바이오정보 보호 가이드라인(안)

2017. 12.

방송통신위원회

KISA 한국인터넷진흥원

[목 차]

Ⅰ. 개요 ····· 1
1) 목적 ····· 1
2) 보호 필요성 ····· 1

Ⅱ. 적용 범위 ····· 2
1) 대상 정보 ····· 2
2) 대상 사업자 ····· 4
3) 법령과의 관계 ····· 4
4) 재검토 기한 ····· 4

Ⅲ. 바이오정보 보호원칙 ····· 5
1) 비례성 원칙 ····· 5
2) 수집·이용 제한의 원칙 ····· 6
3) 목적제한의 원칙 ····· 10
4) 통제권 보장의 원칙 ····· 11
5) 투명성 원칙 ····· 16
6) 바이오정보 보호 중심설계 및 운영원칙 ····· 18

Ⅳ. 기술적·관리적 보호조치 ····· 20
1) 수집·입력 단계 ····· 22
2) 저장·이용 단계 ····· 24
3) 파기 단계 ····· 26

〈 추진 배경 〉

◇ 과거 기업의 출입통제 시스템에 한정되어 사용되었던 바이오정보가 최근 스마트폰 잠금해제, AI 음성비서 서비스 등 정보통신분야 전반에서 그 활용도가 증가하고 있음

※ 전 세계 바이오인식시장 매출은 '15년 20억 달러에서 '24년 149억 달러 규모로 연평균 25.3% 성장 전망(Tractica, 2015)

※ 국내 바이오인식 시장 매출은 '14년 1,745억 원에서 '20년 2,709억 원 규모로 연평균 7.61% 성장(KISA, 2015 국내 정보보호산업 실태조사)

◇ 바이오정보는 모든 사람에 고유하고 시간이 지나도 쉽게 변하지 않으며 패스워드, OTP카드 등과 달리 별도로 기억하거나, 소지할 필요가 없어 편리성이 높지만, 한 번 유출될 경우 변경이 어려워 지속적으로 정보가 악용될 수 있음

최근, 실제로 바이오정보가 유출되거나 위·변조되는 사례가 발생하여 국민의 우려가 높아지고 있는 상황임

(사례1) 미국 연방 인사관리처(OPM)의 DB가 해킹되어 미국 전·현직 공무원의 지문정보 약 560만 건이 유출('15.6)

(사례2) 위조 실리콘 지문 캡처된 얼굴·홍채사진 등을 이용하여 스마트폰 잠금 해제를 시연

◇ 이에 EU 등 주요 국가들은 개인정보의 한 유형으로 '바이오정보(Biometric Data)'를 구체적으로 정의하고, 바이오정보를 보호하기 위한 보호원칙 등을 담은 가이드라인을 제시

◇ 본 가이드라인은 이러한 흐름에 발맞춰 정보통신망법 시행령과 고시에서 정의하고 있는 바이오정보의 개념을 명확히 해석하여 제시하고, 바이오정보의 보호와 안전한 활용을 위해 필요한 규범적·기술적 보호조치를 안내하고자 함

Ⅰ. 개요

□ **(목적)** 기술발전과 함께 스마트폰 잠금해제, AI 음성비서 서비스 등 바이오정보의 활용이 증가함에 따라, 바이오정보의 보호와 안전한 활용을 위한 원칙 및 조치 사항 안내를 목적으로 함

o 현행 개인정보보호 법령 및 고시에 따라 바이오정보는 개인정보로서 보호되고 있으나, 암호화 저장 이외에는 명시적인 규정이 부재

- 이에, 바이오정보 보호 원칙 및 처리단계별 보호조치를 제시함으로써 바이오정보 보호 방안 마련

□ **(보호 필요성)** 바이오정보는 다른 인증수단과 달리 별도로 기억하거나 휴대가 필요없어 편리성이 높지만, 인증 및 식별 목적의 특성 상 손쉽게 신원확인이 될 수 있어 보호의 필요성이 큼

o 바이오정보는 ① 신원확인 용도로 널리 쓰이고 있어 그 **자체로 개인을 식별**하는 데 사용 가능하고, ② 비밀번호 대용이면서도 일반 비밀번호와 달리 유출 시, **변경이 어려움**. ③ 또한, 일부 바이오정보의 경우 인종·병력 등 **부가적인 정보가 추출**될 수 있으며, ④ 얼굴·지문 등 **이용자의 동의없이 수집**하기가 용이한 경우도 존재하여 위·변조에 악용될 수 있음

o 위와 같은 바이오정보의 특성을 고려한 **보호원칙 및 조치사항 안내가 필요**

※ 인증이나 식별 목적으로 활용되지 않는 경우(예: 이용자가 스마트폰으로 찍은 얼굴사진 위에 스티커 효과 처리)와 보호수준 차등화

Ⅱ. 적용 범위

□ **(대상 정보) 정보통신망법상 바이오정보**(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보)

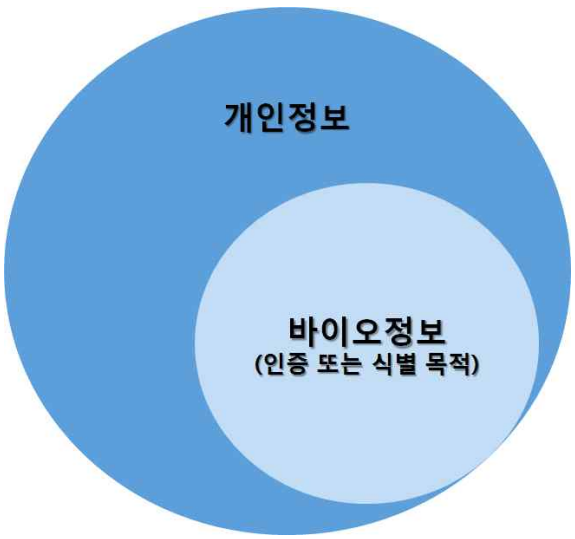
⇒ 바이오정보는 지문, 홍채, 음성, 필적 등 개인의 신체적·행동적 특성에 관한 정보로서 **개인을 인증 또는 식별하기 위하여 기술적으로 처리***되는 개인정보를 말한다.

* '기술적 처리'란 센서 입력장치 등을 통해 이미지 등 원본 정보를 수집·입력하고 해당 원본 정보로부터 특징점을 추출하는 등 개인을 인증 또는 식별하기 위해 전자적으로 처리되는 전 과정을 말함

※ 따라서, 바이오정보는 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력된 '원본정보'와 그로부터 특징 값을 추출하여 생성된 '특징정보'로 구분됨

☞ 사진이나 음성정보 등은 특정 개인을 식별 또는 인증하기 위하여 기술적으로 처리되는 경우에 한해서만 바이오정보에 해당

< 개인정보 및 바이오정보의 관계 >



※ 바이오정보 외 그 자체만으로 특정한 개인을 알아볼 수 있거나(사진, 영상 등) 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 일반 개인정보로서 취급됨

< 바이오정보 활용 유형 및 사례 >

유 형	사 례
인증 (Verification/ Authentication)	o 개인의 바이오정보를 기기 등에 저장된 1개의 바이오정보와 대조하여 특정 개인 본인임을 확인 - (사례 1) 지문·홍채·안면인식 등을 이용한 스마트폰 잠금해제 - (사례 2) 기기 사용자(1인)의 목소리를 다른 불특정 다수의 목소리와 구별·인식하여 작동하는 음성비서 애플리케이션
식별 (Identification)	o 개인의 바이오정보를 데이터베이스에 저장된 다수의 바이오정보와 대조하여 여러 사람 중 특정 개인 본인임을 확인 - (사례 1) 페이스북 태그 추천 기능과 같이 안면인식 기술을 통해 SNS에 올린 사진 속 인물이 누구인지 파악하여 태그할 수 있도록 돕는 이름표 추천 서비스 - (사례 2) 기 등록된 여러 가족 구성원의 음성 중 지금 말하는 사람이 누구인지를 확인하여 대답하는 음성비서 스피커

< 바이오정보가 아닌 사례 >

유 형	사 례
분류 (Categorisation)	o 개인을 인증 또는 식별하지 않고 나이, 성별 등의 기준으로 분류하거나 이용자의 움직임을 단순히 탐지하는 경우 - (사례 1) 안면인식을 통해 연령이나 성별 등을 추정하여 이용자의 유형에 맞는 광고를 내보내는 서비스 - (사례 2) 이용자의 얼굴을 자동인식해 스티커가 얼굴 위에 덧입혀지거나, 그림이 움직이는 등의 특수 효과가 적용된 카메라 애플리케이션

□ **(대상 사업자)** 이용자의 바이오정보를 직접 처리하는 정보통신서비스 제공자를 포함하여 바이오정보의 안전한 이용환경 조성에 관여하고 있는 제조사 등*(이하 '사업자')을 포함

* 바이오정보를 직접 처리하지 않지만 인증결과 값 등을 전송받는 사업자, 바이오정보를 처리하는 스마트폰 등 기기 제조사, 바이오정보에 대한 접근 권한을 통제하는 OS 사업자, 바이오정보가 활용되는 앱 개발자 등

□ **(법령과의 관계)** 바이오정보는 개인정보의 일종이므로 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭: 정보통신망법)' 등 개인정보 관련 법령을 따름

o 가이드라인은 정보통신망법, 시행령, 고시에 대한 해석 기준을 제시함과 동시에 사업자가 자율적으로 준수할 수 있는 규범적·기술적 보호조치 기준을 제안함

※ 추후 바이오정보 보호와 관련한 법규정이 신설/개정 될 경우, 해당 법규정이 가이드라인 보다 우선함

□ **(재검토 기한)** 해당 가이드라인은 '18.1.1일을 기준으로 매 3년이 되는 시점(매 3년째의 12.31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 취함

※ '바이오정보 보호 가이드라인'(정통부, '07년)은 본 가이드라인으로 대체

- 당시에는 출입통제 목적으로 바이오인식시스템을 운영하는 일반 기업 등을 대상으로 일반적인 보호 사항을 안내

Ⅲ. 바이오정보 보호원칙

1. 비례성 원칙

◇ 사업자는 바이오정보를 활용함에 따라 수반되는 위험이 사업 상 바이오정보의 필요성 및 예상되는 편익에 비해 과도하지 않은지 등을 검토 후, 수집·이용 여부를 판단하여야 한다.

◇ 서비스 도입 시 바이오정보의 종류별 특성을 고려하여 침해 위험성을 최소화할 수 있는 바이오정보를 선택하여야 한다.

o 사업자는 수집·이용하려는 바이오정보의 사업 목적 상 필요한 정도와 예상되는 편익이 위험성에 비해 과도하지 않은지 등을 검토한 후, 수집·이용여부를 판단하여야 한다.

- 사업자는 서비스를 도입하기 전, 바이오정보 외에 이용자의 개인정보 침해 위험성을 최소화하면서 사업 목적을 달성할 수 있는 다른 수단이 있는지 검토한다.

o 또한, 바이오정보마다 특성이 상이하여 개별 서비스에 대한 적합도가 다르므로, 사업 목적 달성과 함께 침해 위험성을 최소화할 수 있는 바이오정보를 선택하여야 한다.

※ 다만, 기술 발전에 따라 바이오정보의 특성 및 서비스 적합도가 달라질 수 있으므로 이에 대한 고려가 필요하다.

< 비례성 검토 예시 >

o 사업자가 자사 회원의 앱·웹 이용을 통제하고, 회원 관리를 원활히 하기 위해 모든 회원의 바이오정보를 서버로 전송하여 처리한다면 이는 비례성 원칙에 비추어 지나친 것으로 볼 수 있음

- 단순히 회원을 식별하기 위한 용도라면, 기기 내 안전한 영역에서 처리된 바이오정보의 인증 결과 값 등을 전송받는 방법이 권장됨

o 비대면거래에서의 본인인증 서비스에서는 SNS에서의 이름표 추천 서비스에서 보다 위·변조가 어렵고, 보안성이 높은 바이오정보를 사용하는 것이 적합함

2. 수집·이용 제한의 원칙

◇ 사업자는 바이오정보의 수집·이용 목적, 항목, 보유기간을 이용자에게 명확히 알리고 동의 받아야 한다.

◇ 사업자는 인증·식별 목적에 필요한 최소한의 바이오정보를 수집·이용해야 한다.

◇ 특징정보 생성 후 원본정보는 원칙적으로 파기해야 하며, 원본정보를 파기하지 않는다면 그 이유(목적) 및 보유기간을 별도로 고지 후 동의 받아야 한다.

◇ 바이오정보 처리 과정에서 인종·병력 등 민감한 정보가 추출되지 않도록 관리하여야 한다.

가. 바이오정보의 수집·이용 동의

o 이용자의 바이오정보를 수집하려는 사업자는 웹사이트나 애플리케이션 등을 통해 다음 사항 모두를 이용자에게 명확히 알리고 동의 받아야 한다.

- ① 바이오정보의 수집·이용 목적, ② 수집하는 바이오정보의 항목, ③ 바이오정보의 보유·이용 기간

< 바이오정보 필수 수집·이용 동의 예시 >

■ [필수*] 바이오정보 수집·이용 동의			
목적	항목	보유·이용기간	동의여부
이용자 식별 및 본인 인증	지문정보 (원본정보 및 특징정보)	o 원본정보: 특징정보 생성 시 까지 o 특징정보: 회원탈퇴 시 까지	□ 동의함 □ 동의안함

* 필수동의 여부는 해당 서비스의 특성에 따라 달리 정할 수 있다.

o 원본정보는 특징정보 생성 시, 지체 없이 파기하는 것이 원칙이며, 원본정보를 파기하지 않는다면 그 이유(목적) 및 보유기간을 기존 바이오정보 수집·이용 동의와 구분하여 고지하고, 동의 받아야 한다.

- 특징정보 생성 등 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 원본정보 이외의 원본정보 수집·이용*에 동의하지 아니한다는 이유로 서비스의 제공을 거부하여서는 아니 된다.

* (예시) 인공지능 스피커의 화자인식 알고리즘 고도화를 위한 원본정보 수집·이용 등

< 원본정보 선택 수집·이용 동의 예시 >

■ [선택] 원본정보 수집·이용 동의			
목적	항목	보유·이용기간	동의여부
화자인식 알고리즘 고도화	음성정보	o 회원탈퇴 시 까지	□ 동의함 □ 동의안함

※ 동의를 거부하시는 경우에도 oo서비스는 이용하실 수 있습니다.

정보통신망법 제22조(개인정보의 수집·이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.
1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

정보통신망법 제23조(개인정보의 수집 제한 등) ③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우

정보통신망법 제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자

정보통신망법 제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

1. 제22조의2제2항 또는 제23조제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 자

나. 최소 정보 수집·이용

o 사업자는 인증 또는 식별 목적에 필요한 최소한의 바이오정보를 수집·이용해야 한다.

※ 한 서비스에 한 종류의 바이오정보만을 활용해야 한다는 의미는 아니며, 보안강화 등 사업자 필요에 따라 두 종류 이상의 바이오정보를 수집·이용할 수 있다.

o 특히 원본정보로부터 인종·병력 등 인증·식별 목적과는 무관한 부가적인 정보가 추출될 수도 있으므로,

- 사업자는 특징정보 생성 등 바이오정보 처리 과정에서 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보가 추출·수집·이용되지 않도록 관리해야 한다.

정보통신망법 제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다.

개인정보 보호법 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

2. 제23조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 경우

정보통신망법 제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

2. 제23조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자

3. 목적제한의 원칙

◇ 바이오정보는 이용자에게 동의 받은 인증 또는 식별 이외의 목적으로 무단으로 활용되어서는 아니 된다.

o 인증 또는 식별 목적으로 이용자에게 동의 받은 바이오정보를 무단으로 질병검사 등 다른 목적으로 활용해서는 아니 된다.

- 바이오정보가 인증 또는 식별 목적 외 개인정보로서 동시에 활용되는 것이 제한되지는 않으나,

※ 이용자가 SNS에 올린 사진을 이름표 추천 서비스 목적으로 활용한다면 바이오정보로서 활용되는 동시에 개인정보로서 활용되는 것임

- 인증 또는 식별 이외의 목적으로 활용하기 위해서는 일반 개인정보로서 이용자의 사전 동의 등 적법한 절차를 따라야 한다.

※ 바이오정보는 개념 상 개인을 인증 또는 식별하기 위하여 기술적으로 처리되는 개인정보를 의미함

정보통신망법 제24조(개인정보의 이용 제한) 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
3. 제24조(제67조에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용한 경우

정보통신망법 제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
3. 제24조, 제24조의2제1항 및 제2항 또는 제26조제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

4. 통제권 보장의 원칙

◇ 사업자는 이용자가 바이오정보를 수정하거나 삭제할 수 있도록 다양한 통제 수단을 제공해야 한다.

◇ 이용자가 바이오정보의 제공을 원하지 않거나 신체적 장애 등으로 제공할 수 없는 경우를 대비하여 가능한 대안을 마련하는 것이 바람직하다.

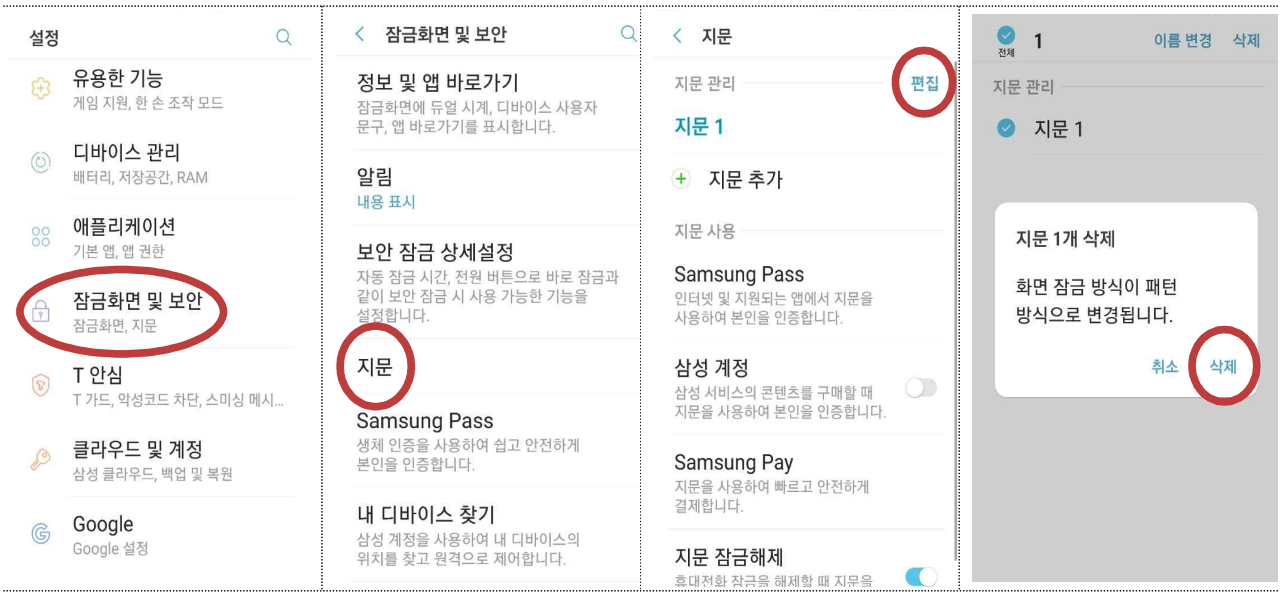
가. 이용자 기기를 통해 통제권을 행사하는 방법

o 바이오정보를 처리하는 기기 제조사 또는 OS사업자는 이용자가 해당 기기 또는 웹·앱 등을 통해 바이오정보를 수정하거나, 삭제할 수 있도록 통제수단을 제공해야 한다.

① 스마트폰에서의 통제 방법

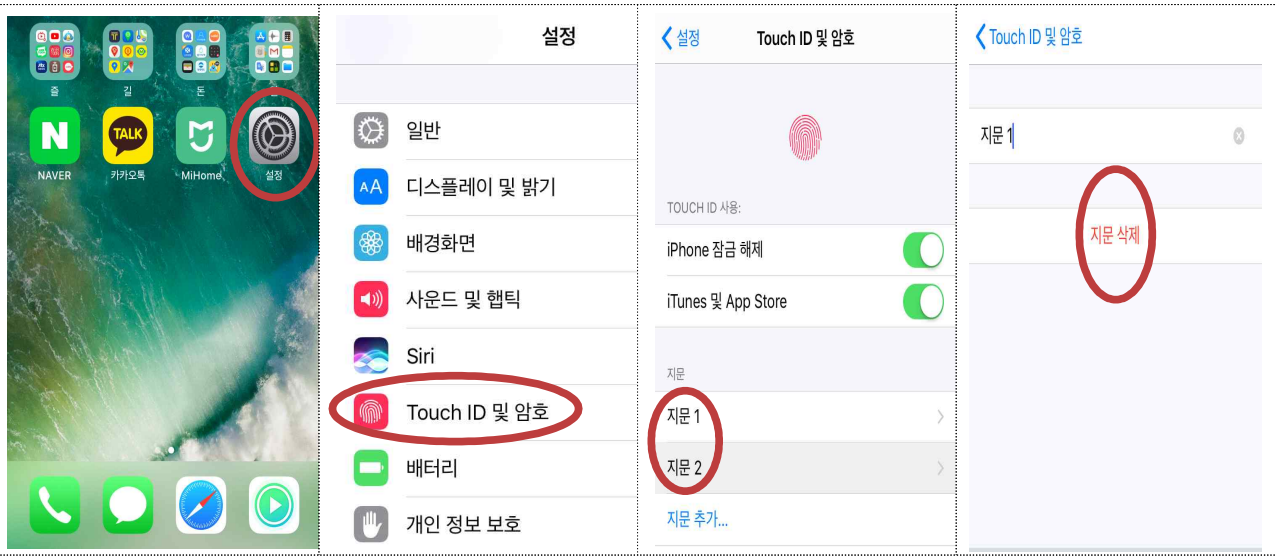
- **(예시 : 안드로이드폰)** ① 설정 → ② 잠금화면 및 보안 → ③ 지문 편집 → ④ 바이오정보 수정·삭제

< 설정 방법 >



- (예시 : 아이폰) ① 설정 → ② Touch ID 및 암호 → ③ 바이오정보 수정·삭제

< 설정 방법 >

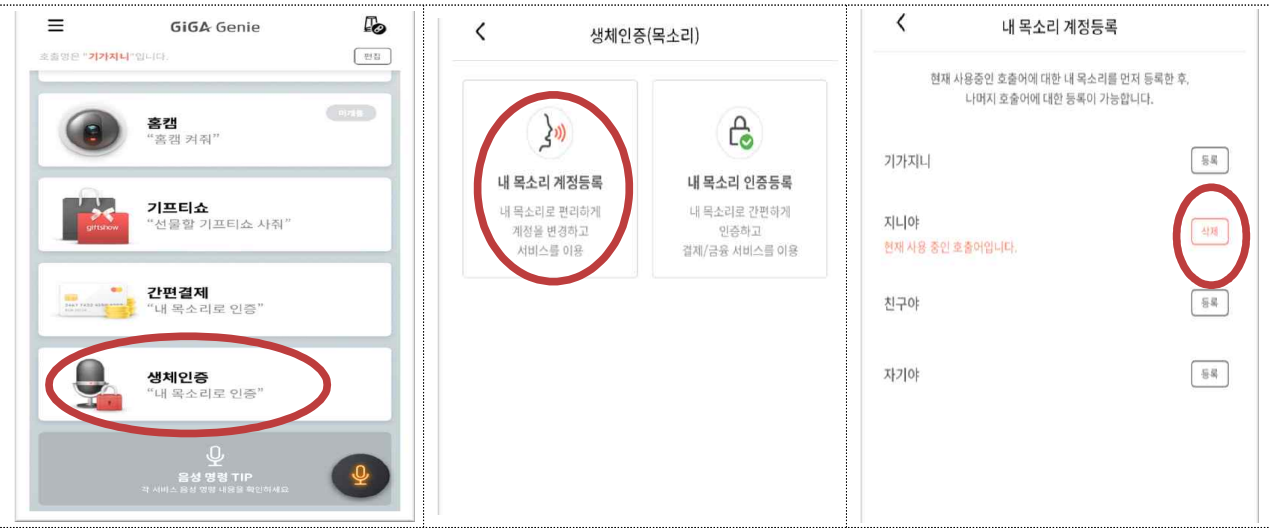


② AI 스피커 등에서의 통제 방법

o AI 스피커 등과 같이 기기에서 직접적인 이용자의 통제권 행사가 어려운 경우, 웹페이지 또는 앱 등을 통해 이용자가 바이오정보를 수정하거나 삭제할 수 있도록 통제수단을 제공해야 한다.

- (예시 : 기가지니 AI 스피커) ① 생체인증 → ② 내 목소리 계정등록 → ③ 바이오정보 수정·삭제

< 설정 방법 >

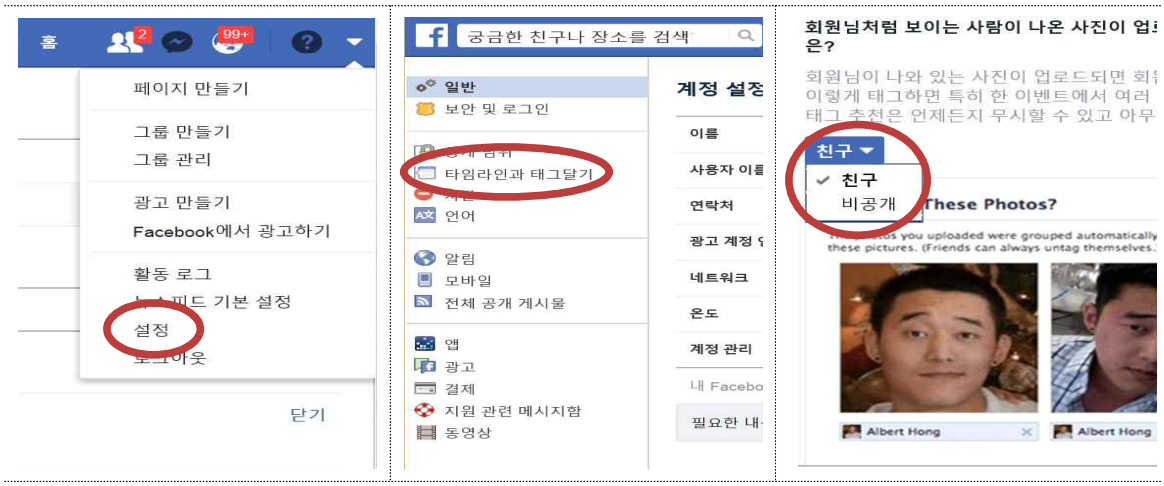


나. 사업자의 웹 또는 앱에서 통제권을 제공하는 방법

o 이용자의 바이오정보를 사업자가 직접 수집하거나 사진, 음성 등과 같이 기(旣) 수집된 개인정보를 바이오정보로 활용하는 경우, 해당 서비스에서 이용자가 직접 통제할 수 있는 수단을 제공해야 한다.

- **(예시 : 페이스북 태그 추천 기능)** ① 설정 → ② 타임라인과 태그 달기 → ③ 태그 추천 기능 설정 및 해제

< 설정 방법 >



o 이용자의 바이오정보를 서버로 직접 수집하는 것이 아니라 스마트폰 등 기기 내에서 처리된 인증 결과 값 등을 서버를 통해 전송받는 경우, 해지 메뉴 등을 통해 이용자가 자신의 바이오정보를 쉽게 통제할 수 있는 방법을 제공해야 한다.

< 바이오정보 통제 방법 안내 예시 >

o OO 바이오정보 인증서비스는 이용자 스마트폰에 등록된 바이오정보를 이용한 본인 인증 서비스입니다.

o 당 사는 이용자의 바이오정보를 서버로 전송하지 않으며, 스마트폰에 등록된 바이오정보와 대조한 결과 값만을 전송받아 본인인증을 진행합니다.

o OO 바이오정보 인증서비스의 해지를 원하실 경우 아래 메뉴를 통해 설정해 주시기 바랍니다.

< OO 바이오정보 인증서비스 설정 >

사용	해지
√	√

다. 대안 마련

o 사업자는 이용자(만 14세 미만의 아동인 경우 아동 또는 그 아동의 법정대리인)가 바이오정보 제공을 원하지 않거나, 신체적 장애 등으로 바이오정보를 제공할 수 없는 상황에 대비하여,

- 가능한 경우* 비밀번호, 아이핀 등 인증 및 식별을 위한 대안을 마련하도록 권고한다.

* 이름표 추천 서비스와 같이 서비스 특성상 바이오정보 이외의 대안을 마련할 수 없는 경우도 있음

정보통신망법 제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.

1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

③ 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다.

④ 정보통신서비스 제공자등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

⑤ 정보통신서비스 제공자등은 제2항에 따라 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다.

⑥ 정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

⑦ 영업양수자등에 대하여는 제1항부터 제6항까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자등"은 "영업양수자등"으로 본다.

정보통신망법 제31조(법정대리인의 권리) ① 정보통신서비스 제공자등이 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 한다. 이 경우 정보통신서비스 제공자는 그 아동에게 법정대리인의 동의를 받기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다.

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
7. 제31조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우

정보통신망법 제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
7. 제30조제5항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자
8. 제31조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자

정보통신망법 제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.
5. 제30조제3항·제4항 및 제6항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니한 자

5. 투명성 원칙

◇ 사업자는 바이오정보 보호에 관한 사항을 이용자에게 적극적으로 안내해야 한다.

◇ 사업자는 바이오정보 서비스와 관련된 이용자의 문의 및 침해 민원 등을 처리하기 위한 피해구제 기능을 마련·운영해야 한다.

가. 인식확산

o 사업자는 개인정보 처리방침 등을 포함하여 이용자에게 수집·이용되는 바이오정보의 종류, 보호 조치, 통제권 행사 방법, 처리방법 등을 적극적으로 안내하여야 하고, 이용자가 언제든지 이를 확인할 수 있도록 하여야 한다.

나. 피해구제

o 사업자는 바이오정보 서비스와 관련된 이용자 문의, 통제권 행사, 피해 신고 접수 등을 처리하기 위한 피해구제 기능을 마련·운영해야 한다.

o 사업자는 이용자에게 바이오정보의 보호와 관련하여 피해구제 기능을 쉽게 이용할 수 있는 방법을 제공해야 한다.

- 바이오정보 보호책임자의 성명 또는 바이오정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭, 연락처 공개 등

※ 기존 개인정보 보호책임자 및 개인정보보호 업무를 처리하는 부서에서 바이오정보 보호 관련 피해구제 등 업무 수행이 가능하다.

정보통신망법 제27조(개인정보 보호책임자의 지정) ① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

② 제1항 단서에 따른 정보통신서비스 제공자등이 개인정보 보호책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 보호책임자가 된다.

③ 개인정보 보호책임자의 자격요건과 그 밖의 지정에 필요한 사항은 대통령령으로 정한다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 정보통신서비스 제공자등의 사업주 또는 대표자에게 개선조치를 보고하여야 한다. 다만, 제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우에는 개선조치 보고에 대한 사항을 적용하지 아니한다.

정보통신망법 제27조의 2(개인정보 처리방침의 공개) ① 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 경우에는 개인정보 처리방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

② 제1항에 따른 개인정보 처리방침에는 다음 각 호의 사항이 모두 포함되어야 한다.
1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조제1항 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 처리방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 처리방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.

정보통신망법 제76조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.
3. 제27조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
4. 제27조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 공개하지 아니한 자

6. 바이오정보 보호 중심설계 및 운영원칙

◇ 바이오정보를 활용한 서비스의 개발·설계 단계부터 이용자의 바이오정보 보호를 고려하도록 권고한다.

◇ 대량의 바이오정보를 서버로 전송하여 처리하는 경우, 사전에 이용자의 프라이버시에 미칠 영향 및 개인정보 위험 요인 등을 조사·분석·평가하는 절차를 마련하는 것이 바람직하다.

가. 바이오정보 보호 중심 설계

o 바이오정보를 활용한 서비스의 개발·기획 단계에서부터 바이오정보 침해를 예방하고 피해를 최소화할 수 있는 방안을 고려하고 그 운영을 유지하도록 권고한다.

- 특히, 기본 값(Defaults)은 이용자의 바이오정보가 보호될 수 있도록 설정한다.

※ (예시) 특징정보 생성 시, 바이오 원본정보는 삭제되도록 기본설정

- 바이오정보의 전송을 최소화 하도록 설계하는 것을 권장하며, 원본정보로부터 특징정보를 생성하는 알고리즘을 안전하게 관리한다.

- 특징정보로부터 원본정보가 쉽게 복원되지 않도록 특징정보 생성 알고리즘을 설계한다.

- 사업자가 바이오정보 서비스를 위해 시중에 공급된 기성 제품을 도입할 경우, 이용자의 바이오정보가 보호될 수 있는 제품인지를 고려한다.

나. 개인정보 영향평가(Privacy Impact Assessment) 시행

o 바이오정보를 서버로 전송하여 대량으로 처리하는 경우, 이용자의 개인정보보호에 미칠 영향에 대해 미리 조사·분석·평가하는 체계적인 절차를 마련하도록 권고한다.

- 바이오정보를 서버로 전송하여 처리할 경우, 기기 내에서 처리하는 경우보다 바이오정보의 유출 및 오·남용 등의 침해 위협이 커짐에 따라,

- 바이오정보 침해 위험요인을 분석하고 개선사항을 도출하여 침해사고를 예방하도록 개인정보 영향평가를 실시할 것을 권고한다.

※ 자세한 개인정보 영향평가 방법은 「개인정보 영향평가에 관한 고시('17년 9월 개정)」 및 「개인정보 영향평가 수행 안내서」를 참고할 수 있다.

Ⅳ. 기술적·관리적 보호조치

□ 사업자는 바이오정보의 불법 유출·위변조 등을 방지하기 위한 기술적·관리적 보호조치를 취해야 한다.

o 바이오정보 처리 단계별 개인정보 침해위험 요인을 파악하고, 각 단계별 필요한 보호조치를 취하여야 한다.

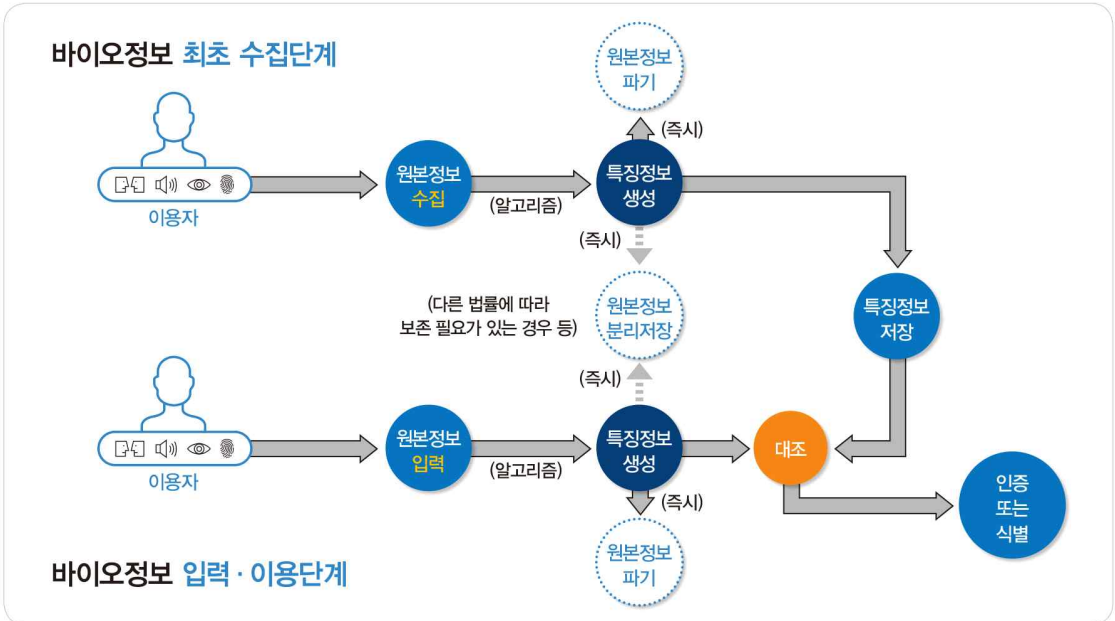
※ 정보통신망법 제28조(개인정보의 보호조치) 및 방통위 고시 「개인정보의 기술적·관리적 보호조치 기준」의 필요한 조치 등을 참고한다.

o 가이드라인에 소개된 보호조치는 바이오정보 처리 시 자율적으로 준수할 수 있는 최소한의 기준이며, 각 사업자는 추가적인 보호조치 또는 기술발전에 따른 새로운 방안을 마련할 수 있다.

< 각 단계별 바이오정보 침해위험 요인 >

① 수집·입력	⇨	② 저장·이용	⇨	③ 파기
동의 없는 수집, 위·변조된 바이오정보 입력, 암호화 저장 전 유출		저장된 정보 유출 네트워크를 통한 전송 시 유출		목적 달성 후 불필요한 보유

< 바이오정보 처리 과정 >



정보통신망법 제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다.

1. 수집·입력 단계

◇ 사업자는 바이오정보가 수집·입력될 때 위·변조된 바이오정보가 처리되지 않도록 보안조치를 취하여야 한다.

◇ 사업자는 바이오정보가 전송될 때, 해킹 등의 공격으로 바이오정보가 외부에 유출되거나 위·변조 되지 않도록 조치하여야 한다.

가. 위·변조된 바이오정보 수집·입력에 대한 대책 마련

o 사업자는 센서 등의 장치를 통해 바이오정보가 수집·입력될 때, 제3자에 의해 위·변조된 바이오정보가 처리되지 않도록 적절한 보안조치를 취하여야 한다.

- 실리콘 인공지문, 녹음된 음성, 캡처된 얼굴·홍채사진 등과 같이 위·변조된 바이오정보가 수집·입력될 경우, 이를 탐지하고 서비스 이용을 거부할 수 있도록 조치하는 것이 바람직하다.

※ 단, 위·변조 탐지 기술의 수준은 서비스 용도 및 바이오정보 침해 위협 정도를 고려하여 사업자의 책임 하에 적절하게 결정할 수 있다.

※ 위·변조 탐지 기술 적용에 관해서는「생체인식 제시형 공격 탐지 제1부 프레임 워크, KS X ISO/IEC 30107-1('18년 1월 예정)」KS 국가 표준을 참고할 수 있다.

나. 바이오정보 수집·입력 시, 전송구간 보호

o 바이오정보가 암호화되어 저장되기 전까지, 인가되지 않은 접근, 해킹 등으로 인한 유출, 위·변조 가능성 등을 방지하기 위하여 바이오정보 수집·입력 시 전송구간 암호화 조치를 취해야 한다.

「개인정보의 기술적·관리적 보호조치 기준」제6조(개인정보의 암호화) ③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
6. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 조치를 하지 아니한 경우

정보통신망법 제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 자

정보통신망법 제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.
3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자

2. 저장·이용 단계

◇ 바이오정보는 안전한 알고리즘을 통해 암호화 하여 저장하여야 한다.

◇ 바이오정보를 서버로 전송하여 처리하는 대신 가능한 한 기기 내 안전한 영역에서 처리하여야 한다.

가. 암호화 조치

o 바이오정보가 저장·전송 등 처리될 때, 제3자에 의한 위·변조, 유출 등의 침해 방지를 위하여 안전한 알고리즘으로 바이오정보(원본 및 특징정보 포함)를 암호화하여 저장 하여야 한다.

※ 원본정보는 변경 불가능하고 인종·병력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 정보가 추출될 수 있으며 특징정보는 유출 시 변경 전까지 인증·식별 목적으로 악용될 수 있음에 따라 암호화 조치 필요

※ 구체적인 암호화 알고리즘, 수행방식, 사례 등은 행정안전부·한국인터넷진흥원의 「개인정보의 암호화 조치 안내서('17년 1월 개정)」 및 암호이용활성화(http://seed.kisa.or.kr/) 홈페이지를 참고할 수 있다.

나. 기기 내 처리

o 바이오정보를 서버로 전송하여 처리할 경우 침해사고 발생 시, 대규모 바이오정보 유출 등 피해 범위가 커지므로, 기기 내 안전한 영역 또는 보안토큰, 스마트카드 등 이용자가 직접 소지할 수 있는 매체에서 바이오정보를 저장·처리하는 방식을 우선적으로 고려하여야 한다.

- 기기 및 보조저장매체 등에 저장할 경우, 바이오정보를 암호화 하여야 한다.

「개인정보의 기술적·관리적 보호조치 기준」제6조(개인정보의 암호화) ② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.
1. 주민등록번호, 2. 여권번호, 3. 운전면허번호, 4. 외국인등록번호, 5. 신용카드번호 6. 계좌번호, 7. 바이오정보
④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

정보통신망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
6. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 조치를 하지 아니한 경우

정보통신망법 제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 자

정보통신망법 제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.
3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자

3. 파기 단계

◇ 원본정보는 특징정보가 생성된 경우, 그 목적이 달성된 것으로 볼 수 있으므로 지체없이 복구 또는 재생되지 않도록 파기하여야 한다.

◇ 법적 근거가 있거나, 이용자 동의를 받아 원본정보를 보관하는 경우 해당 이용자의 다른 개인정보와 분리하여 저장·관리 하도록 권고한다.

o 바이오정보를 활용한 인증 및 식별은 일반적으로 특징정보 비교를 통해 이루어지므로 원본정보에서 특징정보가 생성되면 원본정보의 수집·이용 목적은 달성된 것으로 볼 수 있다.

- 이에 따라, 원칙적으로 원본정보는 특징정보 생성 시, 지체 없이 복구 또는 재생되지 않도록 파기하여야 한다.

- 다만, 사업자의 필요에 의해 이용자 동의를 받아 원본정보를 이용하는 때에는 동의 받은 목적이 달성되거나, 보유·이용기간이 끝난 경우 지체 없이 원본정보를 파기하여야 한다.

※ 다른 법률에 따라 원본정보를 보존하여야 하는 경우에는 해당 법률에서 정하는 바에 따른다.

o 이용자의 동의를 받아 원본정보를 이용하거나, 다른 법률에 따라 원본정보를 보존할 경우, 원본정보는 성명・주소 등 해당 이용자의 다른 개인정보와 분리하여 별도로 저장·관리 하도록 권고한다.

- 원본정보를 별도로 저장·관리하는 경우 접근 통제 및 외부해킹방지 등의 보호조치를 하여야 하며,

- 물리적으로 분리하여 별도로 저장·관리하는 것이 바람직하나, 부득이한 경우 물리적 분리와 동등한 수준으로 논리적으로 분리하여 저장·관리 하도록 한다.

- 원본정보와 이용자의 다른 개인정보를 상호 연결하는 공통 식별자는 임의 값을 활용하여 직접적으로 해당 이용자가 나타나지 않도록 조치한다.

※ 바이오정보 보호를 위한 구체적인 기술적·관리적 보호지침은 「바이오인식 정보의 보호를 위한 기술적 관리적 지침, KS X 1966('18년 1월 예정)」 KS 국가표준을 참고할 수 있다.

정보통신망법 제29조(개인정보의 파기) ①정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우
3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우
4. 사업을 폐업하는 경우

정보통신망법 제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1의2. 제29조제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

참고	바이오정보 보호 가이드라인(안) FAQ

① 현행 법령상 바이오정보 정의에 따르면 인증 또는 식별 목적의 바이오정보 이외 일반 사진 및 음성 등도 암호화 대상인 것으로 해석될 수 있는데?

o 방통위와 행안부 고시 해설서에서는 식별 및 인증 등으로 활용되는 경우 암호화 조치를 취하도록 안내하고 있음

- 다만, 현행 법령의 문언적 의미만을 보면 단순 사진이나 음성파일까지 암호화대상으로 해석될 소지가 있으므로 이번 가이드라인을 통해 그 개념을 명확히 하고, 암호화 대상을 구체화함

※ 법령에 따른 암호화 저장 대상이 아니라고 해도 일반 개인정보 보호에 필요한 보호조치(접근통제, 접속기록 위변조방지 등)는 취하여야 함

② 화자인식의 경우 등록된 이용자를 식별하기 위해서 해당 이용자 이외의 목소리를 수집한 뒤 특징정보와 매칭하는 과정을 거치게 되는데, 이 경우 이용자가 아닌 불특정 다수의 음성도 바이오정보의 활용인지?

o 개별 서비스의 처리과정에 따라 달리 판단해야 할 것이나, 등록된 이용자를 식별하기 위해 불특정 다수의 음성이 기계 내에서 매칭된 후 즉시 파기 되는 등 다른 정보와 쉽게 결합하여도 특정 개인을 알아볼 수 없도록 처리된다면 개인정보에 해당하지 않을 것으로 판단됨

※ 만일 불특정 다수의 목소리가 서버로 전송되고 특정 개인을 알아볼 수 있다면 개인정보로서 수집·이용 동의를 받아야 함

- 다만, 음성의 처리 과정을 누구나 인식할 수 있도록 명확히 고지할 필요가 있음

③ 향후 화자의 음성에서 성별(남/녀), 연령, 감정(슬픔, 화남, 기쁨)을 인식하기 위한 정보를 추출하는 서비스를 할 예정인데, 이러한 정보는 바이오정보에 해당되는지?

o 개인을 인증 또는 식별하기 위한 목적이 아닌 경우 바이오정보에 해당하지 않으나, 음성에서 성별, 연령 등 추가적인 정보를 추출할 경우 개인정보의 목적 외 이용에 해당하지 않도록 적법한 절차를 거쳐야 함

- 화자인식을 통해 특정 개인을 식별 한 후 성별, 연령 등 추가적인 정보를 추출하여 활용할 경우, 이용자의 사전 동의가 필요함

④ 바이오정보 수집·이용 동의를 기존 개인정보 수집·이용 동의와 별도로 받아야 하는 것인지?

o 기존 개인정보 수집·이용 동의와 함께 바이오정보 수집·이용 동의를 받을 수 있음

- 다만, 이용자에게 바이오정보 수집·이용에 대한 사항을 명확히 알리고 동의 받아야 하며,

- 알고리즘 고도화 등을 위해 특징정보 생성 후에도 원본정보를 파기하지 않는다면 그 이유 및 보유기간을 기존 수집·이용 동의와 구분하여 고지하고, 동의 받아야 함

⑤ 원본정보에 대해 별도의 동의를 받아야 하는 이유는?

o 특징정보 생성 시 원칙적으로 원본정보는 목적이 달성된 것으로 보아 파기하여야 하지만, 인공지능 스피커의 성능 개선 등 원본정보 수집·이용이 필요한 경우를 위해 활용이 가능하도록 함

- 다만, 원본정보의 중요성을 고려하여 별도의 동의를 받도록 규정

⑥ 기 수집된 개인정보에서 차후에 특징정보를 추출하려는 경우 동의 방식은?

o 기존의 수집·이용 동의 목적과 다르므로 원본 및 특정정보 모두에 대해 필요한 시점에 동의를 받아야 함

⑦ 바이오정보를 인증 또는 식별 목적과 그 이외의 용도로 함께 활용할 수 있는지?

o 바이오정보는 그 정의에 따라 인증 또는 식별 목적으로 활용되는 경우를 말하며, 그 이외의 목적으로 활용한다면 개인정보 관련 법령을 준수하여 활용 가능

※ 이용자가 SNS에 올린 사진을 태깅 서비스 목적으로 활용한다면 바이오정보로서 활용되는 동시에, SNS를 위한 개인정보로 활용됨

⑧ 원본정보를 삭제한다면 서비스 성능 개선을 위해 화자인증 모듈을 업데이트할 경우 원본정보 등록이 다시 필요하게 되어 이용자가 그때마다 재등록하게 되는 등 불편함을 느끼게 되는데?

o 재등록의 불편방지를 위해 원본정보 제공을 원하는 이용자가 있는 반면에, 어느정도의 불편을 감수하더라도 원본정보 삭제를 원하는 이용자의 의사도 존중할 필요가 있으므로 원본정보는 이용자에게 별도의 동의를 받아 수집하는 것이 바람직함

⑨ 가이드라인에 따르면 특징정보 생성 후 원본정보를 원칙적으로 파기해야 하는데, 이용자가 스스로 공개하거나 클라우드 등에 직접 올린 사진에서 사업자가 특징정보를 추출한 경우 해당 사진을 파기해야 하는지?

o 이용자가 직접 올린 사진에서 사업자가 특징정보를 추출하는 것이 목적 외 이용은 아닌지 우선 확인하여야 하며,

- 이용자의 동의를 받아 특징정보를 추출하였다면, 원본정보는 이용자의 기존 서비스 이용 목적을 위해 파기하지 않을 수 있음

⑩ 이용자의 동의를 받아 원본정보를 활용하는 경우에도 해당 이용자의 다른 개인정보와 분리하여 별도로 저장·관리해야 하는지?

o 특징정보 생성 시 원칙적으로 원본정보는 목적이 달성된 것으로 보아 파기하여야 하지만, 알고리즘 고도화 등 원본정보 수집·이용이 필요한 경우를 위해 별도의 동의를 받아 활용이 가능하도록 함

- 그러나, 원본정보는 변경이 불가능하여 유출 등 침해 예방이 매우 중요하고, 인종·병력 등 부가적인 정보가 추출되어 개인의 프라이버시를 침해할 우려도 있으므로 강화된 보호조치가 필요

⑪ 바이오정보의 종류, 처리방법 등을 안내하고 바이오정보 보호책임자의 성명 또는 관련 부서의 명칭과 연락처를 공개하려면 기존 개인정보처리방침과는 별도로 마련·공개해야 하는 것인지?

o 기존 개인정보 보호책임자 및 개인정보보호 업무를 처리하는 부서에서 바이오정보 보호 관련 피해구제 등 업무를 동시에 수행할 수 있으며,

- 이 경우 공개에 있어서도 기존의 개인정보처리방침상 개인정보 보호책임자 또는 처리 부서의 명칭과 연락처 공개로 갈음할 수 있음
- 다만, 기존 개인정보처리방침을 통해 바이오정보 관련 사항을 함께 안내하는 경우에도 수집하는 바이오정보의 항목 등을 명확히 알아볼 수 있도록 조치하여야 함

⑫ SNS 등에 이미 공개된 사진을 인증·식별 목적으로 활용하는 경우에도 원본정보와 특징정보를 암호화 저장해야 하는지?

o 특징정보의 경우 암호화 저장이 필요하지만, 원본정보가 이용자 스스로 일반 공중에 공개한 사진인 경우, 기밀성이 보장될 이유가 없다는 점에서 암호화 저장의 실익이 없음

※ 암호화 저장 이외 보호조치(내부관리계획 수립·시행, 접근통제, 전송구간 암호화 등)는 하여야 함

⑬ 바이오정보 보호를 위해 참고할 수 있는 국외 가이드라인은 어떤 것들이 있는지?

< 국외 주요 바이오정보 보호 가이드라인 >

주체	가이드라인
International Biometric Industry Association (IBIA, 국제바이오인식협회)	o IBIA Privacy Best Practice Recommendations For Commercial Biometric Use (상업용 바이오인식 사용 대상 IBIA 프라이버시 선진 사례 권고, 2014)
EU ARTICLE 29 DATA PROTECTION WORKING PARTY (WP29, 제29조 작업반)	o Opinion 3/2012 on developments in biometric technologies (바이오인식 기술 발전에 대한 의견 3/2012)
Biometrics Institute (바이오인식 협회)	o Biometrics Privacy Guidelines (바이오인식 프라이버시 가이드라인, 2015)
Commissioner for Privacy and Data Protection (CPDP, 호주 프라이버시 및 데이터보호 감독원)	o Biometrics and privacy (바이오인식과 프라이버시, 2016)
Office of the Privacy Commissioner for Personal Data (PCPD, 홍콩 개인정보보호 위원회)	o Guidance on Collection and Use of Biometric Data (바이오 정보 수집 및 사용 가이드라인, 2016)