장비 등에 대한 자료의 제출을 요구할 수 있다.

라. 사업장 등의 출입 및 검사

- 방송통신위원회는 본인확인기관 및 연계정보 이용기관이 실태점검에 응하지 않거나 위법사실이 있다고 인정되는 경우 점검 공무원으로 하여금 기관에 출입하여 업무상황, 물품·서류, 시설·장비 등을 검사할 수 있다.

- 이 경우, 점검하는 소속 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.

부 록

[별표 3] 본인확인기관의 물리적·기술적·관리적 보호조치

연계정보의 생성·처리 등에 관한 기준(방송통신위원회고시 제2025-4호)

[별표 3] 본인확인기관의 물리적·기술적·관리적 보호조치

1. 연계정보 생성·처리를 위한 연계정보 내부관리 계획 수립 및 시행에 관한 사항

1-1. 물리적·기술적·관리적 조치를 총괄하는 책임자, 실무자 지정 등 연계정보 관리를 위한 조직의 구성·운영에 관한 사항

1-2. 연계정보 담당 인원의 교육에 관한 사항

1-3. 연계정보 담당 인원 식별 및 최소화 준수

1-4. 연계정보 생성·처리·제공 등을 위한 정보시스템에 대하여 연 1회 이상 취약점 점검 및 조치 활동

2. 연계정보 생성 소프트웨어에 대한 보안 통제에 관한 사항

2-1. 연계정보 생성 소프트웨어 및 모듈에 대한 보안 정책 적용

가. 연계정보를 생성하는 소프트웨어 및 모듈에 대하여 정보시스템과 인원에 대한 접근통제 적용

나. 오프라인을 통한 연계정보 생성 시 연계정보를 생성할 수 있는 소프트웨어 및 모듈이 저장된 이동형 저장장치에 대한 보안 통제 수행

3. 연계정보의 위조·변조 방지 조치에 관한 사항

3-1. 연계정보 생성 및 제공 시 무결성 검증 수행

가. 연계정보에 대한 위·변조 여부를 검증할 수 있는 해시 체인 구성

4. 연계정보 생성·처리 사실 확인자료의 기록·보관에 대한 조치 사항

4-1. 연계정보 생성·제공 관련 사실 확인자료의 저장 및 백업 시스템 운영

가. 연계정보 생성과 관련된 기록은 최소 3년간 로그 형태로 보관

나. 연계정보 생성 및 제공 사실 확인 요청 시 이를 처리할 담당부서와 업무절차 수립

다. 연계정보 생성·제공·이용·파기 항목 등을 개인정보 처리방침에 공개하여 쉽게 확인할 수 있어야 함

Ⅰ 본인확인기관의 물리적·기술적·관리적 보호조치 세부 항목 설명

1. 연계정보 생성·처리를 위한 연계정보 내부관리계획 수립 및 시행에 관한 사항

1-1 물리적·기술적·관리적 조치를 총괄하는 책임자, 실무자 지정 등 연계정보 관리를 위한 조직의 구성·운영에 관한 사항

- 개인정보 보호법 준수를 위한 전사적 '개인정보 내부관리계획' 항목에 연계정보 관련 개인정보 보호 조직의 구성 및 운영, 물리적·기술적·관리적 조치를 총괄하는 책임자 및 지정에 관한 사항(기존 CISO, CPO 겸임 가능), 물리적·기술적·관리적 조치를 총괄하는 책임자와 연계정보 처리 실무자의 역할 및 책임에 관한 사항 등에 대한 항목이 포함되어야 한다.

- 조직의 규모 및 연계정보 활용도의 업무 특성을 반영하여 개인정보 보호 및 정보보안을 수행할 실무조직 구성과 함께 경영진이 적극적으로 참여하는 정보보호위원회 등의 의사결정 체계를 수립하여야 한다.

  ① 연계정보 등 개인정보 보호 조직의 구성 및 운영에 관한 사항을 마련하여야 한다.

  ② 연계정보 생성·처리 등에 대하여 실무차원에서 공유·조정·검토의 역할을 수행하고, 이미 구성된 정보보호위원회 등에서 주요 사안에 대하여 승인하고 의사결정을 수행하여야 한다.

1-2 연계정보 담당 인원의 교육에 관한 사항

- 연계정보를 담당하는 연계정보취급자는 연계정보 및 개인정보와 관련된 교육을 이수하여야 한다.

- 주민등록번호를 일방향 해시(Hash) 처리한 연계정보를 담당하는 인원에 대하여 암호화 기술 등 직무 전문성을 확보할 수 있는 연간 인식 제고 활동 및 교육훈련을 수립·운영하고 그 결과에 따른 효과성을 평가하여야 한다.

- 개인정보 보호법 등 법적 요구사항에 따라 연 1회 이상 실시되는 개인정보보호 교육 내용이나 직무 전문성을 수행하는 교육 중 암호화 관련 기술 및 연계정보의 보안 등을 포함하여야 하고, 연계정보를 담당하는 개인정보취급자에 대한 해당 교육 시간은 해당 기관이 정한 내부 규정을 준수하여야 한다.

- 연계정보 관련 교육시행에 대한 기록을 작성하고, 교육효과와 적정성을 평가하여 차기 교육 계획에 미비점을 반영하여야 한다.

1-3 연계정보 담당 인원 식별 및 최소화 준수

- 연계정보는 연계정보취급자 중에서도 업무처리를 위한 최소 인원만 담당하고, 연계정보를 담당하는 인원은 현재 기준으로 명확하게 파악하여야 한다.
- 최소권한 원칙에 따라 연계정보 담당자 및 개인정보취급자의 접근권한 매트릭스(권한 분류 체계)를 작성하고, 주기적으로 업데이트를 수행하여야 한다.

[접근권한 매트릭스 작성 예시]

	AA연계서버	BB저장서버	CC처리서버
A담당자	R	R	-
B담당자	-	R	-
C담당자	RW	RW	RW

- 업무상 반드시 필요한 인력에 대해서만 연계정보 취급을 승인하고 다른 부서 이동 및 담당 업무 변경 등 업무 관련성 여부를 주기적으로 검토하여야 한다. 연계정보 접근권한 신청정보에는 신청자, 신청일시, 신청목적, 사용기간 등이 포함되어야 한다.
- 연계정보에 접근하는 개인정보취급자 계정의 등록·이용·삭제 및 접근권한의 생성·변경·삭제 이력을 남기고, 적정성 여부를 주기적으로 검토하여야 한다.
- 연계정보 관련한 접근권한 과다부여, 권한부여 절차 미준수, 권한 오·남용 등 이상행위가 발견된 경우 그에 따른 조치절차를 수립하고 이행하여야 한다.

1-4 연계정보 생성·처리·제공 등을 위한 정보시스템에 대하여 연 1회 이상 취약점 점검 및 조치 활동

- 연계정보를 생성·처리·제공하는 정보시스템에 대하여 하드웨어, 소프트웨어, 소스 코드 등이

취약점에 노출되어 있는지 확인하고, 연 1회 이상 취약점 점검을 수행하고 취약점 발견 시 조치하여야 한다.

- 연 1회 이상 취약점 점검 절차 수립 및 취약점 조치 활동을 수행하여야 한다.

  ① 구체적으로 본인확인기관 정보시스템(서버, DB, 네트워크, 스토리지 등, 클라우드 이용 시 클라우드 시스템 모두 포함), 본인확인서비스 애플리케이션(홈페이지, AOS/IOS APP) 및 프레임워크, 본인확인서비스 관련 소스 코드 등에 대하여 취약점 점검을 수행한다.

  ② 정보보호시스템 및 개인정보보호 솔루션, 네트워크(라우터, 스위치 등) 장비 등에 대해서도 취약점 점검 후 조치활동을 수행하여야 한다.

- 발견된 취약점에 대한 실제 조치 활동 수립 및 보완조치를 수행하여야 한다.

  ① 취약점 확인에 대한 연계정보 보호책임자 보고 및 승인 절차가 마련되어야 한다.

  ② 위험수용 항목 및 조치 지연 시 연계정보 보호책임자 보고 및 위험관리 방안이 수립되어야 한다.

  ※ 취약점 점검 항목 및 평가방식은 '정보통신기반 보호법' 제9조(취약점의 분석·평가)를 적용하거나 금융회사 또는 전자금융업자의 경우 '전자금융감독규정' 제37조의2(전자금융기반시설의 취약점분석·평가주기, 내용 등)를 적용할 수 있다.

- 스크립트 방식의 취약점 점검 이외에 웹 서비스 및 응용 애플리케이션은 모의침투 테스트(모의해킹) 수행 후 발견된 취약점을 조치하여야 한다.

2. 연계정보 생성 소프트웨어에 대한 보안 통제에 관한 사항

2-1 연계정보 생성 소프트웨어 및 모듈에 대한 보안 정책 적용

가. 연계정보를 생성하는 소프트웨어 및 모듈에 대하여 정보시스템과 인원에 대한 접근통제 적용

- 연계정보를 생성하는 소프트웨어 및 모듈에 대하여 정보시스템 접근통제 및 사용자 접근통제를 수행하여야 한다.

- 연계정보를 생성하는 소프트웨어 및 모듈이 저장된 시스템에 접속하기 위해서는 암호화된 채널 적용 및 승인된 IP 주소 등으로 접근통제 정책이 수행되어야 한다.

  ① 연계정보를 정보통신망으로 전송 시에는 웹 서버에 SSL(Secure Socket Layer) 인증서를 설치하여 암호화 송수신하여야 한다.

  ※ TLS 버전은 보안 강화를 위하여 최소 1.2 이상 버전을 사용하여야 한다.

  ② 동일 네트워크 영역 내 서버에 대한 접근통제 조치도 수행하여야 한다.

- 취약점이 있는 서비스 및 프로토콜은 불가피한 사유가 없는 한 사용을 제한하고, IPsecVPN, SFTP, SSH 등과 같은 안전한 프로토콜을 사용하여야 한다.

  ※ 예를 들면 FTP, Telnet, File-Sharing, NETBIOS 프로토콜 등은 특별한 사유가 없는 한 사용을 제한한다.

- 연계정보를 생성하는 소프트웨어 및 모듈에 대하여 사용자의 접근은 안전한 절차와 필요에 따라 강화된 인증수단을 적용하여야 한다.

  ※ 사용자 인증수단은 비밀번호, 인증서(PKI), OTP(One Time Password), 지문·얼굴 등 생체기반 인증수단을 적용한다.

- 연계정보를 생성하는 소프트웨어 및 모듈이 담긴 정보시스템에 접근할 때에는 인증 실패 횟수 제한(클리핑 레벨 설정), 접속 유지시간(Session Timeout 또는 Idle Timeout), 동일 계정으로 동시 접속 차단 등의 보안통제 정책이 수립되어야 한다.

- 등록되지 않은 IP 주소에서의 접속(국외 IP 주소 등), 주말 또는 새벽 시간 접속 시 등에는 불법 로그인 시도 경고에 대한 알람을 설정하여 연계정보를 생성하는 소프트웨어 및 모듈이 담긴 정보시스템에 대하여 로그인 이력 및 이상행위를 주기적으로 관리하여야 한다.

나. 오프라인을 통한 연계정보 생성 시 연계정보를 생성할 수 있는 소프트웨어 및 모듈이 저장된 이동형 저장장치에 대한 보안 통제 수행

- 온라인이 아닌 오프라인에서 주민등록번호를 연계정보로 일괄 변환할 때 연계정보를 생성할 수 있는 소프트웨어 및 모듈이 저장된 이동형 저장장치에 대하여 사용자 이력관리 및 단말기 통제 정책을 수행하여야 한다.

- 모바일 전자고지 및 금융 마이데이터 서비스 등을 위하여 오프라인을 통하여 주민등록번호를 연계정보로 일괄 변환할 때 사용되는 이동형 저장장치에 대하여 별도의 사용자 및 단말기 통제를 수행하여야 한다.
- 또한 승인된 사용자 목록, 저장장치 책임관리자, 연계정보를 생성할 수 있는 소프트웨어 및 모듈이 저장된 이동형 저장장치 개수 및 보관 담당자 등이 명시되어야 한다.
- 본인확인기관은 연계정보를 생성할 수 있는 소프트웨어 및 모듈이 저장된 이동형 저장장치에 대하여 자산 대장 작성 및 보안 스티커를 부착하고, 이동형 저장장치에 대한 패스워드를 설정하여야 한다.
- 이동형 저장장치에는 로그인, 행위 이력 및 주민등록번호 주입과 변환된 연계정보 등이 로그 형태로 저장되어야 한다. 로그에 반드시 표기되어야 하는 항목으로는 로그인 ID 및 일시, 로그인 실패 이력, 최초 입력된 주민등록번호 건수, 오류 주민등록번호 건수, 최종 성공한 연계정보 변환 건수 등이 포함되어야 한다.

3. 연계정보의 위조·변조 방지 조치에 관한 사항

3-1 연계정보 생성 및 제공 시 무결성 검증 수행

가. 연계정보에 대한 위조·변조 여부를 검증할 수 있는 해시 체인 구성

- 본인확인기관은 본인확인서비스 관련 이용자·이용기관으로부터 받은 개인정보를 해시 처리하여 무결성 검증을 위하여 해시 체인을 구성하여야 한다.
- 본인확인서비스를 위하여 연계정보를 생성 및 제공한 이력에 대하여 이를 해시 처리하여 생성 및 제공에 대한 무결성 검증을 입증하는 기능을 마련하여야 한다.
- 해시 처리된 증적자료를 본인확인서비스를 이용한 이용기관별·이용자별로 체인 형태로 정보를 구성하여야 한다.
- 해시 체인 방법 이외에 본인확인기관은 연계정보 생성 및 제공 이력에 대하여 데이터베이스 또는 서버 로그에 본인확인서비스에 이용한 개인정보를 타임스탬프 형식(YYYY_MM_DD보다 초

정보 소수점이 포함된 디테일한 시간정보 등의 데이터 형태)을 통하여 생성과 제공사실이 위조·변조되지 않았음을 증명하는 테이블 또는 레코드를 저장하는 방법도 가능하다.

4. 연계정보 생성·처리 사실 확인자료의 기록·보관에 대한 조치 사항

4-1 연계정보 생성·제공 관련 사실 확인자료의 저장 및 백업 시스템 운영

가. 연계정보 생성과 관련된 기록은 최소 3년간 로그 형태로 보관

- 연계정보를 생성하고 제공한 이력에 대하여 로그 형태로 DB 또는 별도 백업 시스템에 최소 3년간의 자료를 보관하여야 한다.
- 이용자 또는 이용기관의 연계정보 사실확인자료 요청에 응대하기 위하여 본인확인기관은 연계정보 생성 및 제공 이력에 대하여 최소 3년간의 자료를 보관하여야 한다.
- 연계정보 생성 및 제공 관련 로그에는 이용자 및 이용기관 등을 구분할 수 있는 식별자(CPcode 등), 요청한 정보시스템 IP/Port번호, 요청 URL, CallBack_URL 등이 포함되어야 하며, 연계정보를 생성한 시간과 제공한 시간 정보가 반드시 포함되어야 한다.
- 해당 로그는 위조·변조 방지 및 무결성 보장을 위한 보안 통제 또는 보안 매체가 적용되어야 하며, 장애 발생 및 만일의 사태에 대비하기 위하여 별도의 백업 장비에 보관·관리하여야 한다.

나. 연계정보 생성 및 제공 사실 확인 요청 시 이를 처리할 담당부서와 업무절차 수립

- 이용자 또는 이용기관의 연계정보 생성 및 제공과 관련된 불만을 접수·처리할 수 있는 절차를 마련하고 담당자를 지정하여야 한다.
- 본인확인서비스 이용 등 이용자 및 이용기관으로부터 연계정보의 생성·제공 등과 관련한 불만을 접수하고 처리할 수 있는 상담창구를 마련하여야 한다.

  ※ 상담창구(예): 전화, ARS(IVR), 이메일, 게시판 등

- 연계정보 생성 및 제공과 관련하여 이용자의 개인정보 보유기간 경과 시 파기 절차를 마련하여야 하며, 연계정보 보유기간에 대한 해당 법률 및 근거를 반드시 명시하여야 한다.

※ 다른 법령에 따른 최소 보유기간(예시)

전자상거래 등에서 소비자 보호에 관한 법률

1. 표시·광고에 관한 기록: 6개월
2. 계약 또는 청약철회 등에 관한 기록: 5년
3. 대금결제 및 재화 등의 공급에 관한 기록: 5년
4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년

다. 연계정보 생성·제공·이용·파기 항목 등을 개인정보 처리방침에 공개하여 쉽게 확인할 수 있어야 함

- 본인확인기관의 개인정보 처리방침에 연계정보와 관련된 상세 항목을 이용자가 쉽게 확인할 수 있도록 게시하여야 하며, 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 이용자가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공지·공개하여야 한다.
- 개인정보 처리방침은 법령에서 요구하는 내용을 포함하여야 하며, 기존 개인정보 처리방침에 최신 연계정보와 관련된 내용이 누락되지 않도록 주기적으로 현행화하여 공개하여야 한다.
- 개인정보 처리방침의 상세항목 및 게시 방법은 「개인정보 처리방침 작성지침」(개인정보보호위원회, 2024. 4.)과 「개인정보 처리방침 평가에 관한 고시」(제2024-3호, 2024. 2. 20.)를 참조하여 작성 및 게시하여야 한다.

[별표 4] 연계정보 이용기관의 안전조치

연계정보의 생성·처리 등에 관한 기준(방송통신위원회고시 제2025-4호)

[별표 4] 연계정보 이용기관의 안전조치

1. 연계정보의 안전한 처리를 위한 내부 규정의 수립 및 시행에 관한 사항

1-1. 안전조치를 총괄하는 책임자 지정에 관한 사항
1-2. 연계정보의 취급·관리 절차에 관한 사항
1-3. 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항
1-4. 연계정보의 안전한 저장·전송에 관한 사항
1-5. 연계정보의 유출, 도난 방지를 위한 취약점 점검에 관한 사항
1-6. 그 밖에 연계정보 보호를 위하여 필요한 사항

2. 연계정보를 제공받은 목적 범위 내 연계정보 처리에 관한 사항

2-1. 연계정보취급자를 최소한으로 제한
2-2. 연계정보취급자에 대한 정기적인 교육
2-3. 연계정보 처리 실태에 대한 연 1회 이상 정기적인 점검

3. 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항

3-1. 비인가자의 접근 등에 의해 연계정보와 주민등록번호가 함께 유출되지 않도록 물리적 또는 논리적으로 분리하여 보관

4. 연계정보를 안전하게 저장·전송할 수 있는 암호화 기술 적용에 관한 사항

4-1. 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우 안전한 암호 알고리즘으로 암호화
4-2. 10만 명 이상의 이용자 연계정보를 보유한 대기업·중견기업·법 제44조의5제1항제1호에 해당하는 공공기관 등 또는 100만 명 이상의 이용자 연계정보를 보유한 중소기업·단체는 연계정보를 안전한 알고리즘으로 암호화하여 저장

5. 연계정보 분실·도난 등의 침해사고 발생 시 대응 계획의 수립 및 시행에 관한 사항

5-1. 다음 각 목을 포함하는 계획의 수립 및 시행
가. 연계정보 수집 등 연계정보 처리에 관한 사항의 공개
나. 연계정보 침해사고 발생 시 접수 및 절차
다. 연계정보 이용내역 등 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의철회 등 요구 대응 절차

6. 연계정보 제공기관 및 제공 시기 등에 관한 자료의 기록·보관에 관한 사항

6-1. 연계정보 수집의 근거 및 현황을 확인할 수 있도록 다음 사항을 포함하여 기록
가. 수집 출처
나. 수집 시기
다. 수집 목적
라. 수집 대상 등
6-2. 연계정보의 수집 출처, 수집 시기 등에 관한 자료는 최소 1년간 저장·관리

Ⅰ 규정 취지

- 연계정보 이용기관은 연계정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 「개인정보 보호법」 제29조에 따른 조치와 더불어 「정보통신망법」 시행령 제13조제2항, 「연계정보의 생성·처리 등에 관한 기준」 제11조 및 [별표 4]에 따른 연계정보 이용기관의 조치(이하 "안전조치")를 하여야 한다.

- 한편, 정보통신망법 제23조의6 제2항에서 "연계정보 이용기관은 제23조의5 제1항 각 호에 따른 서비스를 제공하는 경우, 안전조치를 하도록" 규정하고 있는바, 제23조의5 제1항 각 호에 해당하는 전자정부 서비스, 마이데이터 서비스, 전자고지 서비스, 금융 마이데이터 서비스를 제외한 나머지 연계정보 이용기관 사업자의 경우에는(예컨대 본인확인기관으로부터 연계정보를 받아서 온·오프라인 회원관리 서비스를 제공하려는 사업자) 안전조치 의무가 적용되지 않는 것인지 혼란이 있을 수 있다.

- 그러나 정보통신망법 제23조의5 제1항은 본인확인기관이 연계정보를 생성 또는 처리가 가능한 경우를 규정하고 있고, 해당 규정의 주어는 본인확인기관이라고 할 것이므로, 정보통신망법 제23조의6 제2항에서 말하는 "제23조의5제1항 각 호 중 제1호에 따른 서비스"는 "(본인확인기관이) 본인확인서비스를 제공함에 따라 본인확인기관으로부터 연계정보를 받고 이를 이용하여 다양한 서비스를 제공하는 경우"를 의미하기 때문에 본인확인기관으로부터 연계정보를 제공받고 이를 이용하는 사업자라고 한다면 "정보통신망법 제23조의5제1항 각 호에 '따른' 서비스를 제공하는 경우"에 해당하는 것으로 해석하며, 따라서 안전조치 의무가 있다.

Ⅱ 연계정보 이용기관의 안전조치 세부 항목 설명

1. 연계정보의 안전한 처리를 위한 내부 규정의 수립 및 시행에 관한 사항

- 연계정보 이용기관은 연계정보를 수집·저장·이용·제공 등의 처리를 할 때 연계정보가 분실·도난·유출·위조·변조·훼손되지 않도록 연계정보의 안전조치에 관한 내부 규정을 수립·시행하여야 한다. 내부 규정에는 다음 사항을 필수적으로 포함하여야 하며, 각 사항을 실질적으로 이행할 수 있도록 세부적인 내용을 구체적으로 수립하여야 한다.

- 내부 규정은 경영진으로부터 내부 결재 등의 공식적인 승인 절차를 통하여 시행하여야 하며, 전 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

1-1 안전조치를 총괄하는 책임자 지정에 관한 사항

- 연계정보의 안전조치에 관한 사항을 결정하고 이를 적용·관리하는 책임을 지는 자(이하 “연계정보 안전조치 책임자”)를 공식적으로 지정하여야 한다.
- 연계정보 안전조치 책임자는 연계정보 및 개인정보 보호 관련 법·제도, 기술 등에 대한 지식과 경험을 보유한 자로 지정할 필요가 있다.
- 연계정보 안전조치 책임자는 연계정보의 안전조치에 대한 실질적 권한을 가지고 있어야 하며, 조직 내에서 연계정보 안전조치에 관하여 어느 정도 독자적인 의사결정을 할 수 있는 지위에 있는 자로 지정할 필요가 있다.

1-2 연계정보의 취급·관리 절차에 관한 사항

- 연계정보의 수집·저장·이용·제공·위탁·파기 등 연계정보 처리단계별 취급 및 관리 절차를 마련하여야 한다.
- 특히, 연계정보가 정보통신망법, 개인정보 보호법 등 관계 법령에 따라 적법하고 안전하게 처리될 수 있도록 연계정보를 취급하는 직원(이하 “연계정보취급자”)이 준수하여야 할 연계정보 취급 절차를 구체화하여야 한다.
- 연계정보 취급 절차에는 연계정보취급자의 의무 및 책임, 연계정보취급자의 직무상 비밀유지 의무, 계정 및 접근권한 관리, 문서 관리, 보안설정 관리 등이 포함될 수 있다.

1-3 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항

- 연계정보와 주민등록번호의 분리·보관 조치와 관련하여 「연계정보의 생성·처리 등에 관한 기준」 [별표 4] 제3호에 따른 사항을 포함하여야 한다.

- 이를 위한 세부 사항으로 연계정보와 주민등록번호의 분리보관 조치 기준, 대상, 방법, 접근권한 관리 절차 등에 관한 사항이 포함될 수 있다.

1-4 연계정보의 안전한 저장·전송에 관한 사항

- 연계정보의 안전한 저장·전송과 관련하여 「연계정보의 생성·처리 등에 관한 기준」 [별표 4] 제4호에 따른 사항을 포함하여야 한다.
- 이를 위한 세부 사항으로 정보통신망을 통하여 인터넷망으로 연계정보 송수신 시 암호화 및 연계정보 저장 시 암호화를 위한 기준, 대상, 방법과 안전한 암호 알고리즘 사용에 관한 기준 등이 포함될 수 있다.

1-5 연계정보의 유출, 도난 방지를 위한 취약점 점검에 관한 사항

- 연계정보가 유출·도난 등이 되지 않도록 연계정보를 처리하는 시스템이나 응용프로그램 등에 대하여 취약점 점검을 정기적으로 수행하고, 발견된 취약점에 대하여 개선조치를 하여야 한다.
- 취약점 점검은 자체적으로 수행하거나 전문업체 등을 활용할 수 있으며, 점검 도구로는 상용도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있다.
- 취약점 점검 및 조치가 체계적으로 수행될 수 있도록 취약점 점검 대상, 시기, 방법, 항목, 담당자, 보고 절차 등을 포함한 취약점 점검 절차를 마련할 필요가 있다.

1-6 그 밖에 연계정보 보호를 위하여 필요한 사항

- 연계정보의 보유량, 연계정보를 처리하는 방법 및 환경, 연계정보 침해 위험 등을 고려하여 연계정보의 보호를 위하여 필요한 사항을 추가로 포함할 수 있다
- 예를 들면 연계정보 처리 관련 위험평가의 수행, 연계정보 보호조치 이행 실태 점검, 연계정보 접속기록 모니터링, 내부 규정 위반 시 제재 조치 등에 관한 사항이 이에 해당될 수 있다.

2. 연계정보를 제공받은 목적 범위 내 연계정보 처리에 관한 사항

2-1 연계정보취급자를 최소한으로 제한

- 연계정보를 조회, 열람, 파기 등 처리할 수 있는 연계정보취급자의 범위를 업무상 필요한 최소한으로 제한하여야 한다.
- 연계정보취급자 지정 시 업무상 필요성 및 적절성에 대한 검토 및 책임자 승인 절차를 수립·이행하여야 한다.
- 또한, 연계정보처리시스템의 접근권한을 업무 수행에 필요한 최소한의 범위로 연계정보취급자에게 차등 부여하고, 연계정보취급자 또는 연계정보취급자의 업무가 변경된 경우 연계정보처리시스템의 접근권한을 지체 없이 변경 또는 말소하여야 한다.

2-2 연계정보취급자에 대한 정기적인 교육

- 연계정보취급자가 내부 규정 등에 따라 연계정보를 안전하게 처리할 수 있도록 연계정보취급자에 대하여 정기적으로 교육하여야 한다.
- 교육 시행 주기는 연 1회 이상으로 하되, 연계정보취급자의 업무 내용 및 유형에 따라 교육 내용, 방법, 시간, 시행 주기 등을 차등화할 수 있다.
- 교육 내용에는 연계정보 내부 규정 등 연계정보의 안전한 처리를 위하여 연계정보취급자가 필수적으로 준수하여야 할 사항을 포함할 필요가 있다.

연계정보취급자 교육 내용 예시

- 연계정보 보호의 중요성
- 연계정보 내부 규정에 관한 사항
- 연계정보 취급 절차
- 연계정보취급자의 의무 및 책임
- 연계정보 안전조치 사항
- 연계정보 침해사고 대응 절차
- 연계정보 처리 관련 준수사항 및 금지사항 등

2-3 연계정보 처리 실태에 대한 연 1회 이상 정기적인 점검

- 연계정보 안전조치 책임자는 연계정보가 내부 규정에 따라 안전하게 처리되고 있는지에 대하여 연 1회 이상 정기적으로 실태점검을 수행하여야 한다.
- 연계정보 처리 실태를 점검하기 위한 계획을 수립할 때에는 점검 시기, 대상, 조직 및 인력, 항목 및 방법 등을 포함할 필요가 있다.
- 실태점검 결과 문제점이 발견된 경우 개선조치를 하여야 한다.

3. 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항

3-1 비인가자의 접근 등에 의하여 연계정보와 주민등록번호가 함께 유출되지 않도록 물리적 또는 논리적으로 분리하여 보관

- 비인가자의 접근, 취급자의 실수 등에 의하여 연계정보와 주민등록번호가 함께 유출되지 않도록 연계정보와 주민등록번호는 물리적 또는 논리적으로 분리하여 보관하여야 한다.
- 정보시스템의 서버 및 DBMS를 분리하는 물리적인 방식 외에 DBMS의 인스턴스 단위 또는 테이블 단위 분리 등 논리적인 방식으로 분리하는 것이 가능하다.
- 특히 논리적으로 분리하는 경우 연계정보와 주민등록번호에 대한 접근권한을 명확히 구분하고, 업무 필요성에 따라 접근권한을 최소화하여 부여하는 등 접근권한을 엄격하게 관리하여야 한다.

〈표〉 연계정보 및 주민등록번호 분리 보관 방식 예시

No.	DB 분리 방식	설명
1	물리 서버 (하드웨어) 분리	- 하드웨어에서부터 OS, DBMS, 데이터 단위까지 분리됨 - 분리된 DB 간 상호 영향 최소화 가능 - 계정 및 접근권한 분리 용이
2	가상서버(VM*) 분리	- 하드웨어 및 가상화 엔진(하이퍼바이저 등)은 공유하지만 게스트 OS부터 DBMS, 데이터 단위까지 분리됨 - 게스트 OS, DBMS, 데이터 단위에 대해서는 계정 및 접근권한 분리, 상호 영향 최소화 등 독립적 운영 가능 * VM : Virtual Machine

No.	DB 분리 방식	설명
3	DB 인스턴스 분리	- 동일 서버의 DBMS에서 인스턴스를 분리하여 운영하는 방식 - DB 인스턴스 단위로 접근권한 분리 가능 - 하드웨어, OS, DBMS 엔진은 공유하므로 해당 영역에서의 취약점, 침해 등에는 동일하게 영향을 받음
4	DB 스키마 분리	- 동일한 DB 인스턴스 내에서 논리적인 스키마를 분리하는 방식 - 하드웨어, OS, DBMS 엔진, DB 인스턴스는 공유하므로 해당 영역에서의 취약점, 침해 등에는 동일하게 영향을 받음
5	DB 테이블 분리	- 동일한 DB 인스턴스 및 스키마 내에서 테이블 단위로 분리하는 방식 - 하드웨어, OS, DBMS 엔진, DB 인스턴스 및 스키마를 공유하므로 해당 영역에서의 취약점, 침해 등에는 동일하게 영향을 받음 - 테이블 단위로 접근권한를 분리하고 접근제어 및 모니터링을 강화하는 등 엄격한 접근통제 필요

4. 연계정보를 안전하게 저장·전송할 수 있는 암호화 기술 적용에 관한 사항

4-1 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송수신하는 경우 안전한 암호 알고리즘으로 암호화

- 연계정보 이용기관은 연계정보를 웹, API 등 정보통신망을 통하여 인터넷망 구간으로 송수신하는 경우 안전한 암호 알고리즘으로 암호화하여야 한다.
- 암호화 방법에는 SSL/TLS, 응용프로그램 방식 암호화, VPN 등이 있다.
- SSL/TLS 방식으로 암호화하는 경우 SSL v3 및 TLS 1.0 등 취약한 프로토콜은 사용하지 않도록 주의할 필요가 있다.

4-2 10만 명 이상의 이용자 연계정보를 보유한 대기업·중견기업·법 제44조의5 제1항제1호에 해당하는 공공기관 등 또는 100만 명 이상의 이용자 연계정보를 보유한 중소기업·단체는 연계정보를 안전한 알고리즘으로 암호화하여 저장

- 10만 명 이상의 이용자 연계정보를 보유한 대기업·중견기업·법 제44조의5 제1항 제1호에 해당하는 공공기관 등 또는 100만 명 이상의 이용자 연계정보를 보유한 중소기업·단체는 연계정보를 안전한 알고리즘으로 암호화하여 저장하여야 한다.

〈표〉 연계정보 저장 시 암호화 의무 대상자

No.	이용자 연계정보 보유 수	암호화 의무 대상자
1	10만 명 이상의 이용자 연계정보 보유 시	대기업
2		중견기업
3		공공기관 등(국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제5조제3항에 따른 공기업·준정부기관 및 「지방공기업법」에 따른 지방공사·지방공단)
4	100만 명 이상의 이용자 연계정보 보유 시	중소기업
5		단체

- 연계정보 저장 시 암호화를 위하여 상용 암호화 솔루션 적용, 암호화 라이브러리 활용, 클라우드 서비스제공자가 제공하는 암호화 기능 이용 등 다양한 방법을 활용할 수 있다.
- 연계정보를 암호화하는 경우에는 안전한 암호 알고리즘을 사용하여야 한다. 특히 DES, MD5, SHA-1 등 취약한 암호 알고리즘은 사용하지 않도록 주의하여야 한다.
- 또한 처리 속도 등 기술 발전, 시간 경과 등에 따라 안전한 암호 알고리즘은 달라질 수 있으므로 국내외 암호 관련 연구기관이 제시하는 최신 정보의 확인이 필요하다.
- 국내외 암호 연구 관련 기관은 한국인터넷진흥원의 암호이용 활성화 홈페이지(https://seed.kisa.or.kr)의 "암호 표준화 및 유관기관"에서도 확인할 수 있다.

〈표〉 안전한 암호 알고리즘 예시[2](2018년 12월 기준)

구분	공공기관	민간부문
대칭키 암호 알고리즘	SEED, LEA, HIGHT, ARIA	SEED, HIGHT, ARIA-128/192/256, AES-128/192/256 등
공개키 암호 알고리즘 (메시지 암·복호화)	RSAES-OAEP	RSA, RSAES-OAEP 등
일방향 암호 알고리즘	SHA-224/256/384/512	SHA-224/256/384/512 등

※ 연계정보 저장 시 암호화 규정은 예산 확보, 준비 기간 등을 고려하여 2027년 5월 1일부터 시행됨

2) 출처 : 개인정보 암호화 조치 안내서(2020. 12., 개인정보보호위원회)

5. 연계정보 분실·도난 등 침해사고 발생 시 대응 계획 수립 및 시행에 관한 사항

5-1 다음 각 목을 포함하는 계획의 수립 및 시행

- 연계정보 이용기관은 다음 각 목의 사항을 포함하는 연계정보 침해사고 발생 시 대응 계획을 수립하여 시행하여야 한다.

가. 연계정보 수집 등 연계정보 처리에 관한 사항의 공개

- 연계정보 이용기관은 이용자가 연계정보 처리 여부 및 현황을 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 연계정보 처리에 관한 사항을 공개하여야 한다.
- 연계정보를 수집·이용하는 경우에는 연계정보 처리 근거, 연계정보의 수집·이용 목적, 연계정보 보유 및 이용 기간 등에 관한 사항을 공개하여야 한다.
- 연계정보를 제3자에게 제공하는 경우에는 연계정보를 제공받는 자의 명칭, 연계정보를 제공받는 자의 연계정보 이용 목적, 연계정보를 제공받는 자의 연계정보 보유 및 이용기간 등에 관한 사항을 공개하여야 한다.

나. 연계정보 침해사고 발생 시 접수 및 절차

- 연계정보 이용기관은 연계정보의 처리 관련 이용자의 권리 침해, 연계정보의 분실·도난·유출·위조·변조·훼손 등 침해사고 발생 시 신속한 대응 및 이용자 불만 등을 접수·처리할 수 있도록 연계정보 침해사고 대응 계획을 마련하여야 한다.
- 연계정보 침해사고 대응 계획에는 침해사고 유형, 침해사고 보고 체계, 침해사고 대응 조직 구성 및 운영, 침해사고 유형 및 단계별 대응 절차, 이용자 불만 등에 대한 접수 창구 운영에 관한 사항, 이용자 불만 등 접수·처리 절차 등을 포함하여야 한다.

다. 연계정보 이용내역 등 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의철회 등 요구 대응 절차

- 이용자는 언제든지 본인의 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의철회

등(이하 “열람등요구”)을 요구할 수 있다.

- 연계정보 이용기관은 이용자가 열람등요구를 할 수 있는 구체적인 방법과 절차를 해당 연계정보의 수집 방법과 절차보다 어렵지 않도록 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

6. 연계정보 제공기관 및 제공 시기 등에 관한 사항

6-1 연계정보 수집의 근거 및 현황을 확인할 수 있도록 다음 사항을 포함하여 기록

- 연계정보 이용기관은 연계정보를 제공받은 근거 및 현황을 확인할 수 있도록 다음 사항을 포함하여 기록하여야 한다.

〈표〉 연계정보 관련 자료에 포함하여야 할 사항

항목	설명	예시
수집 출처	- 연계정보를 제공한 기관의 명칭	OO평가정보, OO통신사 등
수집 시기	- 연계정보를 제공받은 일시	2024-07-30 17:05 등
수집 목적	- 연계정보를 제공받은 목적	회원 가입 시 본인확인, 전자고지 서비스 제공을 위한 연계정보 변환 등
수집 대상 등	- 연계정보를 제공받은 이용자를 확인할 수 있는 정보(다만, 이용자의 주민등록번호, 연계정보를 포함하지 않도록 주의) - 연계정보를 제공받은 방법 등 그 밖의 필요한 사항을 추가로 포함할 수 있음	회원 일련번호, 회원 아이디 등

6-2 연계정보의 수집 출처, 수집 시기 등에 관한 자료는 최소 1년간 저장·관리

- 연계정보 수집 출처 및 수집 시기 등 연계정보 관련 자료는 최소 1년간 저장·관리하여야 한다.
- 연계정보 관련 자료가 변조·훼손되지 않도록 담당자를 지정하고, 정기적인 백업 등 안전하게 보관하여야 한다.

※ 연계정보 제공기관 및 제공 시기 등에 관한 자료의 기록·보관 규정은 예산 확보, 준비 기간 등을 고려하여 2027년 5월 1일부터 시행

연계정보 처리 및
안전조치 등에 관한 안내서

2025년 6월 인쇄
2025년 6월 발행

발 행 처 방송통신위원회
경기도 과천시 관문로 47, 2동
TEL. (02) 500-9000
URL. http://www.kcc.go.kr

한국인터넷진흥원
전라남도 나주시 진흥길 9
TEL. 1433-25
URL. http://www.kisa.or.kr

〈비매품〉