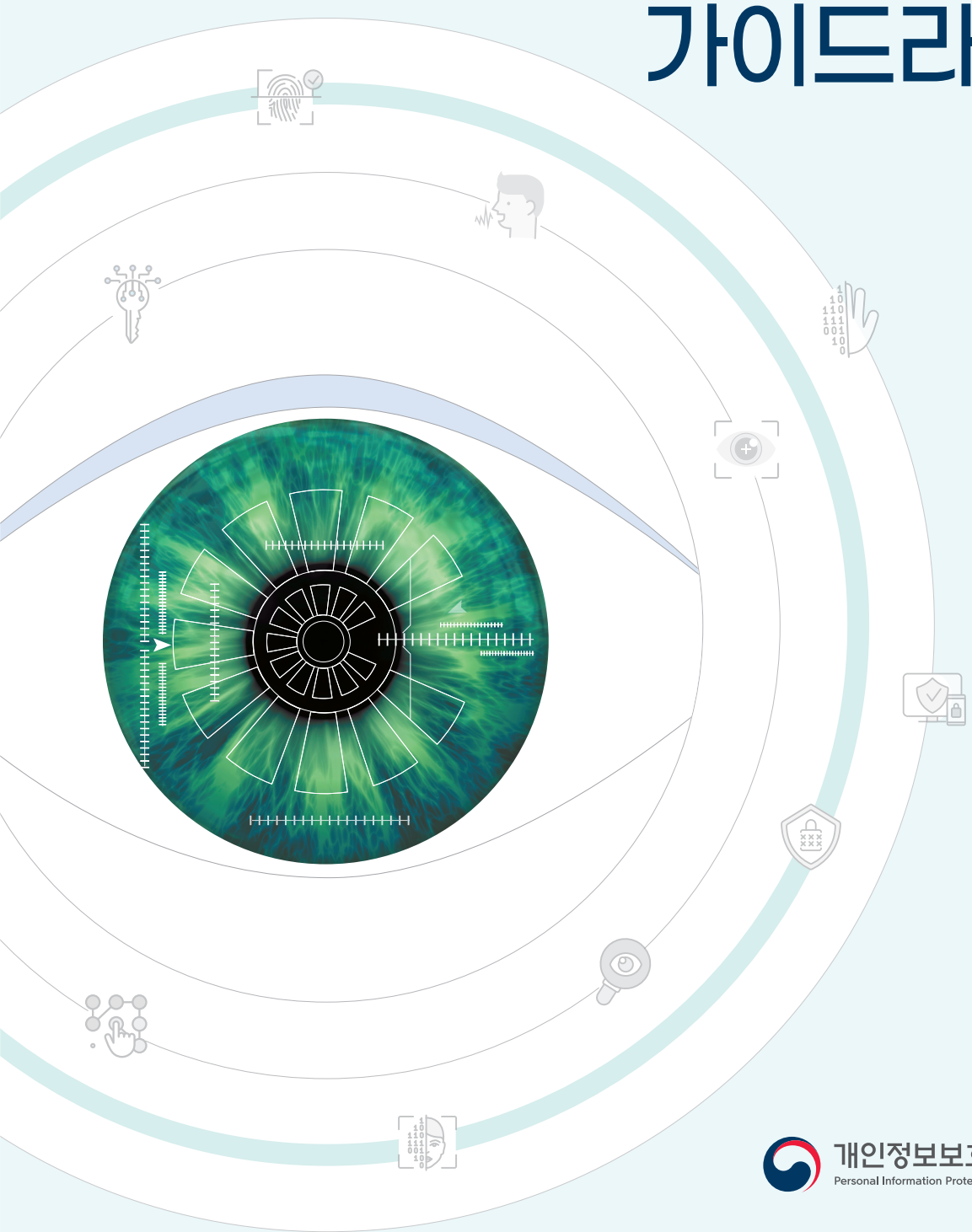
2021. 9.

생체정보 보호 가이드라인



개인정보보호위원회
Personal Information Protection Commission


생체정보 보호
가이드라인

CONTENTS

Ⅰ 개요 01

1. 생체정보 동향 01
2. 목 적 02
3. 생체정보의 개념 03
4. 적용 대상 08
5. 법령과의 관계 08

Ⅱ 생체인식정보의 특성 및 보호 원칙 09

1. 생체인식정보의 특성 09
2. 생체인식정보 보호 원칙 10

Ⅲ 생체인식정보 보호 조치(개인정보처리자 및 제조사) 11

1. 기획·설계 단계 12
2. 생체인식정보 수집 단계 16
3. 생체인식정보 이용·제공 단계 23
4. 생체인식정보 보관·파기 단계 29
5. 상시 점검 32

Ⅳ 안전한 이용환경 조성(제조사의 역할) 34

Ⅴ 생체인식정보 활용 서비스 이용안내(이용자) 37

Ⅵ 활용 안내사항 41

부록 42

1. 자율점검표(개인정보처리자 및 제조사) 42
2. 자율점검표(이용자) 45
3. 일반적인 생체정보에 권장되는 보호 조치 46
4. 생체정보 보호 가이드라인 FAQ 48
5. 용어 설명 52
6. 참고문헌 54

개요

1 생체정보 동향

- 생체정보는 과거 기업의 출입통제 시스템에 한정되어 사용되었으나 최근 스마트폰 잠금해제, AI 음성비서 서비스 등 정보통신분야 전반에서 그 활용도가 증가하고 있음

  ※ 전 세계 생체인식 시장은 2016년 약 24억 달러에서 2025년 약 151억 달러로, 연평균 22.7% 성장할 것으로 예상(Statista, 2020)

  ※ 국내 생체인식 시장은 '18년 2,617억 원에서 '21년 3,577억 원으로 연평균 8.13% 성장(보안뉴스, 시큐리티 월드, 2020 국내외 보안시장 전망보고서)

  - 스마트폰 등 생체정보 이용 기기의 보급이 보편화되고 코로나19로 비대면 서비스로의 전환이 늘어나면서 다양한 분야에서 생체정보 이용이 일상화되고 있음

- 반면, 최근 생체정보가 유출되거나 위·변조되는 사례가 발생하면서 국민의 우려도 높아지고 있음

  사례1 이스라엘의 보안 전문가가 생체인식정보 관련 제조사의 '보안설정이 잘못되어 인터넷에 노출된 서버'에서 암호화되지 않은 사용자 이름, 비밀번호, 지문, 안면정보 등을 발견('19.8)

  사례2 모 부대 소속 군의관들이 실리콘으로 위조지문을 제작하여 출퇴근 확인용 지문인식기에 서로 대신 인식시켜주는 방법으로 담당 지휘관의 직무를 방해하고 초과근무 수당을 수령('19.3)

  사례3 해커집단의 APT공격에 의해 미국 연방부처의 DB가 해킹되어 미국 전·현직 공무원의 개인정보 2,200만 건 및 지문정보 560만 건 유출('15.6)

- 이에 EU 등 주요 국가들은 개인정보의 한 유형으로 '생체인식정보'를 구체적으로 정의하고, 생체인식정보를 보호하기 위한 원칙 등을 담은 가이드라인 등을 발표

외국의 생체인식정보 보호 가이드라인

국가 및 기관	가이드라인
폴란드 개인데이터보호사무소(UODO)	• 생체인식정보 사용에 관한 지침 발표(2021)
Office of the Privacy Commissioner for Personal Data (PCPD, 홍콩 개인정보보호 위원회)	• Guidance on Collection and Use of Biometric Data (생체인식정보 수집 및 사용 가이드라인, 2020)
European Data Protection Board (EDPB, 유럽 개인정보 보호 이사회)	• Guidelines 3/2019 on processing of personal data through video devices (영상정보 가이드라인 3/2019) • Opinion 3/2012 on developments in biometric technologies(생체인식 기술 발전에 대한 의견 3/2012)
Australian Human Rights Commission (호주 인권위원회)	• Human Rights and Technologies (인권과 기술, 2019)
Commissioner for Privacy and Data Protection (CPDP, 호주 프라이버시 및 데이터보호 감독원)	• Biometrics and privacy (생체인식과 프라이버시, 2016)
Biometrics Institute (생체인식 협회)	• Biometrics Privacy Guidelines (생체인식 프라이버시 가이드라인, 2015)
International Biometric Industry Association (IBIA, 국제생체인식협회)	• IBIA Privacy Best Practice Recommendations For Commercial Biometric Use (상업용 생체인식정보 사용 관련 IBIA 프라이버시 선진 사례 권고, 2014)
Cross Government Biometric Group (뉴질랜드 내무부 주재 기관 간 생체인식 그룹)	• Guiding Principles the Use of Biometric Technologies (생체인식 기술 이용 지침 원칙, 2009)

2 목적

◈ 지문·홍채를 이용한 스마트폰 잠금해제, 안면인식을 활용한 출입통제, 음성 기반 AI 비서 서비스 등 다양한 분야에서 생체정보를 활용한 인증·식별 서비스가 증가함에 따라

- 현행 개인정보 보호법령 및 관련 고시 등에서 규정하고 있는 생체정보에 대하여 개념 및 범위를 명확하게 하고
- 생체인식정보 보호를 위한 기본원칙과 처리 단계별 보호 조치 등을 구체적으로 제시함으로써 생체인식정보의 안전한 활용기반을 조성하고자 함

※ '20년 8월 개정된 개인정보 보호법령 개정사항*을 반영하여 기존 「바이오정보 보호 가이드라인」('17.12월)을 수정·보완함

* 개인정보 보호법 시행령 제18조제3호에서 "개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보"를 민감정보로 규정 등

3 생체정보의 개념

가. 생체정보와 생체인식정보의 정의

(1) '생체정보'란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 ①개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 ②특정 개인을 인증·식별하거나 ③개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 ④일정한 기술적 수단을 통해 처리되는 정보

① **개인의 신체적·생리적·행동적 특징**

- 신체적 특징 : 지문, 얼굴, 홍채·망막의 혈관 모양, 손바닥·손가락의 정맥 모양, 장문, 귓바퀴의 모양 등
- 생리적 특징 : 뇌파, 심전도, 유전정보 등
- 행동적 특징 : 음성, 필적, 걸음걸이, 자판입력 간격·속도 등

② **특정 개인을 인증·식별**: 지문·홍채·얼굴 등에서 추출한 특징점 등을 이용(비교·대조)하여 특정 개인임을 확인

i) 인증 : 이용 권한이 있는 특정 개인임을 확인하기 위하여 이용자가 입력한 생체정보를 기기 등에 저장된 정보와 대조하여 본인 여부 확인

※ (예시) 지문을 입력하면 본인 여부를 확인한 후 출입을 허용하는 출입통제 시스템

ii) 식별 : 개인의 생체정보를 데이터베이스에 저장된 다수의 생체정보와 대조하여 여러 사람 중 특정 개인을 구분하여 확인

※ (예시) 기 등록된 여러 가족 구성원의 음성 중 지금 말하는 사람을 확인하여 대답하는 인공지능 스피커

③ **개인에 관한 특징을 알아보기 위해**: 인증·식별 목적이 아닌, 사람의 연령·성별·감정 등의 상태를 확인 또는 분류하는 것

※ (예시1) 안면인식을 통해 연령이나 성별 등을 추정하여 이용자를 분류하는 행위
※ (예시2) 이용자의 얼굴을 자동 인식해 눈·코·입 위치에 맞는 스티커를 얼굴위에 덧입히는 것

④ **일정한 기술적 수단을 통해 처리**: 센서 입력장치 등을 통해 이미지 등 원본정보를 수집·입력하고 해당 원본정보로부터 특징점을 추출하는 등 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 전자적으로 처리되는 전 과정

(2) '생체인식정보'란 생체정보 중 특정 개인을 인증·식별할 목적으로 처리되는 정보

➜ 따라서 생체정보는 특정 개인을 인증·식별하기 위한 목적으로 처리되는 **'생체인식정보'**와 인증·식별 목적이 아닌, 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 처리되는 **일반적인 생체정보(이하 "일반적인 생체정보")**로 구성

참고 | '생체인식정보'와 '일반적인 생체정보'의 구분 및 예시

- **얼굴 사진(영상)의 경우**
  - **생체인식정보** : 얼굴 사진(영상)에서 특징점 등을 기술적으로 추출하여 개인의 인증·식별 목적으로 출입통제(안면인식) 시스템 등에 사용하는 경우는 생체인식정보에 해당
  - **일반적인 생체정보** : 얼굴 사진(영상)에서 특징점 등을 기술적으로 추출하지만 특정 개인의 인증·식별 목적이 아닌 성별, 감정상태(웃는 모습, 화난 모습 등)를 알아보기 위해 사용되는 경우는 '일반적인 생체정보'에 해당
- **음성의 경우**
  - **생체인식정보** : AI 스피커에서 입력된 사람의 음성을 통해 특징점 등을 기술적으로 추출하여 말하는 사람이 누구인지 확인하여 응답하는 경우는 생체인식정보에 해당
  - **일반적인 생체정보** : AI 스피커에서 입력된 사람의 음성을 통해 특징점 등을 기술적으로 추출하지만 특정 개인을 확인하지 않고 단순히 화자의 감정상태(화난 목소리, 기쁜 목소리 등)를 알아보기 위해 사용되는 경우는 '일반적인 생체정보'에 해당

나. 생체인식정보의 구분

(1) 생체인식정보는 개인을 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력되는 '생체인식 원본정보(이하 "원본정보")'와 이로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 '생체인식 특징정보(이하 "특징정보")'로 구분

① 원본정보는 생체인식정보를 전자적으로 처리하는 과정에서 유출되거나 오·남용되는 경우 개인정보 침해 위험성이 크므로

- 원본정보의 안전한 보관을 위해 저장 시 암호화, 원본정보를 특징정보 생성 후에도 보관하는 경우 다른 개인정보와 분리 보관 등 별도의 보호조치 필요

※ "Ⅲ. 생체인식정보 보호 조치, 4. 생체인식정보 보관·파기 단계" 참고

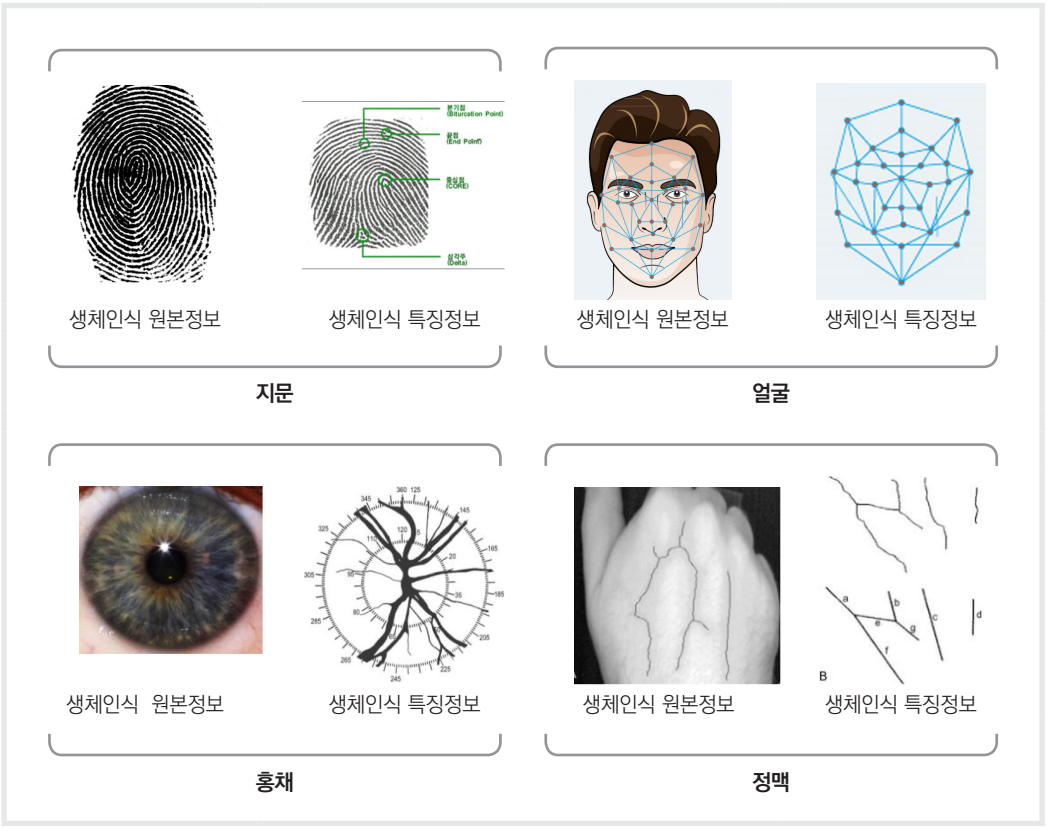
② 특징정보는 「개인정보 보호법 시행령」 제18조제3호*에 따른 민감정보에 해당

* 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보

- 따라서, 민감정보인 특징정보는 「개인정보 보호법」 제23조(민감정보의 처리 제한)가 적용*됨

* 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받거나 또는 법령에서 특징정보의 처리를 요구하거나 허용하는 경우에만 처리 가능

생체인식 원본정보와 생체인식 특징정보 예시



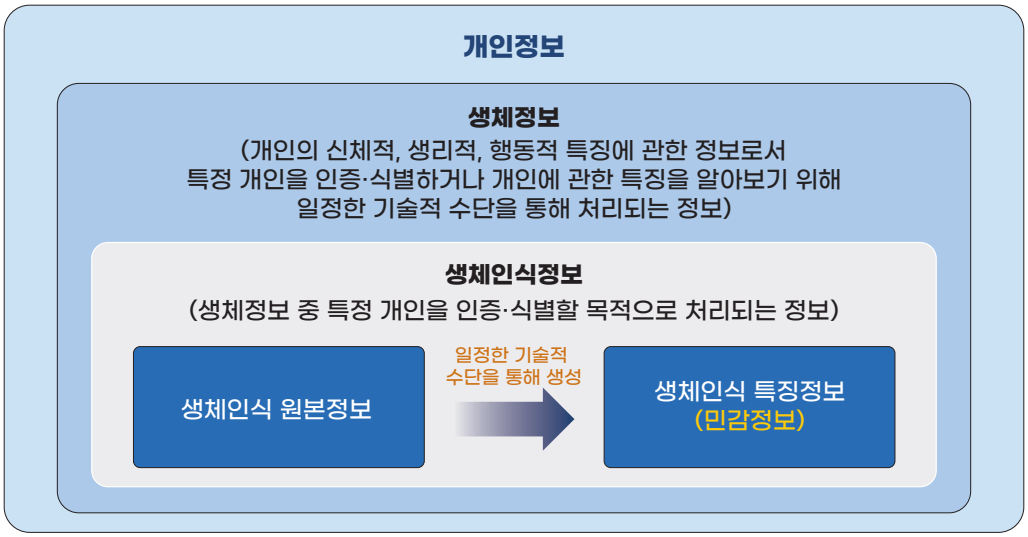
※ 출처 : scienceDirect.com

다. 개인정보, 생체정보, 생체인식정보 간의 관계 및 적용규정

(1) 개인의 신체적, 생리적, 행동적 특징에 관한 정보가 인증·식별 목적 또는 개인에 관한 특징을 알아보기 위해 기술적으로 처리되지 않는다면 일반적인 개인정보에 해당함

※ (예시) 열람·보관 등을 목적으로 수집하는 일반적인 얼굴 사진, 음성파일 등

- 인증·식별 이외의 목적으로 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 기술적으로 처리되는 정보는 일반적인 생체정보에 속하지만, 생체인식정보에는 해당하지 않음



구 분	정 의	
개인정보	그 자체만으로 특정 개인을 알아볼 수 있거나 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보	
생체정보	개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 **특정 개인을 인증·식별하거나 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 일정한 기술적 수단을 통해 처리**되는 정보	
생체인식정보	생체정보 중 **특정 개인을 인증·식별할 목적으로** 일정한 기술적 수단을 통해 처리되는 정보	
	생체인식 원본정보	생체인식정보 중 입력장치 등을 통해 수집·입력된, **특징정보 생성에 이용되는** 정보
	생체인식 특징정보	원본정보로부터 특징점을 추출하는 등의 **일정한 기술적 수단을 통해 생성되는** 정보

(2) 생체인식정보는 본 가이드라인에서 제시하는 보호 원칙과 처리 단계별 생체인식정보 보호 조치 등이 적용됨

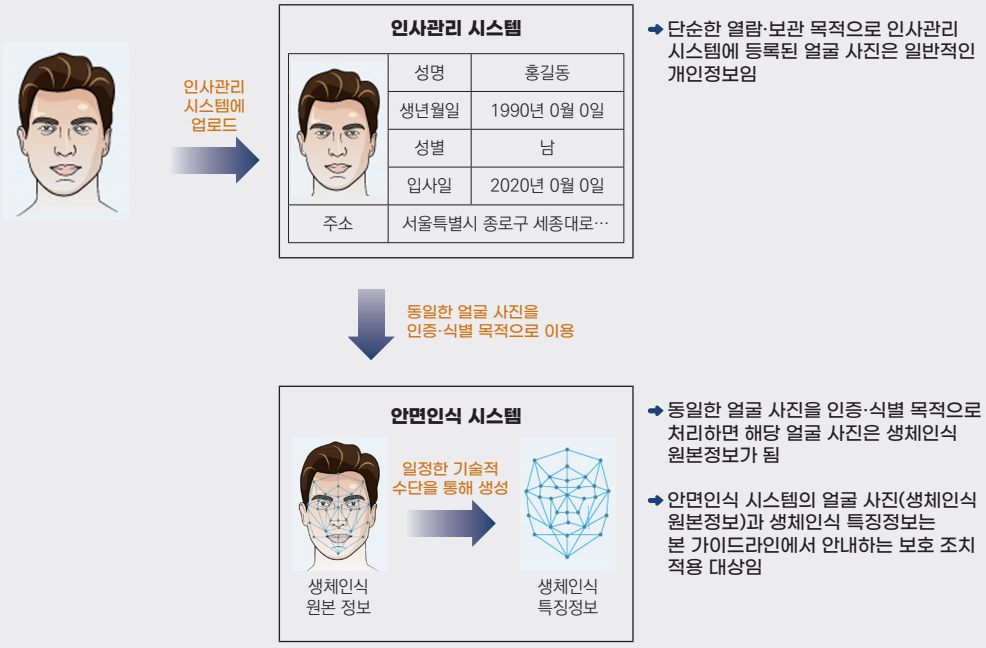
- '일반적인 생체정보'는 생체인식정보에 적용되는 저장 시 암호화, 원본정보 보관 시 분리보관 등이 의무사항은 아니지만,
- 해당 정보가 수집, 전송, 보관 등 처리되는 과정에서 유출되거나 오·남용되는 경우에 예상되는 개인정보 침해 위험성을 고려하여 생체인식정보에 준하는 보호 조치 이행을 권장함

※ "부록 3. 일반적인 생체정보에 권장되는 보호조치" 참고

(3) 일반적인 얼굴 사진·동영상, 음성파일 등을 차후에 인증·식별 목적의 특징정보 생성에 사용하는 경우, 해당 정보는 생체인식정보에 해당하게 되므로 생체인식정보에 적용되는 보호 조치를 이행해야 함

참고 일반적인 개인정보를 특징정보 생성에 사용하는 사례 (예시)

- 카메라로 촬영한 얼굴 사진을 인사관리 목적으로 인사관리 시스템에 등록하는 경우, 해당 얼굴 사진은 일반적인 개인정보임
- 차후에 안면인식 시스템을 도입하면서 얼굴 사진을 이용자로부터 새로 수집하지 않고 인사관리 시스템에 이미 보관되어 있는 얼굴 사진을 특징정보 추출에 사용할 수 있음
  - 이 경우, 얼굴 사진을 수집한 기존의 목적과 다른 목적으로 이용하는 것이므로 특징정보 추출에 사용하기 전에 생체인식정보 수집·이용 동의를 적법하게 받아야 하고,
  - 본 가이드라인에서 안내하는 생체인식정보에 적용되는 보호 조치를 이행하여야 함



4 적용 대상

본 가이드라인은 생체인식정보를 직접 처리하는 개인정보처리자와 생체인식정보 처리 기기를 제조하는 제조사 및 서비스 개발·제공자(이하 '제조사'), 생체인식정보 처리 서비스를 이용하는 정보주체(이하 '이용자')를 대상으로 함

- 개인정보처리자 : 업무 목적으로 개인정보파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 의미
  - ※ 개인정보처리자는 정보통신망법 제2조에서 정의한 정보통신서비스 제공자 포함
  - ※ 지문인식 도어락 등을 사적인 목적(업무 목적 외)으로 설치·운영하는 경우는 개인정보처리자에 해당하지 않음
- 제조사 : 생체인식정보를 처리하는 기기를 제조하거나 생체인식정보 처리 시스템·서비스를 개발하여 고객(개인정보처리자 등)에게 제공하는 법인 등을 의미
  - ※ 생체인식정보를 처리하는 출입통제 기기 제조사, 생체인식정보 처리 시스템을 개발하여 납품하는 개발사, 생체인식정보를 처리하는 스마트폰 제조사 및 OS 사업자, 기기에서 처리된 인증결과 값을 전송받는 사업자 등
- 이용자 : 생체인식정보를 제공하여 출입통제, 스마트폰·앱 로그인, 거래 승인 등 생체인식정보를 처리하는 서비스를 이용하는 정보주체
  - ※ 생체인식정보 활용 출입통제, 복무관리 시스템을 이용하는 임직원, 방문객 및 생체인식정보를 활용하는 스마트폰, 쇼핑·금융 앱 이용자 등

5 법령과의 관계

- 생체정보는 개인정보이므로, 개인정보 보호법, 동법 시행령 및 관련 고시 등이 적용됨
- 다만, 생체정보와 관련하여 다른 법률에 특별한 규정이 있는 경우에는 해당 법률이 적용됨
  - ※ 생체정보 보호와 관련한 법규정이 제·개정되는 경우, 해당 법규정이 가이드라인 보다 우선함

생체인식정보의 특성 및 보호 원칙

1 생체인식정보의 특성

생체인식정보는 유일성·불변성의 특성이 있어 유출 시 피해를 복구하기 어렵고 민감정보가 추출되거나 위·변조되어 악용될 수 있는 특성이 있으므로, 생체인식정보의 이러한 특성을 고려한 특별한 보호 조치 필요

가. 유일성·불변성

- 생체인식정보는 그 자체로 개인을 유일하게 식별할 수 있고 변경이 불가능한 특성으로 인해 한번 유출되면 그 피해를 복구하기 어려움

➜ 따라서 생체인식정보 활용 서비스를 도입하기 전에 생체인식정보 처리에 따른 편익에 비해 개인정보 침해 위험성이 크지 않은지를 고려하여**(비례성 검토)** 해당 서비스 도입 여부를 결정

➜ 생체인식정보 활용 서비스를 도입하는 경우, 서비스 활용 목적에 필요한 최소한의 정보를 **적법하게** 수집 필요

나. 민감정보 추출 가능성

- 원본정보로부터 인종·건강 등 인증·식별 목적과 무관한 민감정보가 추출될 수 있음

  ※ 얼굴, 정맥, 홍채 정보 등으로부터 인종·건강 등 민감한 정보 추출 가능

➜ 생체인식정보는 인증·식별 등 이용자로부터 동의받은 **목적의 범위** 내에서만 이용해야 하고,

➜ 생체인식정보가 처리되는 내용을 이용자에게 **투명하게** 공개해야 함

다. 위·변조 가능성

- 실리콘 인공지문, 캡처된 얼굴·홍채사진 등 위·변조된 생체인식정보를 이용한 해킹 사례가 지속적으로 발생하고 있음

➜ 위·변조된 생체인식정보 입력을 탐지하여 서비스 이용을 거부하는 등 생체인식정보를 **안전하게** 처리하고,

➜ 이용자가 생체인식정보를 스스로 **통제**할 수 있는 수단 제공 필요

2 생체인식정보 보호 원칙

「개인정보 보호법」상의 개인정보보호 원칙(제3조)을 기본으로 생체인식정보의 특성, 개인정보 보호 중심 설계(PbD) 원칙 등을 반영하여 생체인식정보 보호 6대 원칙을 도출

「개인정보 보호법」 상 개인정보보호 원칙	생체인식정보의 특성	개인정보보호 중심설계(PbD)
① 필요 최소한의 정보 수집 및 처리 목적의 명확화 ② 목적 범위 내에서 적법하게 처리, 목적 외 활용금지 ③ 처리목적 내에서 정확성·완전성·최신성 보장 ④ 권리침해 가능성 등을 고려하여 안전하게 관리 ⑤ 개인정보 처리 내역의 공개 및 정보주체의 권리보장 ⑥ 사생활 침해를 최소화하는 방법으로 처리 ⑦ 익명 및 가명 처리의 원칙 ⑧ 개인정보처리자의 책임준수·신뢰확보 노력	① 유일성 ② 불변성 ③ 민감정보 추출 가능성 ④ 위·변조 가능성	① 사후 조치가 아닌 사전 예방 ② 초기 설정부터 프라이버시 보호 조치 ③ 프라이버시 보호를 내재한 설계 ④ 프라이버시 보호와 사업기능의 균형 ⑤ 개인정보 생애주기 전체에 대한 보호 ⑥ 개인정보 처리 과정에 대한 투명성 유지 ⑦ 이용자 프라이버시 존중

생체인식정보 보호 6대 원칙 설명

① 비례성 생체인식정보 처리에 따른 편익에 비해 개인정보 침해 위험성이 크지 않은지를 고려하여 생체인식정보의 활용여부를 판단한다.

② 적법성 생체인식정보의 수집·이용·제공 등 생체정보 처리의 근거는 적법·명확해야 한다.

③ 목적제한 생체인식정보를 정보주체에게 동의 받은 인증·식별 이외의 목적으로 무단으로 활용해서는 안된다.

④ 투명성 생체인식정보 보호에 관한 사항을 정보주체에게 알기 쉽게 공개한다.

⑤ 안전성 생체인식정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전하게 처리하고 관리한다.

⑥ 통제권보장 정보주체가 자신의 생체인식정보를 스스로 통제할 수 있는 수단을 제공한다.

생체인식정보 보호 조치(개인정보처리자 및 제조사)

생체인식정보 보호 조치(총괄표)

1 기획·설계 단계

1. 생체인식정보의 필요성 검토
2. 개인정보보호 중심 설계(PbD) 적용
3. 대체 수단 마련
4. 개인정보 영향평가 수행

2 수집 단계

5. 적법하게 생체인식정보 수집
6. 위·변조된 생체인식정보에 대한 대책 마련
7. 생체인식정보 수집·입력 시 전송구간 보호

3 이용·제공 단계

8. 동의받은 목적의 범위 내 이용
9. 생체인식정보 통제 수단 제공
10. 생체인식정보 수집·입력 단말에서 처리

4 보관·파기 단계

11. 생체인식정보 저장 시 암호화
12. 생체인식정보의 파기
13. 원본정보 보관 시 분리보관

5 상시 점검

14. 개인정보 처리방침 공개
15. 개인정보취급자에 대한 관리·감독

1 기획·설계 단계

- **비례성 원칙을 고려하여 생체인식정보 활용 서비스 도입 여부 판단**
- **기획·설계 단계부터 개인정보보호 중심 설계(PbD) 원칙 적용**
- **이용자가 생체인식정보 제공을 원하지 않거나 제공할 수 없는 상황에 대비하여 생체인식정보 이외의 다른 대체 수단 마련·제공**
- **대량의 생체인식정보를 서버로 전송하여 처리하는 경우, 개인정보 영향평가 수행**

01 생체인식정보의 필요성 검토

권장 비례성

◈ 이용하려는 생체인식정보가 활용 목적상 필요한 정도 및 예상되는 편익에 비해 개인정보 침해 위험성이 크지 않은지를 고려하여 생체인식정보 활용 서비스 도입

- **(서비스 도입 전)** 이용자의 개인정보 침해 위험성을 최소화하면서 처리 목적을 달성할 수 있는 다른 수단이 있는지 검토
- **(도입할 생체인식정보 선택시)** 생체인식정보마다 특성이 다르고, 서비스 형태별로 적합도가 상이하므로, 활용 목적을 달성하면서도 침해 위험성을 최소화할 수 있는 생체인식정보 선택

참고 | 필요성 검토 (예시)

- 스마트폰 앱에서 회원 인증을 위하여 모든 회원의 생체인식정보를 서버로 전송하여 처리한다면 이는 이용하려는 생체인식정보가 필요한 정도에 비해 개인정보 침해 위험성이 큰 것으로 볼 수 있음
  - 단순히 회원을 인증하기 위한 용도라면, 이용자가 소유한 스마트폰 기기 내의 안전한 영역에서 처리된 생체인식정보의 인증 결과 값 등을 전송받는 방법을 권장함
- 스키 리조트에서 시즌권 이용자가 시즌권을 제3자에게 대여하여 부정하게 이용하는 경우를 예방하기 위하여, 기존에 사용하던 인증수단을 생체인식정보 이용 방식으로 변경시 예상되는 경제적·관리적 편익과 개인정보 침해 위험성을 비교·검토하여 도입 여부 판단

02 개인정보보호 중심 설계(PbD) 적용

권장 적법성 안전성 통제권 보장

◈ 생체인식정보 활용 서비스의 기획·설계 단계부터 개인정보보호 중심 설계(PbD*) 원칙을 적용하여 생체인식정보 처리의 모든 과정에서 예상되는 개인정보 침해위험 요인을 사전에 분석하고 예방 조치

* Privacy by Design(PbD) : 제품·서비스 개발 시 기획 단계부터 개인정보 처리의 전체 생애주기에 걸쳐 이용자의 프라이버시를 고려한 정책을 적용하여 설계에 반영하는 것을 의미하며, 국제적으로 광범위하게 통용되는 개인정보보호 원칙임

참고 PbD 원칙 적용 방안 (예시)

■ **PbD 원칙의 적용을 위해 서비스에 필요한 ▲생체인식정보의 유형 및 특성을 분석하고, ▲생체인식정보의 수집·이용 시 법적 근거(동의, 법령 허용 등)와 활용방식(기기 내 처리 등) 결정, ▲생체인식정보의 처리흐름을 사전에 검토하여 생체인식정보 처리에 따른 위험성·침해요인 분석, 대체 수단 마련 등을 순차적으로 수행하여 서비스 전반의 생체인식정보 보호 관련 사항을 검토**

기획·설계 시 사전조치 사항

- **활용하려는 생체인식정보의 유형 및 특성을 분석하여 수집·이용 시 법적근거 검토, '생체인식정보 처리흐름도' 사전 작성**
  - (지문을 이용한 신원확인 서비스의 경우) 수집·이용에 따른 법적근거 사전검토(동의 또는 법령에서 허용), 지문 등록에서부터 인증절차, 보관, 파기에 이르기까지 생체인식정보 처리흐름도 작성을 통한 사전 위험 분석
- **제품·서비스 설정의 기본값(Defaults)은 이용자의 생체인식정보가 보호되는 방향의 값으로 설정**
  - 특징정보 생성 시, 원본정보는 삭제되도록 기본설정 등
- **생체인식정보 유출 및 위·변조에 따른 위험을 최소화하기 위하여 특징정보로부터 원본정보가 쉽게 복원되지 않도록 특징정보 생성 알고리즘을 설계**
- **개인정보취급자(운영자)가 서비스 운영 과정에서 생체인식정보를 안전하게 처리할 수 있도록 서비스 운영지침 및 교육절차 등 마련**
- **개인정보처리자가 생체인식정보 서비스를 위해 시중에 나온 기성 제품을 도입하는 경우, 생체인식정보를 안전하게 보호하는 제품인지 확인하고 도입**

Tip PbD 원칙 적용을 위한 사전위험 분석, 안전성 점검, 법령해석 등을 위해 외부전문가에게 자문을 받거나 전문기관(한국인터넷진흥원 개인정보침해신고센터, ☎118)에 문의 가능

03 대체 수단 마련

권장 | 통제권 보장

◈ 이용자가 생체인식정보 제공을 원하지 않거나, 생체인식정보를 제공할 수 없는 상황*에 대한 대체 수단 마련

* 직업 특성상 지문이 손상되었거나, 부상 등의 사유로 얼굴 인식을 사용할 수 없는 경우 등

- 출입통제, 복무관리 등 물리보안 목적으로 사용되는 경우, 출입카드, 비밀번호 등의 대체 수단 제공 또는 대면확인 절차 마련
- 정보통신서비스를 제공하는 앱의 경우, 핀번호 입력, ARS 인증, 일회용 비밀번호(One-Time Password) 인증 등 지식기반 또는 소유기반의 대체 수단을 동시에 지원하여 이용자가 선택할 수 있도록 허용

참고 | 생체인식정보 대체 수단 (예시)

- IC 카드 기능이 있는 출입카드를 제공
- 키패드를 이용하여 사번과 비밀번호 등을 입력하고 출입
- 신분증 등을 대면 확인 후 출입 허용(필요한 경우 수기명부 등 관리)
- 안면인식의 경우 안면인식기(카메라)가 설치되지 않은 출입구를 별도로 운영
- 아이디/비밀번호, 전자인증서를 이용한 인증
- 스마트폰에 설치하여 사용할 수 있는 모바일 신분증

참고 | 대체 수단 지원 사례

- 빌딩의 보안 관리를 위해 IC카드 기능이 있는 출입카드와 안면인식을 동시에 지원하는 게이트를 설치하여 운영 중에 얼굴정보를 등록하지 않은 이용자가 안면인식기에 자신의 얼굴이 동의없이 촬영되고 이용될 위험성을 지적하여 1개 게이트는 안면인식기를 제거하고 출입카드만 이용하도록 변경하여 운영
- 온라인 쇼핑·금융 앱에서 거래승인 등을 위한 2차 인증수단으로 스마트폰이 지원하는 생체인식정보 기반 인증(지문·홍채·안면인식 등) 이외에 사전에 등록된 핸드폰으로 전송된 인증번호를 입력하여 인증
- 코로나19 이후 지문 또는 정맥을 인식하거나 출입카드를 게이트에 갖다 대면서 발생할 수 있는 접촉을 차단하기 위해 마스크 착용으로 얼굴의 일부만 보여도 인식이 가능한 얼굴인식 기술을 출입통제 시스템에 적용

04 개인정보 영향평가 수행

권장·의무 | 적법성 | 안전성

- 생체인식정보를 서버로 전송하여 대량으로 처리하는 경우, 개인정보 영향평가*를 수행할 것을 권장

> * **개인정보 영향평가**: 개인정보파일의 운용으로 인하여 이용자의 개인정보 침해가 우려되는 경우에 그 위험요인을 분석하고 개선사항을 도출하기 위한 평가(개인정보 보호법 제33조)
>
> ※ 5만 명 이상의 특징정보 처리가 수반되는 개인정보 파일을 운용하는 공공기관 등은 의무 대상

– 개인정보 영향평가를 수행하여 새로운 생체인식정보 활용 서비스 도입 또는 기존 시스템의 중요한 변경사항 발생에 따른 개인정보 침해위험 요인을 사전에 분석하고 보호 대책을 마련

※ 생체인식정보를 중앙의 서버로 전송하여 처리할 경우, 생체인식정보를 수집하는 단말에서 처리하는 경우보다 생체인식정보의 유출 및 오·남용 등의 침해위험이 크므로 개인정보 영향평가 수행을 통한 침해요인 분석 및 개선대책 마련이 필요

- 민간사업자 등 개인정보 영향평가의 의무대상이 아니더라도 생체인식정보를 서버로 전송하여 대량으로 처리하는 경우에는 개인정보 영향평가를 수행할 것을 권장

관련 규정

개인정보 보호법 제33조, 개인정보 보호법 시행령 제35조~제38조, 「개인정보 영향평가에 관한 고시」 등

2 생체인식정보 수집 단계

- 생체인식정보 수집·이용에 대한 동의 절차를 적법하게 이행
- 위·변조된 생체인식정보 수집·입력에 대한 대책 마련
- 생체인식정보 전송시, 해킹 등으로 인해 생체인식정보가 외부에 유출 또는 위·변조되지 않도록 암호화 조치

05 적법하게 생체인식정보 수집

의무 적법성

- 이용자에게 생체인식정보 수집·이용 동의를 받는 경우에는 수집·이용 목적, 수집 항목, 보유·이용기간 등에 관한 내용을 명확히 알려야 함
- 민감정보인 특징정보의 경우에는 다른 개인정보 처리에 대한 동의와 별도 동의가 필요

가. 수집·이용 동의 방법

- 생체인식정보 수집·이용 동의 시 ① 수집·이용 목적, ② 수집 항목, ③ 보유·이용기간, ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용을 명확히 알려야 함

참고 정보통신서비스 제공자의 경우 수집·이용 동의시 고지사항

- 정보통신서비스 제공자의 경우 개인정보보호법 제39조의3(개인정보의 수집·이용 동의 등에 대한 특례) 제1항이 적용되므로 수집·이용 동의 시 필수 고지사항에 **"동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용"**이 포함되지 않으나 이용자 보호를 위하여 해당 사항에 대해서도 명확히 알리고 동의를 받는 것이 바람직

제15조제2항 및 제39조의3제1항에 따른 고지 사항 비교

제15조제2항에 따른 고지 사항	제39조의3제1항에 따른 고지 사항
1. 개인정보의 수집·이용 목적	1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목	2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간	3. 개인정보의 보유·이용 기간
4. 동의 거부권에 대한 사실 및 동의 거부 시 불이익 내용	-

※ 정보통신서비스 제공자 등의 개인정보 처리 등 특례에 관한 자세한 사항은 「개인정보 보호 법령 및 지침·고시 해설」 제6장 참고

- 특징정보의 경우 개인정보 보호법상 민감정보에 해당하므로 다른 개인정보의 처리에 대한 동의와 별도로 수집·이용에 대한 동의*가 필요

  * 「개인정보 보호법」제23조에 따라 다른 개인정보 처리에 대한 동의와 별도 동의 필요. 다만, 법령에서 처리를 요구하거나 허용하는 경우에는 동의없이 처리 가능

- 특징정보 생성 후에도 개인정보처리자의 필요로 원본정보를 보관하는 경우, 원본정보 수집·이용 동의 시 그 목적 및 보유기간 등을 구분하여 안내

  ※ 일반적으로 생체인식정보를 활용한 인증·식별은 특징정보를 비교하여 이루어지며, 이 경우 특징정보가 생성되면 원본정보의 수집·이용 목적이 달성되었으므로 지체 없이 파기가 원칙

  - 이용자가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 서비스의 제공을 거부해서는 아니 되므로
  - 해당 서비스의 본질적 기능 제공을 위해 원본정보의 보관이 반드시 필요한 경우가 아니라면 선택동의 사항으로 수집·이동 동의를 받아야 함

참고 | 생체인식정보 수집·이용 동의서 (예시)

원본정보 수집·이용 동의

항목	목적	보유·이용기간	동의여부
얼굴정보 (원본정보)	**[필수*]** 이용자 식별 및 본인 인증	• **특징정보 생성 시 까지**	☐ 동의함 ☐ 동의안함
	[선택*] 얼굴 인식 알고리즘 연구	• **수집일로부터 1년**	☐ 동의함 ☐ 동의안함

※ 위의 개인정보 처리에 대한 동의를 거부할 권리가 있습니다.
그러나 필수 항목의 동의를 거부할 경우 얼굴정보를 이용한 로그인 기능을 이용할 수 없습니다.

민감정보(특징정보) 처리 동의

항목	목적	보유·이용기간	동의여부
얼굴정보 (특징정보)	이용자 식별 및 본인 인증	• **회원탈퇴 시 까지**	☐ 동의함 ☐ 동의안함

※ 위의 민감정보 처리에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 얼굴정보를 이용한 로그인 기능을 이용할 수 없습니다.

* 필수·선택 동의 여부는 해당 서비스의 특성에 따라 달리 정할 수 있음

참고 | 원본정보 보관시 동의 방식 관련

- 제공하는 서비스의 본질적 기능을 위해 인증·식별 목적으로 수집한 원본정보의 이용이 반드시 필요한 경우는 다른 필수동의 사항과 같이 일괄동의 받는 것도 가능
  - 특정 서비스에서 인증·식별 목적으로 수집한 원본정보를 해당 서비스의 인증·식별 관련된 개선 목적으로 이용하는 것은 당초 수집 목적과 합리적 관련성이 있고, 정보주체의 예측이 가능하며, 정보주체의 이익을 부당하게 침해할 가능성이 낮으므로 특별한 사정이 없는 한 필수동의 사항과 같이 동의받을 수 있음
  - 따라서, 해당 서비스가 아닌 다른 서비스의 개발 및 개선 또는 인증·식별 목적과 합리적 관련성이 없는 기능의 연구·개발 목적 등의 경우에는 필수동의 사항과 같이 일괄동의 받을 수 없음

    ※ (예시) 인공지능 스피커 서비스 이용자로부터 음성인식 로봇 개발에 필요한 음성파일을 수집하는 경우는 선택동의 사항으로 수집·이동 동의를 받아야 함

필수동의 받는 경우 동의서 (예시)

원본정보 수집·이용 동의

항목	목적	보유·이용기간	동의여부
얼굴정보 (원본정보)	**[필수]** • 이용자 식별 및 본인인증 • **본 시스템의 식별 및 인증 성능 개선**	• 특징정보 생성 시까지 **또는 수집일로부터 1년**	☐ 동의함 ☐ 동의안함

※ 위의 개인정보 처리에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 얼굴정보를 이용한 로그인 기능을 이용할 수 없습니다.

본질적 기능을 위해 원본정보의 이용이 반드시 필요한 경우 (예시)

- 인공지능 스피커에서 현재 소프트웨어(v1.0)의 화자인식 성능을 개선하기 위하여(v1.5로 업그레이드) 학습에 필요한 최소한의 원본 음성파일을 보관
- 안면인식 성능 향상 등을 위해 특징값 추출 알고리즘이 변경된 경우, 변경된 알고리즘을 이용하여 특징정보를 재생성하기 위하여 얼굴 이미지를 보관

나. 법령에 별도 근거가 있는 경우

◈ 법령에서 생체인식정보의 처리를 요구하거나 허용하는 경우 이용자의 동의를 받지 않고도 생체인식정보(원본정보 및 특징정보)의 처리 가능

※ 일반적으로 생체인식정보를 활용한 인증·식별은 특징정보 추출이 필요하며, 이 경우 개인정보 보호법 제15조 뿐만 아니라 제23조(민감정보의 처리제한)가 적용됨

법령에서 생체인식정보 처리를 요구·허용하는 경우 (예시)

법 령	내 용
도로교통법 제87조의2 (운전면허증 발급 대상자 본인 확인)	• 지방경찰청장은 운전면허증 발급을 받으려는 사람의 동의를 받아 전자적 방법으로 지문정보를 대조하여 확인할 수 있음
실종아동등의 보호 및 지원에 관한 법률 제7조의2 (실종아동등의 조기발견을 위한 사전신고증 발급 등)	• 경찰청장은 실종아동등의 조속한 발견과 복귀를 위하여 아동등의 보호자가 신청하는 경우 아동등의 지문 및 얼굴 등에 관한 정보를 정보시스템에 등록할 수 있음
여권법 제8조 (여권업무의 수행에 필요한 정보의 수집·보관과 관리)	• 외교부장관은 여권을 발급받는 사람의 지문 등을 수집·보관하고 관리할 수 있음
전자금융거래법 제2조제10호 (정의)	• 이용자의 생체정보는 접근매체 중의 하나에 해당함
주민등록법 제24조 (주민등록증의 발급 등)	• 시장·군수 또는 구청장은 관할 구역에 주민등록이 된 자 중 17세 이상인 자에 대하여 주민등록증을 발급하되, 주민등록증에는 지문을 수록함
출입국관리법 제12조의2 (입국시 생체정보의 제공 등)	• 입국하려는 외국인은 입국심사를 받을 때 생체정보를 제공하고 본인임을 확인하는 절차를 응해야 함
출입국관리법 제28조 (출국심사)	• 출입국관리공무원은 외국인으로부터 제공 또는 제출받은 생체정보를 출국심사에 활용할 수 있음
항공보안법 제14조의2 (생체정보를 활용한 본인 일치 여부 확인)	• 공항운영자 및 항공운송사업자는 관계 행정기관이 보유하고 있는 생체정보를 이용할 수 있음
형의 집행 및 수용자의 처우에 관한 법률 제19조 (사진촬영 등)	• 소장은 신입자 및 다른 교정시설로부터 이송되어 온 사람에 대하여 지문채취를 하여야 함
검찰사건사무규칙 제15조 (수사관계사항의 조회)	• 검사가 사건을 인지한 때에는 피의자의 지문을 채취하여 수사자료표송부서에 의하여 지문대조조회를 하여야 함
경찰공무원임용령 시행규칙 제39조 (응시서류의 제출 등)	• 경찰공무원 공개경쟁채용시험 또는 경찰간부후보생 공개경쟁선발시험에 응시하려는 사람은 지문대조표 1통을 의무적으로 제출해야 함

※ 법령에 근거하여 생체인식정보를 이용자의 동의 없이 처리하는 국가기관·공공기관 등의 경우 생체인식정보가 해당 법령이 허용하는 목적의 범위 내에서 이용되고 있는지 확인·관리 필요

참고 | 개인정보 보호법 제15조 및 제23조 적용 관련 유의사항

- **(제15조)** 생체인식정보는 개인정보의 한 유형이므로 수집·이용 시 개인정보 보호법 제15조를 적용 받음
  - 따라서, 제15조제1항의 제2호 후단, 제3호~제6호에 따라 법령상 의무를 준수하기 위하여 불가피한 경우나 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 등에 해당하는 경우 이용자의 동의 없이 개인정보의 수집·이용이 가능함
- **(제23조)** 다만, 일반적으로 생체인식정보를 활용한 인증 및 식별 서비스에서는 특징정보의 추출이 필요하므로 개인정보 보호법상 민감정보에 해당하는 특징정보의 처리를 위해서는 개인정보 보호법 제23조제1항에 따라 이용자에게 별도 동의를 받거나 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에만 처리가 가능함을 유의

개인정보 보호법 제15조, 제23조

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우.

제23조(민감정보의 처리 제한) ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

관련 규정

개인정보 보호법 제15조, 제16조, 제17조, 제22조, 제23조, 제39조의3,
개인정보 보호법 시행령 제18조 등

06 위·변조된 생체인식정보에 대한 대책 마련

권장 안전성

◆ 센서 등의 장치를 통해 생체인식정보가 수집·입력될 때, 실리콘 인공지문, 캡처된 얼굴·홍채사진, 녹음된 음성 등 위·변조된 생체인식정보를 이용한 공격에 대한 보안대책 마련

- **(위·변조 탐지)** 온도·맥박 감지, 위·변조를 탐지하는 알고리즘 적용 등 위·변조된 생체인식정보를 탐지하는 기술 적용

참고 | 위·변조된 생체인식정보 탐지 기술 (예시)

- 하드웨어 방식 : 인체 피부의 온도 측정, 빛을 흡수·반사·투과·감쇠하는 특성 이용, 손가락 끝의 맥박을 측정, 피부에 흐르는 전기 저항을 측정하는 등 위·변조된 생체인식정보를 감지하는 하드웨어를 추가하여 탐지
- 소프트웨어 방식 : 별도의 하드웨어 없이 센서에서 수집한 영상을 이용하여 위·변조 탐지
  - 위조된 생체인식정보 영상은 실제 인체로부터 수집한 정보 대비 품질이 떨어지는 특성을 이용하여 영상의 밝기, 전경의 윤곽, 융선 등의 명확도 등을 분석하는 알고리즘 적용

※ 위·변조 탐지 기술 적용에 관해서는 「생체인식 제시형 공격 탐지 제1부 프레임워크, KS X ISO/IEC 30107-1」('18년 4월 제정) KS 국가 표준 참고, 「위조 바이오인식 방어력 성능 시험·평가 해설서」(한국인터넷진흥원, '21.6월) 참고

- **(다중 인증)** 생체인식정보 입력시 핀 번호 입력, ARS 인증, 일회용 비밀번호(One-Time Password) 인증 등 지식·소유 기반의 인증수단을 추가로 적용

참고 | 위·변조된 생체인식정보 이용 사례

- 모 부대 소속 군의관들이 실리콘으로 위조지문을 제작하여 출퇴근 확인용 지문인식기에 서로 대신 인식시켜주는 방법으로 담당 지휘관의 직무를 방해하고 초과근무 수당을 수령('19.3)
- 3D 프린터를 이용한 실리콘 위조지문으로 주민센터에서 인감증명서 등 필요서류를 발급받아 50억대 부동산을 불법으로 명의 이전('14.10)
- 독일의 해커단체는 구글 검색을 통해 러시아 대통령 푸틴의 고해상도 사진을 출력하여 홍채 복제가 가능함을 시연('14.4)

07 생체인식정보 수집·입력 시 전송구간 보호

의무 안전성

- 생체인식정보를 정보통신망을 통하여 전송하거나 보조저장매체 등을 통하여 전달하는 경우, 인가되지 않은 접근, 해킹 등으로 인한 유출, 위·변조 가능성 등을 방지하기 위하여 안전한 알고리즘으로 암호화
  - 공공기관은 국가정보원의 검증대상 암호 알고리즘을 적용, 민간부분(법인·단체·개인)은 국내·외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)이 권고하는 암호 알고리즘을 적용

참고 | 안전한 암호 알고리즘 (예시), '18.12월 기준

구분	공공기관	민간부문 (법인·단체·개인)
대칭키 암호 알고리즘	SEED, LEA, HIGHT, ARIA	SEED HIGHT ARIA-128/192/256 AES-128/192/256 Camelia-128/192/256
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 Whirlpool 등

- 생체인식정보를 처리하는 기술적·환경적 여건에 따라 다르나, 일반적으로 응용프로그램 자체 암호화 방식, SSL/TLS 방식, VPN 방식 등 중 적합한 방식 적용 가능

※ 암호화 알고리즘, 수행방식, 사례 등은 개인정보보호위원회·한국인터넷진흥원의 「개인정보의 암호화 조치 안내서('20. 12월)」 및 암호이용 활성화(https://seed.kisa.or.kr/) 홈페이지 참고

관련 규정

「개인정보의 안전성 확보조치 기준」 제7조제1항,
「개인정보의 기술적·관리적 보호조치 기준」 제6조제3항 등

3 생체인식정보 이용·제공 단계

- **이용자로부터 동의받은 목적의 범위 내에서 생체인식정보 이용**
- **이용자가 생체인식정보를 열람하거나 정정·삭제할 수 있는 통제 수단 제공**
- **생체인식정보는 서버로 전송·처리하는 대신 가능하다면 생체인식정보를 수집·입력하는 단말의 안전한 영역에서 처리**

08 동의받은 목적의 범위 내 이용

의무 목적 제한

◈ 인증 또는 식별 목적으로 이용자에게 동의받은 생체인식정보는 무단으로 인사관리, 연구·개발 등 다른 목적으로 활용 불가

– 특히, 원본정보로부터 인종·건강상태 등 인증·식별 목적과는 무관한 민감정보가 추출·수집·이용되지 않도록 관리 필요

◈ 생체인식정보를 인증 또는 식별 이외의 목적으로 활용하기 위해서는 일반 개인정보로서 이용자의 사전 동의 등 적법한 절차 준수 필요

– 개인정보 수집·이용 동의 시 생체인식정보를 인증 또는 식별 이외로 이용하는 목적 및 보유기간 등을 고지하고 동의* 받아야 함

* 단, 법령에서 처리를 요구하거나 허용하는 경우에는 동의없이 처리 가능

참고 인증·식별 외 목적으로 이용 사례

- 출입 시 본인 여부를 사후 증빙하기 위하여 안면인식을 목적으로 입력한 얼굴의 원본 사진을 서버에 보관
- 안면인식 목적으로 등록한 얼굴 사진을 인사관리, 신분증 발급 등에 활용
- 이용자가 SNS에 올린 사진에서 특정 개인을 식별하여 친구태그를 추천하는 기능은 얼굴정보가 생체인식정보로서 활용되는 동시에 개인정보로서 활용되는 것임

법령에서 생체인식정보의 처리를 요구하거나 허용하는 경우라도 해당 법령에서 허용하는 목적 범위 내에서만 이용 가능

- 국가기관, 공공기관 등에서 생체인식정보를 이용자의 동의 없이 처리하는 경우,
  - ⅰ) 법령상의 처리 근거를 명확히 확인하고
  - ⅱ) 생체인식정보가 해당 법령이 허용하는 목적의 범위 내에서 이용되고 있는지 실태점검 등을 통해 확인·관리 필요

참고 | 국가기관의 생체인식정보 이용 관련 해외 사례

- 유럽연합(EU)의 집행위원회는 AI 규제안을 제시하면서 금지되는 AI에 '공공 장소에서 법집행을 목적으로 하는 실시간 원격 생체 인식 시스템으로서 특정 목적 중 하나에 대한 엄격한 필요성이 인정되지 않는 경우'를 포함('21.4월)
- 일리노이주 상원은 연방 이민법 집행 등을 명분 삼아 안면인식 기술이 반헌법적으로 활용될 수 있다는 우려를 반영하여 여타 주나 연방의 이민 당국이 일리노이주 거주자의 생체 데이터에 접근하는 것을 크게 제한하는 결의안을 통과('21.4월)
- 영국 항소법원은 경찰이 사용 중인 자동 안면인식 기술에 대한 소송에서 경찰의 안면인식 기술 사용이 인권과 정보보호법에 위반한다고 판결. 특히 경찰이 너무 많은 재량권을 갖고 있고, 기술 사용에 있어 명백한 지침 역시 갖고 있지 않다고 지적('20.8월)
- 미국 민주당이 연방법 집행기관의 안면인식 기술 사용을 금지하는 '안면인식 및 바이오인식 기술 모라토리엄 법' 안을 발의 ('20.6월)

관련 규정

개인정보 보호법 제18조, 개인정보 보호법 시행령 제15조 등

09 생체인식정보 통제 수단 제공

의무 | 통제권 보장

- 개인정보처리자는 이용자가 자신의 생체인식정보 제공과 이용을 스스로 결정할 수 있도록 생체인식정보의 열람·정정·삭제 등의 통제 수단 제공
  - 이용자 보유 기기 또는 개인정보처리자가 제공하는 서비스 앱·웹 등에서 생체인식정보 통제 기능을 지원하고 쉽게 이용할 수 있도록 안내

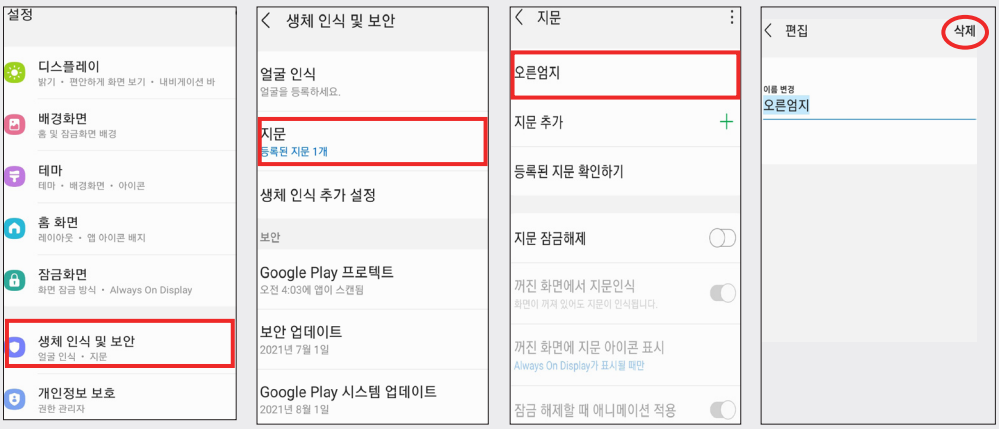
가. 이용자 보유 기기에서 통제 방법

- 생체인식정보를 처리하는 기기 제조사 또는 OS사업자는 이용자가 해당 기기 또는 웹·앱 등을 통해 생체인식정보를 수정하거나, 삭제할 수 있도록 통제 수단을 제공

참고 | 통제방법 예시 : 안드로이드폰

① 설정 → ② 생체인식 및 보안 → ③ 지문 → ④ 생체인식정보 수정·삭제

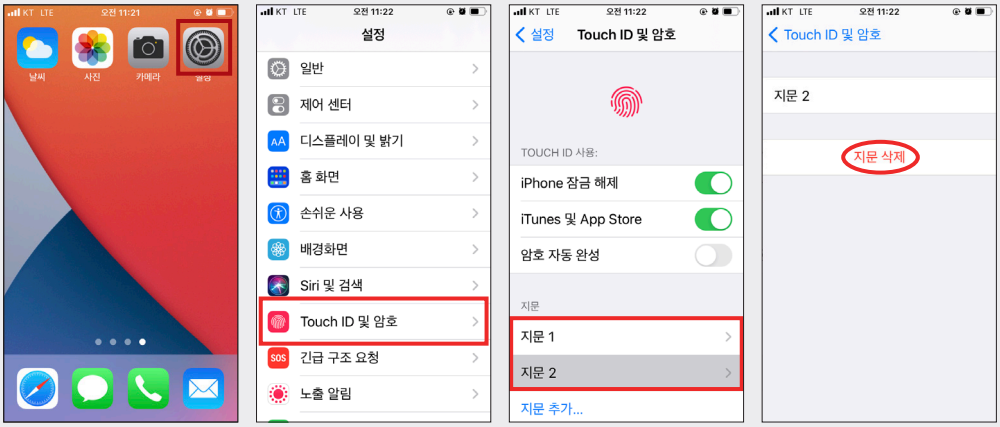
설정 방법 (Android 11 버전 기준)



참고 통제방법 예시 : 아이폰

① 설정 → ② Touch ID 및 암호 → ③ 생체인식정보 수정·삭제

설정 방법 (iOS 14 버전 기준)

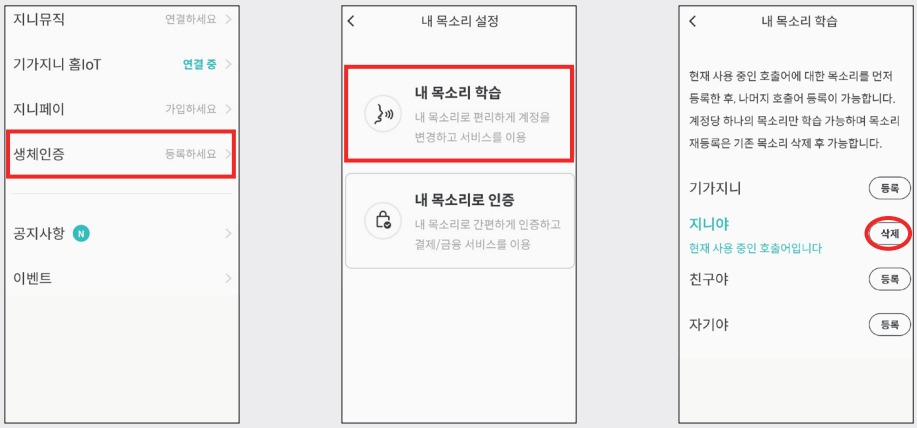


- AI 스피커 등과 같이 기기에서 직접적인 통제권 행사가 어려운 경우, 웹페이지 또는 앱 등을 통해 통제 수단 제공

참고 통제방법 예시 : 기가지니(AI 스피커)

① 생체인증 → ② 내 목소리 학습 → ③ 생체인식정보 수정·삭제

설정 방법



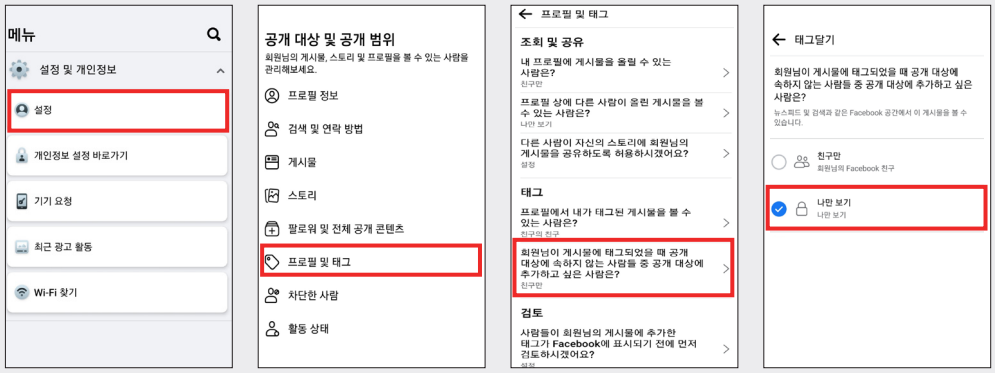
나. 서비스 앱 또는 웹에서 통제 방법

- 생체인식정보를 개인정보처리자가 직접 수집하거나 사진, 음성 등과 같이 이미 수집된 개인정보를 생체인식정보로 활용하는 경우, 해당 서비스에서 이용자가 직접 통제할 수 있는 수단을 제공

참고 통제방법 예시 : 페이스북 태그추천 기능

① 설정 및 개인정보 → ② 설정 → ③ 프로필 및 태그 → ④ 친구태그 공개 대상 변경

설정 방법



- 생체인식정보를 직접 수집하지 않고 스마트폰 등 기기 내에서 처리된 인증 결과 값 등을 전송받는 경우, 해지 메뉴 등을 통해 이용자가 생체인식정보를 통제하는 방법 제공

참고 생체인식정보 통제 방법 안내 예시

▶ OO 생체인증 서비스는 이용자 스마트폰에 등록된 생체인식정보를 이용한 본인 인증 서비스입니다. 당사는 이용자의 생체인식정보를 서버로 전송하지 않으며, 스마트폰에 등록된 생체인식정보와 대조한 결과 값만을 전송받아 본인인증을 진행합니다.

▶ OO 생체인증 서비스의 해지를 원하실 경우 아래 메뉴를 통해 설정해 주시기 바랍니다.

OO 생체인증 서비스 설정

사용	해지
√	√

관련 규정

개인정보 보호법 제35조, 제36조, 제37조, 제39조의7 등

10 생체인식정보 수집·입력 단말에서 처리

권장 안전성

생체인식정보를 서버로 전송하여 처리할 경우 침해사고 발생 시, 대규모 생체인식정보 유출 등 피해 범위가 커질 우려가 있으므로

- 생체인식정보를 수집·입력하는 기기 내 안전한 영역 또는 보안토큰, 스마트카드 등 이용자가 직접 소지할 수 있는 매체에서 생체인식정보를 저장·처리하는 방식을 우선적으로 고려 필요

※ 기기 및 보조저장매체 등에 저장할 경우, 생체인식정보를 암호화해야 함

참고 기기 내 안전한 영역

- OS가 지원하는 신뢰 실행 환경(TEE), 신뢰 플랫폼 모듈(TPM) 등이 제공하는 저장공간
  - 안전한 영역에 생체인식정보를 저장하거나, 안전한 영역에 비밀키를 저장하고, 해당 비밀키를 이용해 생체인식정보를 암호화하여 기기·앱의 저장소에 저장

    ※ Android 기기의 경우 키스토어(KeyStore), TrustZone 등을 활용,
    iOS 기기의 경우 키체인(KeyChain)을 활용 가능

참고 서버에 보관된 생체인식정보 유출 사례

- 이스라엘의 보안 전문가가 생체인식정보 관련 제조사의 '보안설정이 잘못되어 인터넷에 노출된 서버'에서 암호화되지 않은 사용자 이름, 비밀번호, 지문, 안면정보 등을 발견('19.8)
- 해커집단의 APT공격에 의해 미국 연방부처의 DB가 해킹되어 미국 전·현직 공무원의 개인정보 2,200만 건 및 지문정보 560만 건 유출('15.6)

4 생체인식정보 보관·파기 단계

- 생체인식정보의 보관 시 안전한 알고리즘으로 암호화하여 저장
- 특징정보가 생성된 경우, 원본정보는 그 목적이 달성된 것으로 볼 수 있으므로 지체 없이 복구 또는 재생되지 않도록 파기하는 것이 원칙
- 법적 근거가 있거나 이용자의 동의를 받아 원본정보를 보관하는 경우, 해당 이용자의 다른 개인정보와 분리하여 저장·관리

11 생체인식정보 저장 시 암호화 의무 안전성

◈ 생체인식정보 보관 시, 제3자에 의한 위·변조, 유출 등의 침해 방지를 위하여 안전한 알고리즘으로 생체인식정보(원본정보 및 특징정보 포함)를 암호화하여 저장

- 원본정보는 변경이 불가능하고 원본정보로부터 인종·건강 등 다른 민감정보가 추출될 수 있는 등의 사생활 침해 우려가 있으며,
- 특징정보는 유출 시 인증·식별 목적으로 악용될 수 있으므로 암호화 조치 필수

※ 암호화 알고리즘, 수행방식, 사례 등은 개인정보보호위원회·한국인터넷진흥원의 「개인정보의 암호화 조치 안내서('20.12월)」 및 암호이용 활성화 홈페이지(https://seed.kisa.or.kr/) 참고

◈ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키의 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

- 암호키 생성에 필요한 난수는 안전한 난수발생기를 이용하여 생성
- 생성된 암호키는 노출되지 않도록 안전하게 보관하고, 하드웨어 손상 또는 소프트웨어 오류 등으로 인해 소실되지 않도록 별도 장치에 백업

관련 규정

「개인정보의 안전성 확보조치 기준」 제7조제2항, 제7조제5항,
「개인정보의 기술적·관리적 보호조치 기준」 제6조제2항 등

12 생체인식정보의 파기

의무 안전성

- 이용자로부터 동의받은 보유·이용 기간 경과, 개인정보의 처리 목적 달성 등 생체인식정보가 불필요하게 되었을 때, 해당 생체인식정보를 지체 없이 파기*

  * 복원이 불가능한 방법으로 영구삭제

  – 일반적으로 특징정보가 생성되면 원본정보의 수집·이용 목적이 달성된 것이므로, 원본정보는 특징정보 생성 시 지체없이 파기하는 것이 원칙

※ 이용자로부터 동의를 받거나 다른 법령에 근거가 있는 경우에는 원본정보 보관·이용 가능

참고 | 목적 달성 이후에도 생체인식정보 보유 사례 (예시)

- A 스키장은 시즌권 보유자의 본인인증용 정맥정보를 전자상거래법 제6조 및 동법 시행령 제6조에 따라 5년간 보존해야 하는 '계약 또는 청약철회 등에 관한 기록'으로 보고 정맥정보의 보유·이용 기간을 5년으로 지정

  ➜ 시즌권 보유자의 본인인증용 정맥정보는 시즌이 종료되면 처리 목적을 달성하였으므로 지체 없이 파기하여야 함

관련 규정

개인정보 보호법 제21조, 개인정보 보호법 시행령 제16조, 「개인정보의 안전성 확보조치 기준」 제13조 등

13 원본정보 보관 시 분리보관

권장 안전성

- 특징정보 생성시 원본정보를 파기하지 않고 보관하는 경우, 원본정보 유출에 따른 피해를 최소화하기 위하여 원본정보는 해당 이용자의 다른 개인정보와 분리하여 별도로 저장·관리 권장
  - 물리적으로 분리하여 보관하는 것을 원칙으로 하고, 불가피한 경우 물리적 분리와 대등한 수준으로 논리적으로 분리하여 보관 가능
  - 분리 보관된 원본정보에 대한 접근권한을 최소화하고 접근 통제 및 외부 해킹방지 등의 보호조치 이행
  - 이용자의 원본정보와 다른 개인정보를 연결하는 공통 식별자는 임의 값을 활용하여 직접적으로 해당 이용자가 식별되지 않도록 조치

➜ 원본정보를 대량으로 보관·이용하는 국가기관·공공기관 등의 개인정보처리자는 원본정보 유출시 피해가 더 클 수 있으므로 분리보관을 필수로 적용하는 것을 적극 권장함

참고 | 국가기관·공공기관을 위한 권장사항

- 법령에 근거하여 처리하는 경우
  1. 법령상의 처리 근거를 명확히 확인
  2. 생체인식정보가 해당 법령이 허용하는 목적의 범위 내에서 이용되고 있는지 실태점검 등을 통해 확인·관리
  3. 개인정보 처리방침 등을 통해 생체인식정보의 수집·이용에 관한 사항을 명확히 안내
  4. 법령에 따른 의무사항이 아니지만, 가능한 경우 생체인식정보 수집·이동 동의 절차 이행
  5. 생체인식정보 보호를 위한 체계적인 절차, 내부 지침 등을 마련·운영

     ※ A기관은 지문관리체계에 국제표준 기록경영시스템(ISO 30301 인증)을 도입하여 지문관리 업무과정의 책임성과 투명성을 높임('20.11월)

- 원본정보를 대량으로 보관·이용하는 경우
  1. 원본정보 유출시 피해가 더 클 수 있으므로 분리보관을 필수로 적용
  2. 그 밖에 본 가이드라인에서 권장하는 생체인식정보 보호 조치 이행

     ※ ① 생체인식정보의 필요성 검토, ② 개인정보보호 중심 설계(PbD) 적용, ③ 대체 수단 마련, ⑥ 위·변조된 생체인식정보에 대한 대책 마련, ⑩ 생체인식정보 수집·입력 단말에서 처리

➜ 원본정보를 대량으로 처리하는 국가기관·공공기관 등은 위의 보호 조치 이행을 위한 예산 반영 및 주기적인 확인·점검을 통한 관리체계 마련 등 적극적인 노력이 필요

5 상시 점검

- 생체인식정보의 수집·이용에 관한 사항을 개인정보 처리방침 등을 통해 명확히 안내
- 생체인식정보를 직접 처리하는 개인정보취급자 및 수탁자에 대한 관리·감독 및 교육 이행

14 개인정보 처리방침 공개 의무 투명성

◈ 개인정보 처리방침을 통해 이용자에게 수집·이용하는 생체인식정보의 이용목적, 항목, 보유·이용기간, 이용자의 통제권 행사 방법 등을 명확하게 안내해야 하고, 이용자가 언제든지 이를 확인할 수 있도록 해야 함

참고 개인정보 처리방침의 의무수록 사항(법 제30조 및 시행령 제31조)

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보의 파기절차 및 파기방법(법 제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
5. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
6. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
7. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
8. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
9. 처리하는 개인정보의 항목
10. 영 제30조 또는 제48조의2에 따른 개인정보의 안전성 확보 조치에 관한 사항

– 개인정보 처리방침은 이용자가 쉽게 확인할 수 있도록 홈페이지 게시 등의 방법으로 공개

※ 인터넷 홈페이지에 게재할 수 없는 경우에는 개인정보처리자 사무소 등의 보기 쉬운 장소에 게시하거나, 연 2회 이상 발행하는 간행물·소식지·홍보지·청구서 등에 지속적으로 싣거나 계약서 등에 실어 이용자에게 발급도 가능

관련 규정

개인정보 보호법 제30조, 개인정보 보호법 시행령 제31조 등
개인정보 처리방침 작성방법 및 예시는 「개인정보 처리방침 작성 가이드라인」 참고

15 개인정보취급자에 대한 관리·감독 의무 투명성 안전성

◈ 생체인식정보 활용 서비스 개발·운영에 참여하는 개인정보취급자에 대한 관리·감독 및 정기적인 교육 실시

- 개인정보처리자는 개인정보 보호책임자를 지정하고, 생체인식정보가 안전하게 처리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보취급자*에 대한 적절한 관리·감독 이행

  * 생체인식정보를 출입통제 등의 목적으로 이용하는 경우, 생체인식정보의 등록·삭제 등의 업무를 수행하는 보안부서 실무자 등 포함

- 생체인식정보의 안전한 처리를 보장하기 위해 개인정보를 직접 다루는 개인정보취급자에게 정기적인 교육 실시

관련 규정

개인정보 보호법 제28조, 개인정보 보호법 시행령 제32조, 「표준 개인정보 보호지침 제15조」 등

Ⅳ 안전한 이용환경 조성(제조사의 역할)

이용자의 생체인식정보를 수집·이용하는 자는 개인정보처리자이나 개인정보처리자가 생체인식 정보를 안전하게 이용할 수 있는 환경 조성을 위해서는 제조사의 역할이 중요

1 제조사 역할의 중요성

- 개인정보 보호 법령에 따라 생체인식정보를 안전하게 처리할 책임과 의무는 개인정보처리자에게 있으나
  - 생체인식정보의 안전한 관리를 위한 기술적·관리적 보호조치 등은 일반적으로 제조사의 시스템 개발 및 기능 설정에 따라 큰 영향을 받으므로 개인정보처리자의 안전한 생체인식정보 처리를 위해서는 제조사의 역할이 중요

- 제조사는 제품·서비스의 기획·설계 및 개발 단계에서 생체인식정보의 전송·저장시 암호화, 안전한 파기 등 생체인식정보의 안전성 확보에 필요한 기술적·관리적 보호 조치 등을 제품·서비스에 적용

- 제품·서비스를 도입하여 운영하는 개인정보처리자 및 개인이 생체인식정보 처리시스템을 안전하게 관리·운영하는데 필요한 관리 기능을 제공하고 그 이용 방법을 안내

2 안전한 제품·서비스 개발

- 기획·설계 단계부터 개인정보보호 중심 설계(PbD) 원칙을 적용하고 본 가이드라인에서 안내하는 생체인식정보의 안전성 확보에 필요한 기술적·관리적 보호 조치 등을 제품·서비스에 적용
  - 국내외 생체인식정보 보호 관련 표준*을 참고하여 국제적으로 경쟁력 있는 안전한 제품·서비스 개발

    * 「Information security, cybersecurity and privacy protection – Biometric information protection, ISO/IEC 24745:2011」('21.6월), 「생체인식 제시형 공격 탐지 제1부 프레임워크, KS X ISO/IEC 30107-1」('18.4월) 등 참고

(생체인식정보 수집장치 제조사) 지문인식 센서 등 생체인식정보를 이용자로부터 직접 수집하여 특징정보를 추출하는 장치를 제조하는 경우,

- 생체인식정보 유출 및 위·변조에 따른 위험을 최소화하기 위하여 특징정보로부터 원본정보가 쉽게 복원되지 않도록 특징정보 생성 알고리즘을 설계

> **관련 내용** Ⅲ. 생체인식정보 보호 조치, ② 개인정보보호 중심 설계(PbD) 적용

- 원본정보 수집 시 실리콘 인공지문, 캡처된 얼굴·홍채사진, 녹음된 음성 등 위·변조된 생체인식정보를 이용한 공격에 대한 보안대책 마련

> **관련 내용** Ⅲ. 생체인식정보 보호 조치, ⑥ 위·변조된 생체인식정보에 대한 대책 마련

- 고객의 요청 등 특별한 사정이 없다면 원본정보는 특징정보가 생성되면 지체없이 파기하여 원본정보 유출에 따른 개인정보 침해위험 예방

> **관련 내용** Ⅲ. 생체인식정보 보호 조치, ⑫ 생체인식정보의 파기

(생체인식정보 처리 시스템·서비스 제조사) 출입통제·복무관리 시스템 등 생체인식정보를 이용하여 이용자를 인증한 후 특정 서비스를 제공하는 정보처리시스템 제조사, 쇼핑·금융 앱 등 이용자 대상의 온라인 서비스 개발사 등의 경우,

- 전송 및 보관 과정에서 생체인식정보가 유출 및 위·변조되지 않도록 안전한 알고리즘으로 암호화하고 암호키를 안전하게 관리

> **관련 내용** Ⅲ. 생체인식정보 보호 조치, ⑦ 생체인식정보 수집·입력 시 전송구간 보호, ⑪ 생체인식정보 저장 시 암호화

- 원본정보는 특징정보가 생성되면 지체없이 파기하는 것이 원칙이며, 이용자로부터 동의를 받거나 법령에 근거가 있어 원본정보를 파기하지 않고 보관하는 경우 다른 개인정보와 분리하여 보관하도록 설계·제조

> **관련 내용** Ⅲ. 생체인식정보 보호 조치, ⑬ 원본정보 보관 시 분리보관

- 쇼핑·금융 앱 등 온라인 서비스인 경우, 이용자가 자신의 생체인식정보 제공과 이용을 스스로 결정할 수 있도록 생체인식정보의 열람·정정·삭제 등의 통제 수단 제공

관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑨ 생체인식정보 통제 수단 제공

- 일반적으로 개인정보 처리시스템에 요구되는 접근 권한 관리, 접근 통제, 접속기록 관리 등 기술적·관리적 보호 조치에 필요한 기능 지원

※「개발자 대상 개인정보 보호조치 적용 안내서」(개인정보보호위원회, '20.12월) 참고

- 본 가이드라인에 소개된 내용 이외에도 생체인식정보가 유출·변조·훼손되지 않도록 추가적으로 소프트웨어 개발보안(시큐어코딩)* 적용, 보안 취약점 점검** 등을 통해 보안 강화 조치 이행 권장

* 「소프트웨어 개발보안 가이드」(행정안전부, '19.11월) 참고
** 「소프트웨어 보안약점 진단가이드」(행정안전부, '19.6월), 「바이오인식 정보의 보호를 위한 기술적·관리적 지침 KS X 1966:2018」('18.4월) 등 참고

3 개인정보처리자 관련 안내사항

- 생체인식정보를 안전하게 처리하기 위해 제품·서비스를 관리·운영하는 방법을 제품 설치 설명서, 사용 설명서, 교육 등을 통해 개인정보처리자에게 안내

※ 현관문에 설치된 지문인식 도어락 등 생체인식정보를 업무 목적으로 이용하지 않는 (개인정보처리자가 아닌) 일반 이용자에게도 안내 필요

참고 주요 안내사항 (예시)

- 기기 도입 시 안전한 키 생성 등 초기 설정 방법
- 목적 달성 시 생체인식정보 삭제 및 안전한 데이터 백업 방법
- 고객이 개인정보처리자인 경우, 생체인식정보 수집·이용 동의 필요사항 안내
- 생체인식정보 처리 기기 폐기 시, 기기에 보관된 생체인식정보의 안전한 파기 방법 안내

Ⅴ 생체인식정보 활용 서비스 이용안내(이용자)

이용자가 생체인식정보 활용 서비스를 이용하기 전에 사전확인을 위해 알아두어야 할 사항과 생체인식정보 활용 서비스를 안전하게 이용하기 위한 구체적인 이용 방법과 주의사항 등을 안내함

1 사전확인

1 생체인식정보를 자신이 통제할 수 있는 서비스인지 확인

- 서비스 이용 전 생체인식정보를 본인의 스마트폰이나 보안토큰, 스마트카드 등 본인이 직접 소지할 수 있는 매체에 저장·처리하는 서비스 방식인지 여부를 확인
  - 생체인식정보를 서버로 전송하여 처리하는 서비스의 경우 침해사고 발생 시 대규모 생체인식정보 유출로 피해가 커질 우려가 있으므로
  - 생체인식정보를 본인이 소지하여 통제할 수 있는 경우보다 개인정보 처리방침 및 이용약관을 면밀히 검토하고 본인의 생체인식정보에 대한 통제권을 적극적으로 행사하는 등 서비스 이용 시 주의 필요

2 적절한 대체 수단 요구

- 생체인식정보 제공을 원하지 않거나 본인이 제시하기 어려운 특정한 생체인식정보만을 요구하여 서비스 혜택을 받을 수 없는 경우에는 다른 생체인식정보 또는 적절한 대체 수단을 요구할 수 있음
  - 출입통제, 복무관리 등 물리보안 서비스인 경우, 출입카드, 비밀번호 등의 대체 수단 또는 대면확인 절차 마련 등을 요구할 수 있음
  - 정보통신서비스를 제공하는 앱의 경우, 서비스 제공자가 지원하는 핀 번호 입력, ARS 인증, 일회용 비밀번호(One-Time Password) 인증 등 생체인증 서비스 이외의 대체 수단을 선택

관련 내용 Ⅲ. 생체인식정보 보호 조치, ③ 대체 수단 마련

3 적법하게 수집·이용 동의를 받는지 확인

개인정보처리자가 생체인식정보 수집·이용 동의를 적법하게 받는지 확인

- 서비스 제공을 위해 필요한 최소한의 정보 외에 과도한 수집·이용 동의를 요구하고 있지 않은지 확인
- 생체인식정보 수집·이용 동의 시 일괄 전체동의를 클릭하기 전에 특화된 부가 서비스 제공 등을 위해 수집하는 선택동의 항목을 확인하고 동의여부 결정
- 특징정보 생성 후에도 원본정보를 파기하지 않고 보관하는 경우, 원본정보를 보관하는 목적과 보유기간 등을 확인하고 동의 필요

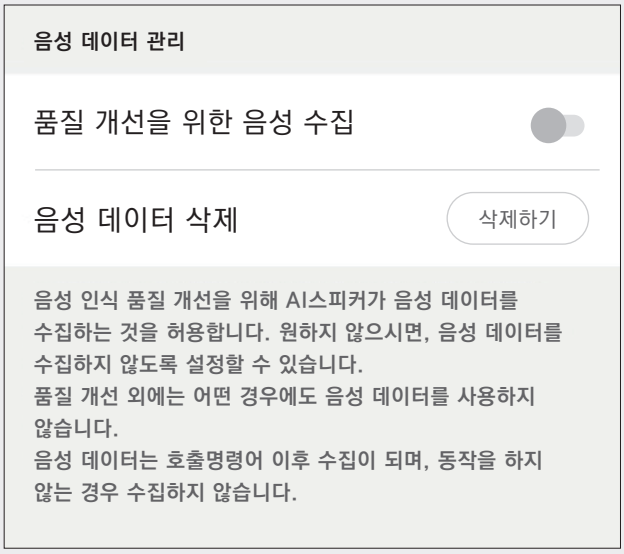
관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑤ 적법하게 생체인식정보 수집

이용하는 서비스가 원본정보의 서버 저장에 대한 동의를 요구하는지 확인

- 원본정보는 그 자체로 개인을 유일하게 식별할 수 있고 변경이 불가능한 특성으로 한번 유출되면 그 피해를 복구하기 어려우므로,
- 해당 서비스를 이용하는 목적을 달성하는데 필수적인 경우가 아니라면 원본정보의 서버 저장에 동의하지 않는 것을 권장함

참고 | 원본정보 수집·이용 동의 설정 (예시)

- AI 스피커 서비스를 제공하는 A사는 음성인식 품질 개선을 위한 음성정보(원본정보) 수집에 대한 동의 기능을 제공함으로, 원하지 않으면 음성을 수집하지 않도록 설정



4 개인정보 처리방침 및 이용약관을 면밀히 검토

- 서비스 가입 시 개인정보 처리방침 및 이용약관을 통해 서비스 제공자가 수집·이용하는 생체인식정보의 이용목적, 항목, 보유·이용기간, 이용자의 통제권 행사 방법 등을 면밀히 검토

관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑭ 개인정보 처리방침 공개

- 생체인식정보를 포함하여 본인의 개인정보를 과도하게 수집하거나, 부당하게 이용하는 부분이 있는지 검토하고
- 특징정보 생성 후 원본정보를 파기하지 않는다면 그 목적 및 보유기간 등을 확인해야 함

2 서비스 이용

5 생체인식정보가 동의한 목적으로 사용되는지 확인

- 서비스 웹사이트 및 앱에 접속하여 본인의 생체인식정보가 어떻게 처리되고 있는지, 당초 동의한 목적으로 사용되고 있는지 등을 확인
  - 본인의 생체인식정보가 자신이 동의하지 않은 목적으로 이용되는 등 권리침해가 우려되는 경우, 개인정보처리자에게 자신의 개인정보에 대한 열람·처리정지·정정·삭제를 요구할 권리가 있고,
  - 생체인식정보 처리와 관련하여 권리 또는 이익을 침해받은 이용자는 개인정보침해 신고센터에 침해 사실을 신고 가능

참고 한국인터넷진흥원 개인정보침해신고센터 이용방법

- 전화 : 118
- 이메일 : privacyclean@kisa.or.kr
- 홈페이지 : 개인정보침해신고센터(https://privacy.kisa.or.kr)

6 본인의 생체인식정보에 대한 통제권 행사

- 본인의 기기 등에서 생체인식정보에 대한 통제방법을 확인하고 필요 시 본인의 생체인식정보를 수정하거나 삭제
  - 생체인식정보를 이용하는 온라인 서비스 등은 이용자의 자기정보 통제권을 제공하기 위하여 본인의 생체인식정보의 저장 여부 확인, 삭제, 동의 취소 등의 기능을 지원함
  - 이용자는 해당 기능을 이용하여 자신의 생체인식정보를 보호하기 위해 적극적인 통제권을 행사

관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑨ 생체인식정보 통제 수단 제공

7 생체인식정보 외 추가적인 인증수단 적용

- 스마트폰에 등록한 지문·얼굴 등 생체인식정보는 본인 확인, 거래 승인 등에 편리하게 이용할 수 있으나, 제3자 등이 본인도 모르게 악용할 소지가 있으므로
  - 금융 거래 등 중요한 서비스인 경우 핀 번호 입력, ARS 인증, 일회용 비밀번호(One-Time Password) 인증 등 지식·소유 기반의 추가 인증수단을 적용

참고 | 생체인식정보 도용 사례

- 의뢰인 가정에 파견된 전문 요양보호사가 환자의 휴대폰에 ○○페이 애플리케이션을 몰래 다운로드한 뒤 자신의 계좌에 연동하고, A씨의 돈을 무단으로 갈취. 전신마비인 환자에게 사진을 찍어주겠다며 접근한 뒤 어플리케이션에서 요구하는 신분 확인 과정을 통과
- 12세 소년이 단체 채팅방에서 방장이 "○○페이 잔액을 캡처해 보내면 10배의 금액을 보내주겠다"는 말에 속아, 새벽 3시 자고 있던 어머니 리모 씨를 흔들어 깨운 뒤 스마트폰으로 얼굴을 스캔하여 어머니의 계좌에서 돈을 출금

VI 활용 안내사항

1. 본 가이드라인은 생체인식정보를 처리하는 서비스·시스템을 직접 구축·운영하는 경우
   - 기획·설계 단계에서 생체인식정보 보호에 필요한 조치를 사전 점검하고,
   - 구축·운영 단계에서 생체인식정보가 안전하게 처리되는지 점검 시 활용할 수 있음
2. 개인정보처리자가 시중에 공급된 생체인식정보 활용 제품을 도입할 경우, 생체인식정보를 안전하게 보호하는 제품을 선택하는 점검기준으로 활용할 수 있음
3. 생체인식정보를 처리하는 제조사는 제품 또는 서비스 개발 시 설계 지침 및 테스트 기준 등으로 활용 가능하고, 개발자 등을 대상으로 하는 교육용 교재로 활용할 수 있음
4. 생체인식정보 활용 서비스를 이용하는 이용자는 자신의 생체인식정보가 적법하고 안전하게 수집·이용되고 있는지 점검하는 기준으로 활용할 수 있음
5. 본 가이드라인에서 제시하는 의무·권장사항은 생체인식정보를 처리하는 유형·방식에 따라 구체적 이행방법이 달라질 수 있으므로, 관련 법령·고시의 규정*, “개인정보 보호 법령 및 지침·고시 해설(’20.12)” 등을 종합적으로 참고하여 활용

   * 개인정보 보호 관련 법률, 시행령, 고시 등: 국가법령정보센터(law.go.kr) 참고
6. 본 가이드라인에서 제시하는 보호 조치는 생체인식정보 처리 시 자율적으로 준수할 수 있는 최소한의 기준이며, 추가적인 보호 조치 또는 기술발전에 따른 새로운 방안을 마련하기를 권장함
7. 본 가이드라인 관련 상담, 개인정보보호 법령 질의 등에 관한 사항은 ‘개인정보 침해신고센터’(privacy.kisa.or.kr, 국번없이 ☎118)로 문의
8. 본 가이드라인은 생체정보 보호 관련 법령·고시·지침 등의 제·개정 및 기술 환경 변화를 반영하여 지속적으로 수정·보완할 예정임

   ※ 생체정보 보호와 관련한 법규정이 제·개정되는 경우, 해당 법규정이 가이드라인보다 우선함

부록

부록 1 **자율점검표**(개인정보처리자 및 제조사)

단계	구분	점검항목	[YES / NO / 미해당]
기획·설계 단계	필요성 검토	이용하려는 생체인식정보가 활용 목적상 필요한 정도와 예상되는 편익에 비해 개인정보 침해 위험성이 크지 않은지를 고려하여 생체인식정보 활용 서비스 도입을 결정하였는가? • 생체인식정보 외에 이용자의 개인정보 침해 위험성을 최소화하면서 처리 목적을 달성할 수 있는 다른 수단이 있는지 검토 필요	□□□ 1-❶
	PbD 적용	기획·설계 단계에서부터 PbD 원칙을 적용하여 생체인식정보 처리 과정에서 예상되는 생체인식정보 침해위험 요인을 사전에 분석하고 예방 조치하였는가?	□□□ 1-❷
	알고리즘 설계·관리	특징정보로부터 원본정보가 쉽게 복원되지 않도록 특징정보 생성 알고리즘을 설계하고 알고리즘이 공개되지 않도록 관리하고 있는가?	□□□ 1-❷
	기본값 설정	기본 값(Defaults)은 이용자의 생체인식정보가 보호되는 방향의 값으로 설정되도록 설계하였는가? • (예시) 특징정보 생성 시, 바이오 원본정보는 삭제되도록 기본설정	□□□ 1-❷
	기성 제품 도입 시	생체인식정보 서비스를 위해 시중에 나온 기성 제품을 도입하는 경우, 생체인식정보를 안전하게 보호하는 제품인지 확인하였는가? • 생체인식정보를 안전하게 보호하는 제품인지 검토를 위한 점검기준으로 본 자율점검표를 활용할 수 있음	□□□ 1-❷
	대체 수단 마련	생체인식정보 이외에 인증·식별을 위한 대체 수단의 제공을 고려하였는가? • 이용자가 생체인식정보 제공을 원하지 않거나, 신체적 장애 등으로 생체인식정보를 제공할 수 없는 상황에 대비하여, 출입카드, 비밀번호 등 대체 수단 마련 권고	□□□ 1-❸
	개인정보 영향평가 수행	생체인식정보를 서버로 전송하여 대량으로 처리하는 경우 개인정보 영향평가의 수행을 검토하였는가? • 생체인식정보를 서버로 전송하여 처리할 경우, 생체인식정보를 수집·입력하는 단말에서 처리하는 경우보다 유출 및 오·남용 등에 따른 침해 위협이 크므로 개인정보 영향평가 수행을 권고	□□□ 1-❹

단계	구분	점검항목	[YES / NO / 미해당]
수집 단계	적법하게 생체인식정보 수집	생체인식정보(원본정보 및 특징정보) 수집·이용 동의를 적법하게 받고 있는가? • 민감정보인 특징정보는 다른 개인정보에 대한 동의와 별도로 받아야 함 ※ 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에는 이용자의 동의없이 생체인식정보 처리 가능	□□□ 2-❺
	원본정보 보관 동의	특징정보 생성 시 원본정보를 파기하지 않고 보관하는 경우 원본정보 수집·이용 동의 시 그 목적 및 보유기간을 구분하여 안내하고 있는가? ※ 다른 법령에 따라 원본정보를 보관하여야 하는 경우는 해당 법령에서 정하는 바에 따름	□□□ 2-❺
	위.변조에 대한 대책 마련	센서 등의 장치를 통해 생체인식정보가 수집·입력될 때, 위·변조된 생체인식정보에 대한 대책을 마련하고 있는가? • 실리콘 인공지문 등 위·변조된 생체인식정보가 수집·입력될 경우, 이를 탐지하고 서비스 이용이 거부될 수 있도록 조치 • 생체인식정보 입력시 핀번호 입력, 일회용 비밀번호(OTP) 인증, ARS 인증 등 지식·소유 기반의 추가 인증수단을 적용	□□□ 2-❻
	전송구간 보호	생체인식정보를 정보통신망을 통하여 전송하거나 보조저장매체 등을 통하여 전달하는 경우 안전한 알고리즘으로 암호화하고 있는가?	□□□ 2-❼
이용·제공 단계	동의받은 목적 내 이용	수집한 생체인식정보를 이용자로부터 동의받은 인증 또는 식별 목적의 범위 내에서 이용하고 있는가? • 생체인식정보를 인증·식별 이외의 목적으로 활용하는 경우, 일반 개인정보로서 이용하는 목적 및 보유기간 등을 고지하고 동의받아야 함	□□□ 3-❽
	통제 수단 제공	이용자가 생체인식정보를 수정하거나 삭제할 수 있도록 통제 수단을 제공하고 있는가? • 이용자 보유 기기, 개인정보처리자가 제공하는 서비스 앱·웹 등에서 생체인식정보 수정·삭제·동의취소 기능 등 지원	□□□ 3-❾
	수집·입력 단말에서 처리	기기 내 안전한 영역 또는 보안토큰, 스마트카드 등 이용자가 직접 소지할 수 있는 매체에서 생체인식정보를 저장·처리하는 방식을 고려하여 적용하였는가?	□□□ 3-❿

단계	구분	점검항목	[YES / NO / 미해당]
보관·파기 단계	저장 시 암호화	생체인식정보 원본정보 및 특징정보를 안전한 알고리즘으로 암호화하여 저장하고 있는가?	☐☐☐ 4-⓫
	생체인식 정보의 파기	동의받은 보유·이용기간이 경과하거나 처리 목적이 달성되면 생체인식 정보를 지체 없이 파기하고 있는가?	☐☐☐ 4-⓬
	특징정보 생성 시 원본정보 파기	특징정보 생성 시 원본정보를 지체 없이 파기하고 있는가? • 원본정보를 보관해야 하는 특별한 필요가 없거나, 법령에 근거가 없는 경우 원본정보는 특징정보 생성 시, 지체 없이 파기하는 것이 원칙	☐☐☐ 4-⓬
	원본정보 보관 시 분리보관	특징정보 생성 후 원본정보를 파기하지 않고 보관하는 경우 해당 이용자의 다른 개인정보와 분리하여 저장·관리하고 있는가? • 원본정보를 보관하는 경우 해당 이용자의 다른 개인정보와 물리적 또는 논리적으로 분리하여 저장·관리를 권고	☐☐☐ 4-⓭
상시 점검	개인정보 처리방침 공개	개인정보 처리방침 등을 통해 이용자에게 생체인식정보 처리 내용을 안내하고 있는가? • 개인정보 처리방침은 이용자가 쉽게 확인할 수 있도록 홈페이지 게시 등의 방법으로 공개 • 개인정보처리자 사무소 등의 보기 쉬운 장소에 게시하거나, 연 2회 이상 발행하는 간행물·소식지·홍보지·청구서 등에 지속적으로 싣거나 계약서 등에 실어 이용자에게 발급도 가능	☐☐☐ 5-⓮
	개인정보 취급자에 대한 관리·감독	생체인식정보를 취급하는 개인정보취급자에 대한 관리·감독 및 정기교육 등을 수행하고 있는가?	☐☐☐ 5-⓯

부록 2 **자율점검표**(이용자)

단계	구분	점검항목	[YES / NO / 미해당]
사전 확인	통제 가능여부 확인	생체인식정보를 본인의 스마트폰이나 보안토큰, 스마트카드 등 본인이 직접 소지할 수 있는 매체에 생체인식정보를 저장·처리하는 서비스 방식인지 확인하였는가? • 생체인식정보를 서버로 전송하여 처리하는 방식은 개인정보 침해 위험성이 크므로 서비스 이용에 주의 필요	□ □ □ 1-❶
	대체 수단 요구	생체인식정보 제공을 원하지 않거나 본인이 제공할 수 없는 특정한 생체인식정보만을 요구하는 경우, 적절한 대체 수단을 요구하였는가? • 다른 생체인식정보 지원, 출입카드, 비밀번호 등의 대체 수단 또는 대면확인 절차 마련 등을 요구할 수 있음	□ □ □ 1-❷
	적합하게 수집·이용 동의	개인정보처리자가 적법하게 수집·이용 동의를 받고 있는지 확인하였는가? • 필수 고지 항목, 특징정보 별도 동의 등 확인	□ □ □ 1-❸
	원본정보 수집·이용 동의에 유의	원본정보를 서버에 보관하는 서비스인 경우, 원본정보가 서비스의 본질적 기능 제공을 위해 필수적인 경우인지를 확인하고 동의 여부를 결정하였는가?	□ □ □ 1-❸
	개인정보 처리방침 검토	서비스 가입 시 개인정보 처리방침 및 이용약관을 통해 서비스 제공자가 수집·이용하는 생체인식정보의 이용목적, 항목, 보유·이용기간, 이용자의 통제권 행사 방법 등을 면밀히 검토하였는가?	□ □ □ 1-❹
서비스 이용	동의한 목적 내 이용	자신의 생체인식정보가 어떻게 처리되고 있는지, 동의받은 목적 내에서 이용되고 있는지 등을 확인하였는가?	□ □ □ 2-❺
	통제권 행사	개인정보처리자가 제공하는 생체인식정보를 통제(수정·삭제 등)하는 기능을 알고 있는가? • 자신의 생체인식정보를 보호하기 위해 불필요한 원본정보 삭제, 수집·이용 동의 취소 등 적극적으로 통제권 행사	□ □ □ 2-❻
	추가적인 인증수단 적용	금융 거래 등 중요한 서비스인 경우 핀 번호 입력, ARS 인증, 일회용 비밀번호 인증 등 지식·소유 기반의 추가 인증수단을 적용하였는가? • 제3자가 수면 중인 이용자의 지문을 이용하여 서비스에 로그인하는 등 본인도 모르게 악용될 위험에 대비	□ □ □ 2-❼

부록 3 일반적인 생체정보에 권장되는 보호 조치

일반적인 생체정보는 유출되거나 오·남용되는 경우 개인정보 침해 위험성이 크고, 언제든지 인증 또는 식별 목적으로 사용될 가능성이 있으므로, 생체인식정보에 준하는 보호 조치 이행을 권장함

- 전송구간 보호 : 정보통신망을 통하여 전송하거나 보조저장매체 등을 통하여 전달하는 경우 안전한 알고리즘으로 암호화

  ※ 정보통신서비스 제공자는 '개인정보의 기술적·관리적 보호조치 기준' 제6조제3항 및 제4항에 따른 의무사항

  관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑦ 생체인식정보 수집·입력 시 전송구간 보호

- 저장 시 암호화 : 유출되거나 오·남용되는 경우 개인정보 침해 위험성이 크므로 저장 시 안전한 알고리즘으로 암호화하여 저장

  관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑪ 생체인식정보 저장 시 암호화

- 생체정보의 파기 : 특별한 이유*가 없다면 특징점 추출 등에 이용된 개인의 신체적, 생리적, 행동적 특징에 관한 정보는 특징점 생성 시 지체 없이 파기하는 것이 원칙

  * 서비스 제공을 위해 필요한 정보라면 이용자의 동의를 받아 보관·이용 가능

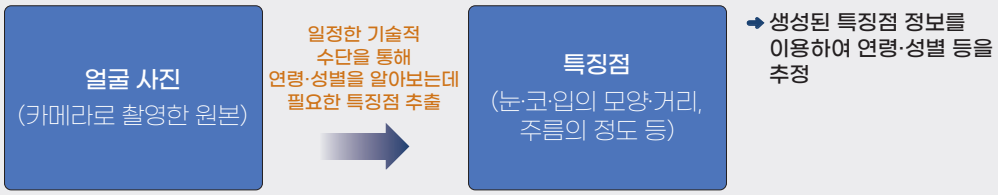
  관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑫ 생체인식정보의 파기

- 보관 시 분리보관 : 특징점 추출 등에 이용된 개인의 신체적, 생리적, 행동적 특징에 관한 정보를 특징점 생성 후에도 보관하는 경우 다른 개인정보와 분리하여 별도로 저장·관리

  관련 내용 Ⅲ. 생체인식정보 보호 조치, ⑬ 원본정보 보관 시 분리보관

참고 | 생체인식정보에 준하는 보호조치가 권고되는 사례 (예시)

- 자율주행차 등에 설치된 카메라를 이용하여 운전자의 피로도, 졸음 여부 등을 판단하여 안전 운전을 위한 경고 메시지를 내보내는 시스템
- 안면인식(사진·영상)을 통해 연령이나 성별 등을 추정하여 이용자의 유형에 맞는 광고를 내보내는 서비스



➜ 인증·식별 목적으로 기술적 처리되는 정보가 아니므로 일반적인 생체정보에 해당

➜ 다만, 일반적인 생체정보는 언제든지 인증·식별 목적으로 사용될 가능성이 있으므로 생체인식정보에 준하는 보호조치 권장

부록 4 생체정보 보호 가이드라인 FAQ

Q1 **스마트 폰으로 촬영하여 SNS, 클라우드에 저장하는 일반적인 사진 및 음성 등도 생체정보에 해당하는지?**

A 일반적인 사진 및 음성 등이 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되지 않는다면 일반적인 개인정보에 해당함

Q2 **디지털 광고판에 설치된 카메라로 이용자의 얼굴 사진에서 성별, 연령대, 감정(입술 모양) 등을 추출하는 서비스인 경우 수집하는 얼굴 사진을 암호화하여 저장해야 하는지?**

A 추출하는 정보가 개인을 인증 또는 식별에 사용할 수 없는 정보라면 생체인식정보가 아닌 일반적인 생체정보이므로 암호화 의무대상이 아님

- 하지만, 일반적인 생체정보의 경우에도 유출되거나 오·남용되는 경우 개인정보 침해 위험성이 크고, 언제든지 인증 또는 식별 목적으로 사용될 가능성이 있으므로, 원본정보에 준하는 보호 조치 이행을 권장함

Q3 **화자인식의 경우 등록된 이용자를 식별하기 위해서 해당 이용자 이외의 목소리를 수집한 뒤 특징정보와 매칭하는 과정을 거치게 되는데, 이 경우 이용자가 아닌 불특정 다수의 음성도 생체인식정보의 활용인지?**

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

※ 불특정 다수의 목소리가 서버로 전송되고 특정 개인을 알아볼 수 있는 경우, 정보가 기기 내에서만 처리되나 개인이 식별되는 경우 등은 모두 생체인식정보로서 이용자의 수집·이용 동의를 받아야 함

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

Q4 화자의 음성에서 성별(남/녀), 연령, 감정(슬픔, 화남, 기쁨)을 인식하기 위한 정보를 추출하는 서비스를 할 예정인데, 이러한 정보는 생체인식정보에 해당되는지?

A 개인을 인증 또는 식별하지 않고 성별, 연령, 감정 등의 정보만을 추출하기 위하여 수집하는 음성정보는 생체인식정보에는 해당하지 않으나, 일반적인 생체정보에 해당함

- 일반적인 생체정보는 생체인식정보에 적용되는 저장 시 암호화, 원본정보 보관 시 분리보관 등이 의무사항이 아니지만,
- 해당 정보가 수집, 전송, 보관 등 처리되는 과정에서 유출되거나 오·남용되는 경우에 예상되는 개인정보 침해 위험성을 고려하여 생체인식정보에 준하는 보호 조치 이행을 권장함

Q5 기 수집된 개인정보에서 차후에 특징정보를 추출하려는 경우 동의 방식은?

A 기존의 수집·이용 동의 목적과 다르므로 원본정보 및 특징정보 모두에 대해 필요한 시점에 수집·이용 동의를 받아야 함

- 이 경우 민감정보에 해당하는 특징정보에 대한 동의는 다른 개인정보의 처리에 대한 동의와 별도로 받아야 함

Q6 생체인식정보를 인증 또는 식별 목적과 그 이외의 용도로 함께 활용할 수 있는지?

A 개인을 인증 또는 식별하기 위해 수집한 생체인식정보를 그 외의 목적으로 동시에 활용할 수 있음

- 다만, 인증 또는 식별 목적으로 동의받은 생체인식정보를 다른 목적으로 활용하기 위해서는 일반적인 개인정보로서 수집·이용하는 목적 및 보유기간 등을 고지하고 동의받는 등 적법하게 처리하여야 함

※ (예시) 이용자가 SNS에 올린 사진에서 특정 개인을 식별하여 친구태그를 추천하는 기능은 얼굴정보가 생체인식정보로서 활용되는 동시에 개인정보로서 활용되는 것임

Q7 가이드라인에 따르면 특징정보 생성 후 원본정보를 원칙적으로 파기해야 하는데, 이용자가 스스로 공개하거나 클라우드 등에 직접 올린 사진에서 특징정보를 추출한 경우 해당 사진을 파기해야 하는지?

A 이용자가 직접 올린 사진에서 개인정보처리자가 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

Q8 이용자의 동의를 받아 원본정보를 활용하는 경우에도 해당 이용자의 다른 개인정보와 분리하여 별도로 저장·관리해야 하는지?

A 원본정보는 변경이 불가능하므로 유출시 피해를 복구하기 어렵고 민감정보가 추출될 수 있는 등 개인정보 침해 위험성이 크므로 강화된 보호조치가 필요

- 원본정보의 안전한 보관을 위해 저장 시 암호화, 원본정보를 특징정보 생성 후에도 보관하는 경우 다른 개인정보와 분리 보관 등의 보호 조치가 요구됨

Q9 SNS 등에 이미 공개된 사진을 인증·식별 목적으로 활용하는 경우에도 원본정보와 특징정보를 암호화 저장해야 하는지?

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

※ 암호화 저장 이외의 보호 조치(내부관리계획 수립·시행, 접근통제, 전송구간 암호화 등)는 하여야 함

Q10 시행령 개정('20.8월) 이전에 이용자 동의를 받아 생체인식정보(특징정보 포함)를 처리하고 있었는데, 시행령 개정 이후에 기존 이용자로부터 민감정보인 특징정보의 수집·이용 동의를 추가로 받아야 하는지?

A 시행령 개정 이전에 이용자의 동의를 받는 등 적법하게 수집한 특징정보를 수집 당시의 목적에 따라 이용하는 경우에는 추가적인 동의 없이 이용할 수 있음

※ 시행령 개정 이후에 수집하는 특징정보에 대해서는 별도 동의 필요

Q11 DNA 검사 등에 사용되는 유전정보가 생체인식정보에 포함되는지?

A 유전정보*를 개인을 인증·식별할 목적으로 사용하는 경우 본 가이드라인이 적용되는 생체인식정보에 해당함

* 인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보(생명윤리법 제2조제14호)

- 하지만 유전정보를 이용한 유전자 검사 등에 관해서는 「생명윤리 및 안전에 관한 법률」에서, 범죄수사 및 범죄예방 목적의 이용에 관해서는 「디엔에이신원확인정보의 이용 및 보호에 관한 법률」에서 별도로 정하고 있으므로 해당 법률이 우선 적용됨

Q12 바이오정보 용어를 생체정보로 변경한 이유는 무엇인지?

A 바이오정보가 생명공학 전체분야를 포함하는 정보로 인식되는 경우가 있고, 타 법령에서 한글 표현인 생체정보 용어가 사용되고 있는 점 등을 고려하여 생체정보로 변경함

- 또한, 특정 개인을 인증·식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 생체인식정보로 정의하여 생체정보와 생체인식정보의 구분을 명확히 함

부록 5 용어 설명

* 가나다순

- **개인정보** 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보이거나 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보(개인정보 보호법 제2조제1호)

  ※쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려해야 함

- **개인정보 영향평가** 개인정보파일의 운용으로 인하여 이용자의 개인정보 침해가 우려되는 경우에 그 위험요인을 분석하고 개선사항을 도출하기 위한 평가(개인정보 보호법 제33조)

- **개인정보 처리업무의 위탁** 개인정보처리자(위탁자)가 개인정보 수집·이용 등의 처리 자체를 제3자(수탁자)에게 위탁하거나, 개인정보의 이용·제공 등 처리가 수반되는 업무를 수탁자에게 위탁하는 것을 의미

- **개인정보보호 중심 설계(PbD)** 원칙 기획 단계부터 파기 단계까지 전체 생애주기에 걸쳐 프라이버시와 개인정보를 보호하는 기술 및 정책을 적용하는 것을 의미

  ①사후 조치가 아닌 사전 예방, ②초기 설정부터 프라이버시 보호조치, ③프라이버시 보호를 내재한 설계, ④프라이버시 보호와 사업기능의 균형, ⑤개인정보 생애주기 전체에 대한 보호, ⑥개인정보 처리 과정에 대한 가시성 및 투명성 유지, ⑦이용자 프라이버시 존중 등 7대 원칙으로 구성

- **개인정보처리방침** 개인정보처리자의 개인정보 처리 기준 및 보호조치 등을 보호법 제30조에 따른 기재사항을 포함하여 문서화 한 것(개인정보 보호법 제30조)

- **개인정보처리자** 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인(개인정보 보호법 제2조제5호)

- **개인정보취급자** 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(개인정보 보호법 제28조제1항)

- **개인정보파일** 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(개인정보 보호법 제2조제4호)

- **민감정보** 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 「개인정보보호법 시행령」으로 정하는 정보(개인정보 보호법 제23조제1항)

- **생체인식정보** 생체정보 중 특정 개인을 인증·식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보. 생체인식 원본정보와 생체인식 특징정보로 구분됨

- **생체인식 원본정보** 생체인식정보 중 개인을 인증 또는 식별 목적으로 입력장치 등을 통해 수집·입력되는 정보
- **생체인식 특징정보** 생체인식정보 중 생체인식 원본정보로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 정보. 보호법 시행령 제18조제3호에 따른 민감정보에 해당
- **생체정보** 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보
- **이용자** 생체인식정보를 제공하여 출입통제, 스마폰·앱 로그인, 거래 승인 등 생체인식정보를 처리하는 서비스를 이용하는 정보주체
- **정보주체** 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람(개인정보 보호법 제2조제3호)
- **정보통신서비스 제공자** 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자(정보통신망법 제2조제1항제3호)
- **제조사** 생체인식정보를 처리하는 기기를 제조하거나 생체인식정보 처리 시스템·서비스를 개발하여 고객(개인정보처리자 등)에게 제공하는 법인 등

부록 6 참고문헌

1. 개인정보 보호 법령 및 지침·고시 해설, 개인정보보호위원회. 2020.12.
2. 개인정보의 안전성 확보조치 기준 해설서, 개인정보보호위원회, 2020.12.
3. 개인정보의 기술적 관리적 보호조치 기준 해설서, 개인정보보호위원회, 2020.12.
4. 개인정보의 암호화 조치 안내서, 개인정보보호위원회, 2020.12.
5. 개인정보 영향평가 수행 안내서, 개인정보보호위원회, 2020.12.
6. 개인정보 수집 최소화 가이드라인, 개인정보보호위원회, 2020.12.
7. 개인정보 처리 위·수탁 안내서, 개인정보보호위원회, 2020.12.
8. 개인정보 처리방침 작성 가이드라인, 개인정보보호위원회, 2020.12.
9. 온라인 개인정보 처리 가이드라인, 개인정보보호위원회, 2020.12.
10. 개발자 대상 개인정보 보호조치 적용 안내서, 개인정보보호위원회, 2020.12.
11. 바이오인식 정보의 보호를 위한 기술적·관리적 지침, KS X 1966:2018, 2018.4.
12. 생체인식 제시형 공격 탐지 제1부 프레임워크, KS X ISO/IEC 30107-1, 2018.4.
13. Information security, cybersecurity and privacy protection – Biometric information protection, ISO/IEC 24745:2011, 2011.6.
14. Information technology – Vocabulary – Part 37: Biometrics, ISO/IEC 2382-37:2017, 2017.2.
15. Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security, ITU-T X.1086, 2008.11.
16. 소프트웨어 보안약점 진단가이드, 행정안전부, 2019.6.
17. 소프트웨어 개발보안 가이드, 행정안전부, 2019.11.
18. 위조 바이오인식 방어력 성능 시험·평가 해설서, 한국인터넷진흥원, 2021.6.
19. 패스워드 선택 및 이용안내서, 과학기술정보통신부, 2019.6.

※ 개인정보 관련 해설서·안내서·지침·가이드라인 등에 대한 최신 자료는
"개인정보보호위원회 누리집(www.pipc.go.kr)"(정책·법령/법령정보/지침·가이드라인),
"개인정보보호 포털(www.privacy.go.kr)"(자료마당/지침자료)에 게시되어 있음

발 행: 2021년 9월
발 행 처: 개인정보보호위원회
지원기관: 한국인터넷진흥원

- 본 가이드라인은 생체정보 보호 관련 법령 제·개정 및 기술 환경 변화를 반영하여 지속적으로 수정·보완할 예정입니다.
- 최신 자료는 “개인정보보호위원회 누리집(www.pipc.go.kr)”, “개인정보보호 포털(www.privacy.go.kr)”에서 확인할 수 있습니다.