

Przetwarzanie danych biometrycznych

INFORMACJA

**Generalnego Inspektora Ochrony Danych
Osobowych o zagrożeniach płynących z
upowszechnienia danych biometrycznych**

**BIURO
GENERALNEGO INSPEKTORA OCHRONY
DANYCH OSOBOWYCH**

- ☐ Definicje danych biometrycznych.
- ☐ Formy występowania danych biometrycznych.
- ☐ Główne cechy danych biometrycznych.
- ☐ Podstawowe parametry techniczne systemów biometrycznych.
- ☐ Zagrożenia związane z przetwarzaniem danych biometrycznych.
- ☐ Obowiązek przeprowadzania oceny skutków przetwarzania danych biometrycznych na prywatność.
- ☐ Uprzednie konsultacje z organem nadzorczym w zakresie oceny skutków przetwarzania dla ochrony danych.
- ☐ Wnioski dotyczące wykorzystania danych biometrycznych w kontaktach z obywatelami

Definicje danych biometrycznych

Co to są dane biometryczne ?

„**Dane biometryczne**” - właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa. *Opinii 4/2007 Grupy Roboczej Art. 29 (WP136)*

„**Dane biometryczne**” - dane osobowe, które wynikają **ze specjalnego przetwarzania technicznego**, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej **oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby**, takie jak wizerunek twarzy lub dane daktyloskopijne. *Art. 3 pkt 14 RODO*

„**Dane biometryczne**” - informacje wyodrębnione z próbki biometrycznej i stosowane do utworzenia wzorca odniesienia, albo wzorca dopasowywanego. *PN-ISO 19092:2008*

Definicje systemu biometrycznego

Co to jest biometria, system biometryczny?

„**Biometria**” - użycie specyficznych atrybutów odzwierciedlających unikalne cechy osoby, takie jak odcisk linii papilarnych palca, struktura układu żył krwionośnych (palca, nadgarstka), cechy charakterystyczne głosu, w celu potwierdzenia tożsamości osoby. *Norma ISO/IEC 2382:2015 Information technology - Vocabulary*

„**System biometryczny**” - system, którego zadaniem jest automatyczne rozpoznanie lub uwierzytelnienie osoby fizycznej na podstawie jej cech biologicznych lub behawioralnych. *Norma ISO/IEC 24745:2011 Information technology – Security techniques – Biometric information protection*

Specyfika przetwarzania danych biometrycznych

Formy występowania danych biometrycznych

Dane biometryczne wykorzystywane w systemach biometrycznych do identyfikacji lub weryfikacji osób mogą występować w formie **przetworzonej** lub w formie **nieprzetworzonej**, tzw. surowej.

„**Surowe dane biometryczne**” - to nieprzetworzone cyfrowe dane biometryczne pobrane z urządzenia pomiarowego (np. obraz odcisku palca, lub strumień audio), nadające się do późniejszego przetwarzania w celu utworzenia próbki biometrycznej lub wzorca

„**Wzorzec odniesienia**” - dane reprezentujące miary biometryczne zarejestrowanej osoby, wyodrębnione z próbki biometrycznej zarejestrowanej osoby, zazwyczaj przechowywane w systemie biometrycznym i stosowane przez system biometryczny w celu sprawdzenia zgodności z przedkładanymi później wzorcami dopasowania

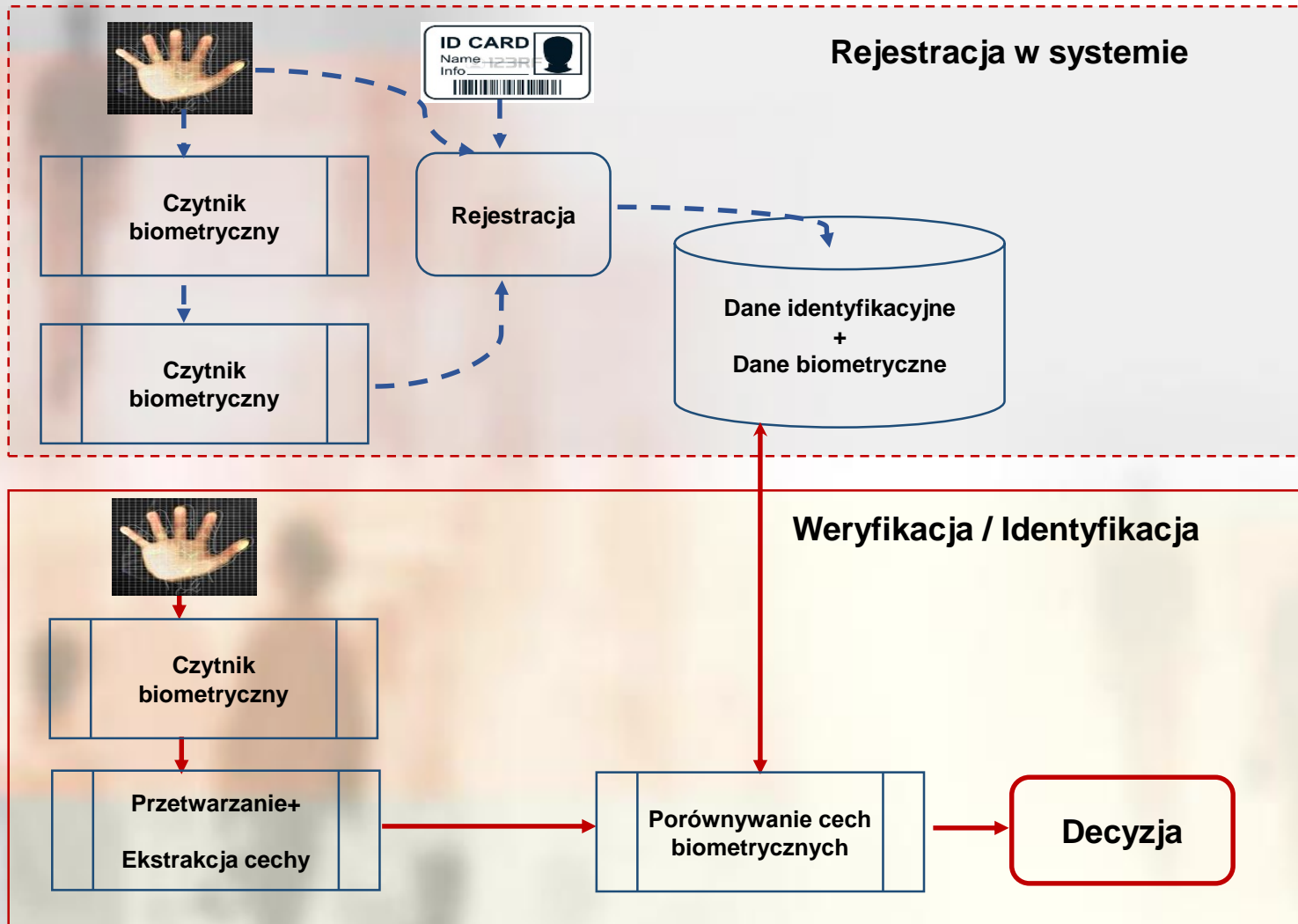
„**Wzorzec dopasowania**” - dane reprezentujące miary biometryczne osoby, wyodrębnione z próbki biometrycznej w celu porównania z wzorcami odniesienia

Właściwości danych biometrycznych

Dane biometryczne wykorzystywane w systemach biometrycznych do identyfikacji lub weryfikacji osób powinny charakteryzować się takimi właściwościami, jak:

- **Uniwersalność** - właściwość polegająca na możliwości pobrania próbki od możliwie największej grupy osób (np. kształt dłoni będzie bardziej uniwersalną cechą niż odcisk linii papilarnych, gdyż linie papilarne mogą być wytarte, zniekształcone raną);
- **Unikalność** – właściwość polegająca na posiadaniu cech wyróżniających dany rodzaj próbki od innych rodzajów próbek (np. układ linii papilarnych palca bardziej wyróżnia osobę niż jej kolor włosów);
- **Stołość (niezmiennność)** – właściwość polegająca na niezmienności danej cechy w czasie;
- **Łatwość pobrania** (collectability) – łatwość i wygoda pobrania próbki;
- **Wydajność** (performance) – solidność, pewność, szybkość i dokładność przetwarzania;
- **Akceptowalność** – brak negatywnych skojarzeń, brak obaw wpływu na zdrowie, a także przyjazność i wygoda dla osób w procesie pobierania próbki (np. łatwiej jest pobrać odcisk palca niż kod DNA);
- **Łatwość obejścia** (Circumvention) – definiowana jako możliwość oszukania system np. łatwiej jest oszukać system podstawiając nagrany dźwięk niż kod DNA).

Struktura systemu biometrycznego



Podstawowe parametry systemu biometrycznego

Do podstawowych parametrów technicznych systemu biometrycznego należą:

Wskaźnik błędnych akceptacji (ang. *False Accept Rate – FAR*), jest to prawdopodobieństwo w systemie jeden do jednego, że system biometryczny nieprawidłowo zidentyfikuje daną osobę fizyczną lub nie odrzuci oszusta. Wskaźnik wyraża się w % błędnie zakwalifikowanych wzorców dopasowania do wzorców odniesienia, jako niepasujące do siebie.

Wskaźnik błędnych odrzuceń (ang. *False Reject Rate – FRR*), jest to prawdopodobieństwo, że w systemie dojdzie do błędnego odrzucenia. Do błędnego odrzucenia dochodzi, jeżeli osoba fizyczna nie zostaje dopasowana do jej własnego istniejącego wzorca biometrycznego.

Inne parametry systemu biometrycznego

Do innych ważnych parametrów technicznych systemu biometrycznego należą:

Akceptowalność – brak negatywnych skojarzeń, brak obaw wpływu na zdrowie, a także przyjazność i wygoda dla osób w procesie pobierania próbki (np. łatwiej jest pobrać odcisk palca niż kod DNA).

Łatwość użycia – łatwość, szybkość i wygoda pobrania próbki (np. łatwiej i szybciej można pobrać obraz układu żył krwionośnych palca niż obraz źrenicy oka).

Czas rejestracji – czas niezbędny do pobrania, przetworzenia i rejestracji w systemie biometrycznym wzorca odniesienia.

Czas weryfikacji – szybkość podejmowania przez system biometryczny decyzji zwłaszcza w systemach identyfikacji typu jeden do wielu.

Wiarygodność – miara zaufania do wydawanych przez system decyzji mierzona wartością współczynników błędnego odrzucenia i błędnej akceptacji (FAR, FRR).

Wielkość wzorca – wielkość obszaru pamięci zajmowanej w systemie biometrycznym przez wzorzec odniesienia.

Porównanie właściwości próbek biometrycznych

Wartości poszczególnych parametrów systemów biometrycznych:

Parametr, właściwość	Oceny właściwości próbek biometrycznych od najbardziej do najmniej korzystnych
Akceptowalność	głos, rysy twarzy, naczynia krwionośne palca, linie papilarne, kształt dłoni, tęczęwka, podpis odręczny, siatkówka
Łatwość użycia	głos, rysy twarzy, kształt dłoni, naczynia krwionośne palca i dłoni, linie papilarne, tęczęwka, siatkówka
Czas weryfikacji	linie papilarne, naczynia krwionośne palca, tęczęwka, kształt dłoni, naczynia krwionośne dłoni, siatkówka, głos
Czas rejestracji	linie papilarne, naczynia krwionośne palca, naczynia krwionośne dłoni, tęczęwka
Wiarygodność	siatkówka, tęczęwka, naczynia krwionośne palca, linie papilarne, kształt dłoni, głos, sposób pisanie na klawiaturze
Wielkość wzorca	kształt dłoni, siatkówka, tęczęwka, naczynia krwionośne palca, linie papilarne, sposób pisanie na klawiaturze, głos, naczynia krwionośne dłoni

Źródło: M. Plucińska, J. Wójtowicz, „Analiza Techniki biometrycznych do uwierzytelnienia osób”, w *Elektronika* 4/2014

Zagrożenia związane ze stosowaniem biometrii

Zagrożenia związane z przetwarzaniem danych biometrycznych

Możliwość ujawnienia danych wrażliwych. Właściwości niektórych źródeł danych biometrycznych, z których pobierane są próbki, takich jak siatkówka i źrenica oka, właściwości ruchowe (chód, sposób wypowiedzania się) mogą zdradzać poza cechami niezbędnymi do identyfikacji czy weryfikacji osoby także inne właściwości, jak np. zmęczenie, stres, stan zdrowia, w tym bycie pod wpływem działania narkotyków, czy spożycia alkoholu.

Ograniczone możliwości zmiany i unieważnienia wzorca. Technologia biometryczna bazuje na indywidualnych cechach danej osoby, których nie można zmienić w przypadku nieupoważnionego pozyskania przez nieuprawnione osoby tak jak np. w przypadku hasła czy posiadanej rzeczy np. karty kredytowej, które w przypadku kompromitacji można w każdej chwili zmienić na inne.

Zagrożenia związane ze stosowaniem biometrii

Zagrożenia związane z przetwarzaniem danych biometrycznych

Możliwość użycia bez wiedzy osoby, której dane dotyczą. Szereg danych biometrycznych takich jak np. obraz twarzy, sposób chodzenia, czy właściwości ruchowe mogą być zarejestrowane i wykorzystane przez system biometryczny bez wiedzy osoby, której dane dotyczą. Zagrożenie to jest istotne zwłaszcza w kontekście użycia nowoczesnych kamer monitoringu wizyjnego, które wyposażone w specjalne oprogramowanie rozpoznawania twarzy może nie tylko nagrywać obraz otoczenia w celach prewencyjnych i dowodowych na wypadek incydentu, ale również w innych, bliżej nieokreślonych.

Trudności pobrania próbki biometrycznej. Niektóre rodzaje danych biometrycznych mogą być trudne do pobrania, np. pobranie linii papilarnych z wytartych pracą lub skaleczonych palców. Inne dane jak np. kształt twarzy może być celowo zniekształcany ubiorem (zasłona, szalik, maska) lub zachowaniem np. uśmiech, co w konsekwencji może prowadzić do obniżenia jakości poprzez zwiększenie zawodności systemu (błędne rozpoznanie).

Zagrożenia związane ze stosowaniem biometrii

Zagrożenia związane z przetwarzaniem danych biometrycznych

Podatność na łączenia danych. Ograniczone możliwości zmiany danych biometrycznych, których nie można zmieniać tak jak np. hasła oraz ograniczona liczba źródeł danych biometrycznych (10 palców, dwie dłonie, jedna twarz) stwarzają ryzyko łączenia danych przetwarzanych przez tą samą osobę w różnych serwisach. Dotyczy to sytuacji, kiedy w różnych systemach użyto np. tego samego rodzaju próbki biometrycznej i tej samej metody przekształcania surowego obrazu próbki do postaci wzorca odniesienia.

Brak przejrzystości. Wielu producentów systemów biometrycznych wykorzystuje poufne, znane tylko sobie algorytmy wykorzystywane do przekształceń i porównywania wzorców biometrycznych, przez co nie można ich darzyć takim samym zaufaniem jak tych, które poddawane są przeglądowi i ocenie stron trzecich. Mogą istnieć wówczas obawy, czy system wykorzystywany jest tylko do np. weryfikacji tożsamości, czy również do np. oceny trzeźwości, stanu zdrowia, czy stanów emocjonalnych.

Zagrożenia związane ze stosowaniem biometrii

Zagrożenia związane z przetwarzaniem danych biometrycznych

Możliwość błędnej identyfikacji, weryfikacji, klasyfikacji. Technologia biometryczna identyfikacji bazuje na porównywaniu wyekstrahowanych cech biometrycznych pobranej próbki z wyekstrahowanymi w taki sam sposób cechami biometrycznymi próbki wzorca. Stąd różnica pobranych próbek może spowodować różnicę ich wyekstrahowanych cech, co w konsekwencji może prowadzić do błędnego rozpoznania (błędnej akceptacji lub błędnego odrzucenia).

Możliwość fałszerstwa. Niektóre metody biometryczne podatne są na próby podrobienia próbki i oszukanie czytnika. Jedną z najbardziej podatnych na podrobienie próbek jest np. odciski linii papilarnych palca.

Zagrożenia związane ze stosowaniem biometrii

Przykładowy sposób oszukania systemu rozpoznawania odcisków palca

Proces oszukania składa się z dwóch etapów:

Etap pierwszy to pobranie próbki odcisku palca ofiary. W etapie tym podkłada się ofierze szklane naczynie, lusterko lub inny przedmiot o gładkiej strukturze bez nadruków.

Etap drugi to preparacja sztucznego odcisku. W etapie tym na pozostawione ślady linii papilarnych można nałożyć pył, np. grafit, lub nanieść cienką warstwę cyjanoakrylu, które spowodują ich lepsze wyróżnienie. Uzyskany obraz należy sfotografować i odpowiednio przetworzyć usuwając zniekształcenia i szумы a następnie podłożyć pod czytnik linii papilarnych.

Inną metodą oszustwa jest utworzenie odlewu odcisku przy użyciu masy lateksowej lub ciastoliny – niebrudzącej i niewysychającej masy plastycznej. Na podstawie przeprowadzonych w latach 2008-2009 prób stwierdzono, że przy użyciu tej metody można było oszukać około 90 % obecnych wówczas na rynku czytników linii papilarnych*

Źródło: D. Matltoni, D. Maio, A.K. Jain: Prabhaker S. Handbook of Fingerprint Recognition, 2nd Edition, Springer, 2009, www.giodo.gov.pl

Zalety i korzyści związane ze stosowaniem biometrii

Do najważniejszych zalet i korzyści związanych ze stosowaniem biometrii należą:

Brak możliwości dzielenia się danymi biometrycznymi z inną osobą. Użycie danych biometrycznych zapobiega dzieleniu się użytkownikami danymi identyfikującymi, np. podczas wejścia do ściśle chronionych obszarów wymagających bezwzględnej rozliczalności. Różne osoby nie mogą sobie tych danych przekazywać między sobą w celu np. wejścia do ściśle chronionego obszaru.

Brak możliwości zapomnienia. Danych biometrycznych w przeciwieństwie do hasła nie można zapomnieć. Nie ma potrzeby ich zmieniać, odnawiać (chyba że stosowane są w odniesieniu dla osób młodych w okresie wzrostu).

Odporność na ataki fałszerstwa (dla niektórych metod). Systemy identyfikacji i weryfikacji biometrycznej są bardziej odporne na fałszerstwa poprzez ataki typu phishing, podglądnięcie, odgadnięcie czy kradzież niż inne metody uwierzytelniania.

Wiarygodność. Najnowsze systemy biometryczne charakteryzują się bardzo dużą niezawodnością i dokładnością.

Zestawienie zagrożeń oraz korzyści i zalet biometrii

Zagrożenia i wady biometrii

**Możliwość ujawnienia
danych wrażliwych**

**Możliwość użycia bez
wiedzy właściciela**

**Podatność na łączenia
danych**

**Trudności pobrania próbki
biometrycznej**

**Ograniczone możliwości
zmiany i unieważnienia**

Brak przejrzystości

**Możliwość fałszerstwa i
błędnej identyfikacji**

Korzyści i zalety biometrii

**Brak możliwości wymiany
i dzielenia się danymi**

**Brak możliwości
zapomnienia**

**Duża odporność na
niektóre rodzaje
fałszerstw**

**Duża wiarygodność,
dokładność**



Biometria linii papilarnych - zagrożenia i zalety zastosowań

W metodzie tej obecnie do pobierania próbki stosowane są układy sensorowe, dające w wyniku informację graficzną od razu w postaci cyfrowej. Obraz linii papilarnych jest rejestrowany na powierzchni dwuwymiarowej tablicy sensorów jako zmiany pojemności lub temperatury między zróżnicowaną powierzchnią palca (rowki i grzbiety linii papilarnych). Uzyskany cyfrowy obraz linii papilarnych jest analizowany następnie pod kątem identyfikacji lokalnych nieciągłości we wzorze linii papilarnych nazywanych minucjami. We wzorze takim można wyróżnić około 100 charakterystycznych punktów (początki, zakończenia, rozwidlenia, oczka, haczyki, itp.) z których tworzony jest matematyczny wzorec odcisku palca.

Wiarygodność metody jest zależna od liczby minucji branych pod uwagę. Czytniki linii papilarnych są zwykle wyposażane dodatkowo w mechanizmy rozpoznawania imitacji (manekina) palca. Metoda ta zawodzi tam, gdzie osoby rozpoznawane mają brudne palce, wytarte lub skaleczone. Łatwa dostępność odcisków palca budzi obawy, że zostaną pobrane i wykorzystane bez zgody i wiedzy właściciela. Ze względu na wykorzystywanie tej metody w kryminalistyce, ma ona negatywne psychologiczne konotacje z policyjnymi metodami śledczymi.

Brak możliwości wymiany i dzielenia się danymi

Brak możliwości zapomnienia

Możliwość użycia bez wiedzy właściciela

Podatność na łączenia danych

Trudności pobrania próbki biometrycznej

Ograniczone możliwości zmiany i unieważnienia

Możliwość fałszerstwa i błędnej identyfikacji



Biometria układu żył dłoni - zagrożenia i zalety zastosowań

W technologii identyfikacji biometrycznej wykorzystującej układ żył krwionośnych dłoni, wprowadzonej przez japońską firmę Fujitsu, dane od identyfikowanej osoby pobierane są przez czytnik do którego należy zbliżyć dłoń na odległość kilku centymetrów.

Czujnik bada, czy w dłoni występuje przepływ krwi, a następnie skanuje dłoń nieszkodliwym dla zdrowia promieniowaniem podczerwonym. Do odczytu obrazu układu żył krwionośnych wykorzystuje się nieszkodliwe promieniowanie podczerwone. Pobieranie próbek biometrycznych jest czynnością intuicyjną i szybką. Nie jest łatwe pobranie próbki bez wiedzy osoby, której dotyczy (jeśli osoba jest przytomna).

Metoda pobierania próbki jest higieniczna (wystarczy zbliżyć dłoń) i neutralna dla zdrowia.

Metoda ma zastosowanie dla prawie każdej osoby. Charakteryzuje ją duża szybkość identyfikacji i wysoki poziom bezpieczeństwa (FAR=0,00001%, FRR =0,01%). Duże bezpieczeństwo przechowywania danych i odporność na kojarzenie danych przy zastosowaniu szyfrowania.

Brak możliwości wymiany i dzielenia się danymi

Brak możliwości zapomnienia

Duża odporność na niektóre rodzaje fałszerstw

Duża wiarygodność, dokładność

Możliwość użycia bez wiedzy właściciela (mała)

Podatność na łączenia danych

~~**Trudności pobrania próbki biometrycznej**~~

Ograniczone możliwości zmiany i unieważnienia

~~**Możliwość fałszerstwa i błędnej identyfikacji**~~



Biometria rysów twarzy- zagrożenia i zalety zastosowań

W technologii identyfikacji biometrycznej wykorzystującej rysy twarzy zarejestrowany obraz poddawany jest odpowiedniej obróbce i matematycznemu przekształceniu do postaci wzorca cyfrowego.

Obróbka obrazu polega na zlokalizowaniu twarzy i oczu, a następnie pozycji oczu w stosunku do siebie i całej twarzy. Na etapie analizy wstępnej rozpoznane są okulary i zarost. W kolejnym etapie tworzona jest geometryczna siatka charakterystycznych punktów twarzy, która zapisywana jest w formie cyfrowej. Do identyfikacji i weryfikacji wykorzystuje się nie obraz twarzy, ale jej charakterystyczne punkty.

W celu wykrycia fałszyfikatów (fotografia, manekin), stosuje się kamery rejestrujące emitowane ciepło i jego rozkład niewidoczny optycznie. Zaletą tej metody jest łatwość stosowania, nieinwazyjność i dość duża akceptowalność społeczna.

Metoda ta stosowana bez odczytu termicznego, np. z wykorzystaniem kamer użytych w laptopach czy telefonach komórkowych, jest podatna na fałszerstwa takie jak fotografia, maska, manekin.

**Brak możliwości wymiany
i dzielenia się danymi**

**Brak możliwości
zapomnienia**

**Odporność na niektóre
rodzaje fałszerstw (zależy
od technologii)**

**Wiarygodność, dokładność
(zależy od technologii)**

**Możliwość użycia bez
wiedzy właściciela**

**Podatność na łączenia
danych**

~~**Trudności pobrania
próbki biometrycznej**~~

**Ograniczone możliwości
zmiany i unieważnienia**

**Możliwość fałszerstwa i
błędnej identyfikacji**

Prawne podstawy przetwarzania danych osobowych - legalność

Legalność przetwarzania danych osobowych regulują art. 23 ust 1 u.o.d.o.
art. 7 dyrektywy 95/46/WE

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- 1) osoba, której dane dotyczą, **wyrazi zgodę**, chyba że chodzi o usunięcie dotyczących jej danych;
- 2) **jest to niezbędne** dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- 3) **jest to konieczne do realizacji umowy**, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
- 4) **jest niezbędne do wykonania określonych prawem zadań** realizowanych dla dobra publicznego;
- 5) realizowanych przez administratorów danych albo odbiorców danych, a **jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów** przetwarzania, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Zachowanie staranności w celu ochrony interesów podmiotu danych

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

- 1) przetwarzane zgodnie z prawem;
- 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2;
- 3) merytorycznie poprawne i **adekwatne w stosunku do celów**, w jakich są przetwarzane;
- 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

(art. 26, ust. 1)

(art. 6 dyrektywy 95/46/WE)

Wyniki przeprowadzonych kontroli przetwarzania danych biometrycznych

Rodzaj biometrii	Administrator danych	Cel przetwarzania	Podstawa prawna	Ocena zgodności
Odcisk linii papilarnych	Komenda Główna Policji	Identyfikacja osób podejrzanych i ocena ich udziału w przestępstwie	Przepis prawa art. 20 ust. 2, pkt 2 ustawy o policji	Brak zastrzeżeń
Odcisk linii papilarnych	Urzędy wojewódzkie, konsulaty	Wydawanie dokumentów ID (paszportów)	Przepis prawa art. 18 ust. 1 pkt 11 ustawy o dok. paszportowych	Brak zastrzeżeń
Odciski linii papilarnych	Podmioty publiczne i prywatne	Kontrola wejścia osób zatrudnionych oraz rozliczanie czasu pracy	Brak podstawy prawnej. Nieważność uzyskanej zgody	Wydano decyzje nakazujące zaprzestanie przetw. (4 przypadki)
Odciski linii papilarnych	Podmioty prywatne	Kontrola dostępu i rozliczanie wykupionych usług	Brak podstawy prawnej. Brak zgody	Wydano decyzję usunięcia wad prawnych (1 przypadek)
Odciski linii papilarnych	Podmioty prywatne	Kontrola dostępu i rozliczanie wykupionych usług	Brak podstawy prawnej. Nieprawidłowo pozyskana zgody	Wydano decyzję usunięcia wad prawnych (1 przypadek)
Tęczówka oka	Podmioty prywatne (bank)	Kontrola dostępu do określonych stref bezpieczeństwa i usług	Przepis prawa art. 36 ust.1 UODO	Brak zastrzeżeń (1 przypadek)
Układ żył krwionośnych palca	Podmioty prywatne (bank)	Kontrola dostępu do określonych stref bezpieczeństwa i usług	Przepis prawa art. 36 ust. 1 UODO	Brak zastrzeżeń (1 przypadek)

Biometria w wytycznych Grupy

Art. 29

Wymagania dotyczące przetwarzanie danych biometrycznych w świetle przepisów Dyrektywy 95/46/WE omówiono w następujących dokumentach Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołananej na mocy art. 29 Dyrektywy 95/46/WE:

1. Working document on biometrics (WP80) przyjęty w dniu 1 sierpnia 2003 r.).
2. Opinia 4/2007 w sprawie pojęcia danych osobowych WP 136) przyjęta 20 czerwca 2007 r.
3. Opinia 02/2012 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych WP 192) przyjęta w dniu 22 marca 2012 r.
4. Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) przyjęta 27 kwietnia 2012 r.

Working document on biometrics (WP80) przyjęty 1 sierpnia 2003 r.

Working document on biometrics (WP80) definiuje pojęcie systemu biometrycznego, technik biometrycznych oraz zwraca uwagę na:

1. Automatyczne przetwarzanie danych biometrycznych w systemach identyfikacji i weryfikacji.
2. Zasadę **adekwatności i proporcjonalności** w odniesieniu do przetwarzania danych biometrycznych.
3. Sytuacje, kiedy dane biometryczne mogą należeć do kategorii danych objętych szczególną ochroną (ujawnianie pochodzenia etnicznego, przynależności rasowej lub stan zdrowia).
4. **Unikalność danych biometrycznych i zagrożenia z tym związane w zakresie możliwości łączenia danych pozyskiwanych z różnych źródeł.**
5. Bezpieczeństwo przetwarzania danych biometrycznych w zależności od architektury systemu, w tym miejsca przechowywania wzorca danych biometrycznych „template” (w pamięci urządzenia biometrycznego, w centralnej bazie danych, w nośniku danych typu smart card, plastic card, optical cards).

Rozwiązania zaproponowane w normie ISO/IEC 24745:2011.

Wymagania dotyczące bezpieczeństwa:

- **Poufność** – właściwość zapewniająca, że dane (template) nie zostały udostępnione lub ujawnione nieupoważnionym osobom.
- **Integralność** – właściwość zapewniająca, że dane (template) nie zostały zmienione i pozostają kompletne.
- **Odnawialność i unieważnianie** (Renewability and revocability) jest wymagana w celu uniemożliwienia atakującemu nieautoryzowanego wykorzystywania.

Rozwiązania zaproponowane w normie ISO/IEC 24745:2011.

Wymagania dotyczące prywatności:

- **Nieodwracalność** (Irreversibility) -- zabezpieczenie przed użyciem danych biometrycznych w innym celu niż zakładano, dane biometryczne powinny być nieodwracalnie przetworzone. Przechowywany w systemie biometryczny wzorzec odniesienia (template) nie powinien być możliwy do wykorzystania w celu łączenia danych pochodzących z innych aplikacji i baz danych.
- **Dyskretność** (Confidentiality) – Zabezpieczenie biometrycznego wzorca odniesienia przed nieautoryzowanym pobraniem lub ujawnieniem jego wartości.

Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii

Biometrycznych zwraca uwagę na:

1. Różne źródła danych biometrycznych i ich rodzaje , w tym:
techniki fizyczne i fizjologiczne, w ramach których mierzy się fizyczne i fizjologiczne cechy danej osoby, takie jak: zgodności linii papilarnych, analiza obrazu palca, analiza wzoru DNA, analiza położenia porów itp.;
techniki behawioralne, przy pomocy których mierzy się zachowanie danej osoby i które obejmują sprawdzanie podpisu odręcznego, analizę dynamiki pisanie na klawiaturze, analizę chodu itp.
2. Różnorodność systemów biometrycznych, różne fazy przetwarzania danych oraz **konieczność stosowania oceny wpływu na prywatność dla każdej fazy budowy systemu oraz dla każdej fazy przetwarzania danych.**
3. Ryzyko związane ze stosowaniem danych biometrycznych do celów identyfikacji w dużych scentralizowanych bazach danych ze względu na potencjalnie szkodliwe skutki w zakresie ochrony prywatności (np. łączenie danych).
4. Nowe technologie biometryczne, w tym łączenie różnych technik identyfikacji i weryfikacji w celu zwiększenia niezawodności (np. urządzenie ViRDI www.giodo.gov.pl AC7000)

Szczególne kategorie danych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Art. 4 pkt 14, art. 9)

Dane biometryczne - oznaczają dane osobowe, które wynikają **ze specjalnego przetwarzania technicznego**, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz **umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby**, takie jak wizerunek twarzy lub dane daktyloskopijne (**Art. 4 pkt 14**)

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, **danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej** lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. (**Art. 9 ust. 1**)

Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, **danych biometrycznych** lub danych dotyczących zdrowia. (**Art. 9 ust. 4**)

Art. 9 ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- a) osoba, której dane dotyczą, **wyraziła wyraźną zgodę** na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- e) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- ----- (Art. 9 ust. 2)

Art. 9, ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą;
- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 i jest proporcjonalne do celu oraz nie narusza prywatności. (Art. 9 ust. 2)

Dane biometryczne w RODO – zalecenie oceny skutków dla ochrony danych

Dane biometryczne i ocena skutków dla ochrony danych (motyw 89 RODO)

Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych.

RODO w odniesieniu do operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych wprowadza obowiązek przeprowadzania oceny skutków dla ochrony danych. ([Motyw 98 preambuły](#))

Ocenie skutków dla ochrony danych należy dokonywać w przypadkach, w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej na podstawie profilowania oraz w przypadku przetworzenia szczególnych kategorii danych osobowych, w tym **danych biometrycznych** oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa. ([Motyw 91 preambuły](#))

Oceny skutków dla ochrony danych – jakich sytuacji dotyczy

Ocena skutków dla ochrony danych (Art. 35 RODO)

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania **dokonyuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.**
2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.
3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
 - a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
 - b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub**
 - c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Oceny skutków dla ochrony danych – jakie działania są niezbędne

Ocena skutków dla ochrony danych zawiera co najmniej (Art. 35 pkt. 7 RODO)

- a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- b) ocenę, czy operacje przetwarzania są **niezbędne oraz proporcjonalne w stosunku do celów**;
- c) ocenę **ryzyka naruszenia praw lub wolności** osób, których dane dotyczą, o którym mowa w ust. 1; oraz
- d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych.

Upřednie konsultacje – kiedy należy je porzeprowadzać.

Upřednie konsultacje (Art. 36 pkt. 1 i 2 RODO)

1. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.
2. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58.
tj. wydania ostrzeżenia, udzielenie upomnienia, nakazanie dostosowania operacji przetwarzania do przepisów RODO, wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania, nakazania sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono.

Uprzednie konsultacje na etapie tworzenia prawa.

Państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania. (Art. 36 ust. 4 RODO)

Upřednie konsultacje – jakie działania należy wykonać.

Konsultując się z organem nadzorczym zgodnie z ust. 1, administrator przedstawia mu: (Art. 36 ust 3 RODO)

- a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
- b) cele i sposoby zamierzonego przetwarzania;
- c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;
- d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
- e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz
- f) wszelkie inne informacje, których żąda organ nadzorczy.

Wykorzystanie danych biometrycznych w kontaktach z obywatelami

Biorąc pod uwagę szczególne właściwości danych biometrycznych oraz uwarunkowania prawne (zaliczenie ich do danych szczególnie chronionych), użycie danych biometrycznych powinno być ograniczone do przypadków, gdzie to jest niezbędne i proporcjonalne.

Do takich przypadków należy zaliczyć:

1. Wydawanie środków identyfikacji elektronicznej, dla których rozporządzenie eIDAS UE Nr 910/2014 wymaga zapewnienia **wysokiego poziomu bezpieczeństwa**, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej (Rozporządzenie wykonawcze Komisji (UE) 2015/1502;
2. Wydawanie dokumentów podróży (paszportów) i dokumentów tożsamości;
3. Dostępu do ściśle strzeżonych pomieszczeń (systemów) wymagających wysokiego poziomu bezpieczeństwa, w tym potwierdzenia tożsamości osoby poprzez dowody identyfikacji fotograficznej lub biometrycznej.

W każdym jednak przypadku przetwarzanie danych biometrycznych powinno być dopuszczalne tylko w przypadku posiadania odpowiedniej podstawy prawnej.

Wykorzystanie danych biometrycznych przez podmioty prywatne

Zgodnie z przepisem art. 35 ust. 10 RODO ocena skutków nie będzie wymagana jedynie w przypadkach jeśli przetwarzanie danych biometrycznych wymagane jest przez przepis prawa lub przetwarzanie tych danych jest nie zbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, **a ocena skutków dla ochrony danych została przeprowadzona w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej.**

W przeprowadzanej ocenie skutków dla ochrony danych osobowych, z uwagi na wymienione zagrożenia i specyfikę danych biometrycznych należy rozważyć, czy przetwarzanie danych biometrycznych dla realizacji określonego celu jest rzeczywiście niezbędne, tj. związana z tym **ingerencja w prywatność osoby fizycznej jest adekwatna i proporcjonalne do celu, w jakim dane te będą przetwarzane.**

Dotyczy to również sytuacji, w których podstawą przetwarzania danych biometrycznych jest dobrowolnie wyrażona zgoda osoby, której dane są przetwarzane.

Wykorzystanie danych biometrycznych przez podmioty prywatne

W odniesieniu do przypadków, gdzie podstawą prawną przetwarzania danych biometrycznych nie jest wprost przepis prawa, ich użycie musi być zgodne z ogólnie obowiązującymi przepisami prawa.

Pomioty reprezentujących organy władzy publicznej, które zobowiązane są do działania na podstawie i w granicach prawa, (art. 7 Konstytucji RP) dane biometryczne mogą przetwarzać tylko wówczas, gdy zezwala na to wprost przepis prawa.

Podmioty prywatne, dane biometryczne mogą przetwarzać obecnie na podstawie ogólnych zasad określone w przepisach UODO a w przyszłości na podstawie zasad określonych w RODO.

W każdym jednak przypadku, mając na uwadze wymienione zagrożenia związane z przetwarzaniem danych biometrycznych podjęcie decyzji w tym zakresie powinno być poprzedzone wykonaniem oceną skutków projektowanego rozwiązania dla ochrony danych.

Dziękuję za uwagę

Dr inż. Andrzej Kaczmarek, [CISA](#)

**Biuro Generalnego Inspektora Ochrony
Danych Osobowych**