Metodický pokyn pro zpracování biometrických údajů na UK

Metodika definuje pravidla a postupy pro zacházení s biometrickými údaji, které identifikují fyzické osoby, nebo které mohou být ve spojení s jinými zpracovávanými údaji s těmito osobami spojeny.

Metodika se vztahuje na veškeré biometrické údaje, které spravuje Univerzita Karlova, a to bez ohledu na místo jejich původu a čas vzniku, s výjimkou záznamů historických.

Za historické záznamy, na které se nařízení nevztahuje, se považují všechny záznamy, které nemají vztah k žijícím osobám.

Obsah

1.1 Pojmy a příklady

Metodika se drží pojmů, jak jsou definovány v OR č. 16/2018 – Zásady a pravidla ochrany osobních údajů, zejména definice pojmu osobní údaj.

1.1.1 Biometrický údaj

Biometrickým údajem je každý údaj, který má svou podstatu v biologické podstatě jedince a současně s ním mohou spojeny údaje umožňující jeho identifikaci. Příkladem údajů jsou: snímky osoby, otisky prstů, podpisy, **záznam hlasu** apod.

Metodika se týká výhradně biometrických údajů živých osob umožňujících jejich jednoznačnou identifikaci buď samostatně, nebo ve spojení s dalšími údaji, které jsou v rámci UK také zpracovávány.[1]

Biometrická šablona je uložený referenční údaj spojený s dalšími daty o osobě, který umožňuje jiné biometrické údaje porovnat a tak osobu, které se nové údaje týkají, jednoznačně identifikovat.[2]

Úřadem se v dokumentu rozumí Úřad pro zpracování osobních údajů (ÚOOÚ).

Zvláštní kategorie osobních údajů je kategorie vymezená platnou legislativou, do které biometrické údaje spadají. Jejich zpracování je v rámci UK možné pouze v případě výslovného souhlasu dotčené osoby (subjektu údajů).[3]

Rozsáhlé zpracování Rozsáhlým zpracování se pro účely metodiky rozumí zpracování údajů o minimálně 1000 subjektech.[4]

1.1.2 Využití biometrických údajů

Z hlediska nakládání s biometrickými údaji existují 3 kategorie nakládání:

---

[1] Přesné vymezení stanovuje nařízení GDPR, čl. 4 odst. 14: Biometrickými údaji jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

V negativním vymezení se metodika netýká např. lékařských biologických vzorků, u kterých není znám původce a nelze jej z do dokumentace k vzorku dohledat.

[2] Šablona může mít formu reversibilní, kdy její data lze použít pro identifikaci osoby (např. kompletní fotografie) nebo ireversibilní, kdy data není možné využít (typicky matematický model vzájemných poloh klíčových bodů tváře).

Z hlediska legislativy ale není mezi těmito šablonami rozdíl, protože lze většinou i z ireversibilního modelu získat dostatečně přesnou informaci. Viz např. [ÚOOÚ 1]

[3] Nařízení GDPR, kapitola II, čl. 9. uvádí více možných důvodů zpracování, ale jiné nejsou pro UK aplikovatelné.

[4] Viz [WP29 1]: Pojem rozsáhlého zpracování není dosud jednoznačně ukotven (ani v novějších zdrojích) a je proto třeba vycházet z rozlišení, že rozsáhlým zpracování se rozumí zpracování, které přesahuje rozsah praxe zpracování jednotlivými osobami.

1.1.2.1 Sběr bez dalšího využití

V rámci sběru jsou biometrické údaje sbírány, ale nejsou přiřazovány ke konkrétním osobám.

Příkladem jsou nahrávky přednášek nebo záznamy z kamerového systému bez rozpoznávání osob.

Důležité pro zařazení sběru do této kategorie je, že sbíraná data jsou v kvalitě, která potenciálně umožňuje jednoznačnou identifikaci třeba i následně. Existuje tedy reálný scénář, kdy uložené údaje nebyly porovnáváním s biometrickou šablonou zpracovány a UK ani šablonami nedisponuje, ale jiný subjekt, pokud by materiál získal, tuto identifikaci může provést.

Vzhledem ke kvalitě běžné používaných nahrávacích zařízení, jsou takovými údaji fotografie osob i mnoho záznamů kamer s vyšším rozlišením.[5]

1.1.2.2 Využití pro autentizaci osob

V případě využití pro autentizaci není smyslem využití identifikovat osoby, které by bez provedeného zpracování byly „anonymní“, ale ověřit, že osoba je skutečně tou, za kterou se vydává.

Typickým příkladem je použití dynamického biometrického podpisu k ověření identity osoby. Jeho použití je výhradně ve spojení s ověřováním identity podepisující osoby (autentizací) a není používáno anonymně.

Dodatečné použití šablon pro autentizaci osob pro identifikaci anonymních osob z existujících záznamů většinou nepřichází v úvahu vzhledem k charakteru těchto šablon, jejichž použití vyžaduje snímání biometrických údajů speciálním zařízením s vědomou součinností autentizované osoby, ale nelze ji paušálně vyloučit.

V rámci využívání těchto údajů je důležité rozhodnutí ÚOOÚ, které uchovávání biometrických šablon a jejich zpracování za účelem identifikace osob považuje za zpracování zvláštní kategorie osobních údajů.

1.1.2.3 Využití pro identifikaci osob

Šablony jsou využívány automatickým nebo poloautomatickým způsobem k identifikaci konkrétních osob, které by bez použití metody zůstaly neidentifikované.

---

[5] V rámci využití osobních údajů, které nejsou využity k identifikaci, je možné aplikovat ustanovení GDPR kapitola II, čl. 11: Pokud účely, pro něž správce zpracovává osobní údaje, od správce nevyžadují nebo již nevyžadují identifikaci subjektu údajů, nemá správce povinnost uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů výlučně kvůli dosažení souladu s tímto nařízením.

Na základě tohoto článku je možné údaje uchovávat bez výslovného souhlasu údajů. I nadále ovšem údaje zůstávají osobními údaji, resp. údaji zvláštní kategorie a týkají se jich ostatní ustanovení bez ohledu na to, že nejsou spojeny s identifikovanou osobou.

Typickým příkladem je rozpoznávání osob na záznamech kamerového systému. V automatizovaném režimu probíhá trvale, v poloautomatickém pouze pro sekvence vybrané předem fyzickou osobu.

Do kategorie identifikace patří i přístupové systémy využívající biometrické údaje, např. turnikety využívající snímání krevního řečiště.

1.1.2.4 Využití pro soukromé účely

V rámci UK lze předpokládat soukromé využití zejména ze strany studentů pořizujících audiovizuální záznamy přednášek. Používání těchto záznamů se se řídí metodikou práce s AV záznamy.

Obecně se tato metodika nevztahuje na jiné využití biometrických údajů, než takové, kde je UK správcem údajů. Svými činnostmi včetně činností výukových ale UK nesmí podporovat individuální vytváření a zpracování osobních údajů pracovníky nebo studenty.

Využívání údajů studenty rozebírá bod 2.3.1.

1.1.3 Příklady biometrických údajů a míst vzniku

Následující příklady uvádějí typické zdroje evidencí biometrických údajů. Výčet nesmí být považován za kompletní – neuvedení údaje zde neznamená, že není biometrickým údajem, nebo nepodléhá pravidlům stanoveným metodikou.

Údaj	**Místa vzniku**
Fotografie a videonahrávka využívající charakteristických znaků k identifikaci osob	Pokročilé kamerové systémy střežící prostory fakulty Audiovizuální nahrávka přednášky nebo diskuze uložená spolu s kontaktními informacemi o účastnících umožňující propojení audiovizuálního záznamu s dalšími údaji Audiovizuální nahrávka zkoušení spolu s identifikací zkoušeného
Vlastnoruční podpis	Kopie osobního dokladu, který podpis obsahuje. Např. podpis pracovní smlouvy. Smlouva poskytuje dostatek dalších údajů, aby bylo možné podpis spojit s konkrétní osobou.
Záznam hlasu s rozpoznáváním osoby	Záznam přednášky s uvedením přednášejícího
Otisk prstu nebo jiný jednoznačný identifikátor (oční rohovka, žilní řečiště atd.)	Přístupové systémy identifikují osoby podle biologických znaků Dokument podepsaný dynamickým podpisem
Biometrické údaje z lékařských vyšetření (např. záznam EKG)	Lékařská zpráva

Biometrickým údajem není každý záznam osoby. Např. zpracování fotografií není zpracováním biometrických údajů, pokud nejsou zpracovávány technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby.[6]

[6] Nařízení GDPR, důvod 51.

2. Pravidla pro zpracování biometrických údajů

Kapitola definuje obecná pravidla, která platí pro všechny případy zpracování, pokud není v následující kapitole uvedeno jinak.

2.1 Právo pořizování a zpracování údajů

2.1.1 Zpracování na základě souhlasu

Univerzita Karlova může biometrické údaje zpracovávat výhradně na základě výslovného souhlasu subjektu údajů Důležité je, že souhlas musí být svobodný, tj. jeho účastník musí mít právo jeho odmítnutí bez omezení poskytovaných služeb. Z toho vyplývá zásada:

Zpracování biometrických údajů nesmí být nezbytnou součástí procesů UK

Zpracování biometrických údajů může být využíváno jako nástroj usnadnění procesů (např. jednodušší identifikace) pro subjekt, nikoli jako nástroj řešení interních postupů.

Příklady aplikace:

Fotokopie osobních dokladů smí být uchovávány výhradně na základě svobodného souhlasu. Svobodným se rozumí, že návrh udělení souhlasu nesmí vyvolávat dojem nezbytnosti tohoto kroku. Pro pořízení fotokopie musí být jednoznačně stanovený účel.

Audiovizuální nahrávky ve vysokém rozlišení (zahrnuje i běžný FHD[7] záznam), pokud jsou spojeny se informací o přednášejícím, jsou biometrickým údajem a smí být zpracovávány pouze s jeho výslovným souhlasem.

2.1.2 Zpracování z důvodu oprávněného zájmu

V rámci běžných agend UK (pracovně-právní vztahy a povinnosti zaměstnavatele, zajištění studia, péče o majetek, povinnosti vůči poskytovatelům finančních prostředků, plnění úkonů výkonu státní správy) **neexistují činnosti, kde by zpracování biometrických údajů bylo možné opřít o oprávněný zájem** a nebyl nezbytný svobodně udělaný souhlas subjektu.

Příklady:

- Pracoviště UK uchovává kopii osobních dokladů za účelem ověření, že údaje byly správně opsány. Kopie je založena ve složce v uzamčené skříni pracoviště. Případ je v dalších příkladech opakovaně rozebírán jakožto příklad neoprávněného nakládání s biometrickými údaji (a podrobně rozebrán např. v [ÚOOÚ 1]). Zpracování není oprávněným zájmem UK, protože téhož lze dosáhnout méně invazivními prostředky bez zpracovávání biometrických údajů z osobního dokladu (fotografie, podpis).
- Přípravný kurz pro studenty středních škol organizovaný fakultou v prostorách fakulty vydal studentům průkazky s fotografiemi, kterými se prokazují při vstupu do budovy. Průkazky byly vygenerovány do PDF souboru, ze kterého byly tištěny. Soubor byl uchováván pro vytištění náhradní karty pro případ ztráty.

  Vytištění vstupních karet včetně fotografie je oprávněným zájmem pořádající organizace, ale potřeba tohoto kroku musí být součástí informací s nabídkou kurzu a přihlašující osoba je s tím seznámena před podáním přihlášky a zaplacení kurzovného.

[7] FHD = 1080 bodů v menším z rozměrů záznamu je běžné rozlišení obrazovek notebooků i mobilních telefonů.

Uchovávání PDF souboru je neoprávněným zpracováním, protože nenaplňuje účel identifikace osoby u vstupu. Je možné použít méně invazivního postupu – opakovaného vyfocení účastníka.

V případě, že by fotografie na členské kartě nesloužila k identifikaci osob a ochraně majetku (např. v případě kurzů pořádaných mimo budovu), je použití fotografie na průkazce možné pouze výhradně se svobodným souhlasem – účastník by měl mít možnost mít průkazku bez osobní fotografie.

2.1.3 Zpracování pro vědecké účely

Zpracování osobních údajů pro vědecké účely nespadá z hlediska členění do předchozích bodů, ale i v tomto případě je zpracování biometrických údajů ve smyslu definice z předchozí kapitoly podmíněno výslovným souhlasem subjektu. Zpracování nesmí přesáhnout rozsah uvedený v souhlasu.

Příklady:

Laboratoř vyvíjející nástroje identifikace osob podle hlasu má vzorky hlasů účastníků výzkumu. Laboratoř se na účastníky opakovaně obrací a v rámci telefonátů testují přenos algoritmů. Pro práci je proto nezbytné zpracovávat šablony jejich hlasu a mít je uchované spolu s identifikací konkrétní osoby (za jednoznačnou identifikaci je nutné považovat i mobilní telefonní číslo soukromého telefonu, i když tým nemusí nutně vědět jméno nebo další osobní údaje). Tým pracuje s biometrickými údaji a musí mít pro jejich zpracování potřebný souhlas subjektů.

Laboratoř např. pro potřeby výzkumu nesmí využít nahrávek telefonických hovorů ze záznamníku katedry bez prokazatelného souhlasu osob, které záznam zanechaly.

Biometrické údaje nesmí být uchovávány po ukončení vědeckého výzkumu. Souhlas subjektů udělený pro určitý výzkum nesmí být zobecňován pro jiný výzkum, ani kdyby šlo o výzkum vedený stejným týmem v příbuzné oblasti. Pro další výzkum mohou být údaje použity pouze v případě nového souhlasu nebo po jejich anonymizaci.

2.1.3.1 Anonymizace údajů

Biometrické údaje, pokud nejde o dlouhodobé studie, je pro vědecké účely většinou možné zpracovávat anonymizované. Principy anonymizace se mohou uplatnit na biometrické údaje stejným způsobem, jako na jiné druhy osobních údajů.

Příklady:

Záznamy EKG jsou zkoumány s ohledem na možnost odhalení srdeční choroby. Vzorky mohou být zpracovávány anonymně s tím, že spolu se vzorkem je známo, zda u subjektu byla choroba odhalena jinými prostředky. Přesto není důvod, aby vědeckému týmu byla známa totožnost osoby. I když je EKG zápis biometrickým údajem, bez dalších údajů na jeho základě nelze obecně osobu určit (např. porovnáním s jinými záznamy) a lze je zpracovávat

jako údaje nepodléhající ochraně osobních údajů včetně např. zveřejnění signifikantní sekvence v rámci vědecké práce bez souhlasu subjektu.

Na výzkum uvedený výše (rozpoznávání hlasu) není možné anonymizaci využít, protože laboratoř s osobami, které vzorek poskytly, spolupracuje při výzkumu (kontaktuje je opakovaně). Anonymní vzorky jsou v tomto případě nepoužitelné. Laboratoř musí zpracovávat a chránit vzorky v souladu se zásadami zabezpečení osobních údajů.

2.1.4 Zpracování na základě smlouvy

Zpracování na základě smlouvy je analogií zpracování na základě souhlasu v tom smyslu, že účastník vyjadřuje souhlas uzavřením smlouvy.

Stále se objevuje mylný výklad, kdy organizace zpracovává osobní údaje a odvolává se na smlouvu s třetím subjektem, typicky poskytovatelem dotace. Tento výklad je zcela chybný! Smluvní základ je relevantní výhradně v případě, kdy smluvním partnerem je subjekt, jehož údaje jsou zpracovávány.

Rozdíl smluvního základu oproti souhlasu je v tom, že smlouva může obsahovat další ustanovení. Typicky omezuje právo subjektu od smlouvy odstoupit bez vyrovnání závazků nebo právo organizace uchovávat údaje i po ukončení poskytování služby pro případné reklamace nebo jiné oprávněné nároky organizace.

Z hlediska zpracování biometrických údajů platí pro smluvní základ stejné pravidlo, jako pro souhlas: Zpracování je možné výhradně v rozsahu stanoveném smlouvou, kterou subjekt svobodně uzavřel.

2.2 Zdůvodnění zpracování a související dokumentace

Je nezbytné, aby zpracování bylo podloženo zdůvodněním, proč je nezbytné využívání biometrických údajů. Důvodová zpráva je nezbytná i v případě, že je zpracování prováděno na základě souhlasu subjektu.

Zdůvodnění musí obsahovat:

- Proč není možné použít zpracování bez použití biometrických údajů.
- Jaká je přidaná hodnota pro subjekt údajů, která opravňuje jejich použití.
- V případě odvolávání se na oprávněný zájem je nezbytný balanční test zpracování údajů.
- Balanční test je nezbytný vždy v případě systémů zpracovávajících audiovizuální obraz z veřejně přístupných prostor.[8]

[8] [ÚOOÚ] důvod 91. Poznámka: Je velmi nepravděpodobné, že by UK měla pro toto zpracování oprávněný důvod. Protože identifikace osob je v tomto případě záležitostí orgánů činných v trestním řízení a UK by jej měla provádět výhradně v součinnosti a na základě pokynů těchto orgánů.

Výše uvedená poznámka se nevymezuje proti sledování veřejně přístupných prostor (např. chodeb budov) kamerovým systémem obecně, ale proti sledování s následným zpracováním záznamu za účelem identifikace osob, které se v prostoru pohybují.

- Pro každou kategorii údajů musí existovat vymezení, kteří příjemci k nim musí mít přístup a v jaké části jejich zpracování.

Dokumentace agendy zpracování musí zahrnovat:

- Ověření, že biometrické údaje jsou zpracovávány pouze subjekty z Evropské unie.[9]
- Podrobný účel zpracování jednotlivých kategorií osobních údajů. Nad rámec popisu agend tak musí být samostatně popsáno zpracování biometrických údajů, aby nemohlo dojít k mýlce, které kategorie údajů se které zpracování týká.
- Kategorie příjemců, kteří budou nebo mohou mít přístup k biometrickým údajům.
- Popis zabezpečení údajů samostatně pro každou kategorii údajů. Zabezpečení musí zahrnovat
    - Ochranu před neoprávněným přístupem (zabezpečení přístupu);
    - účinnou ochranu i v případě neoprávněného přístupu (typicky šifrování, oddělení biometrických dat od jiných údajů umožňujících identifikaci osoby);
    - kontrolu každého jednotlivého přístupu k biometrickým údajům spolu se zdůvodněním, proč bylo vykonáno odkazem na dokumentovaný způsob zpracování (vyžaduje logování přístupu s možností identifikace konkrétní osoby a důvodu použití. V případě automatického zpracování vyžaduje logování operací, ke kterým byla data využita);
- Popis zaručeného mechanismu odstraňování biometrických údajů, když pomine důvod jejich zpracování.[10]
- Pokud biometrické údaje zpracovávají společní správci, musí se dokumentace vztahovat ke zpracování u všech společných správců. UK nesmí přenechat odpovědnost na jiném společném správci bez toho, aby se pracovníci ubezpečili o plnění všech požadavků této a ostatních metodik UK.

Každé místo zpracování biometrických údajů musí být jednoznačně identifikováno a střeženo. V případě porušení zabezpečení jakýchkoli osobních údajů musí být zřejmé, zda byla porušena i ochrana zabezpečení biometrických údajů.[11]

V případě rozsáhlého zpracování musí být součástí dokumentace i souhlasné stanovisko pověřence pro ochranu osobních údajů.

Příklady logování:

Laboratoř uchovávající vzorky hlasu pro testování (viz příklad z bodu 2.1.3) uchovává záznamy v úložišti s chráněným přístupem s tím, že úložiště neobsahuje identifikace osob, pouze hlasové vzorky. Při využití pro testování je vytvořen záznam, který zaznamená, kteří pracovníci prováděli testování a

[9] Viz [GDPR] čl. 27, odst. 2 písm. a)

[10] Zaručený způsob musí být automaticky spouštěný v okamžiku, kdy pominou důvody zpracování těchto údajů. Odstranění nesmí být závislé na paměti osob (někdo si musí vzpomenout) ani spojeny s událostmi, které nastávají až s odstupem po ukončení důvodů pro zpracování biometrických údajů (typicky skartace složky několik let po uplynutí její skartační lhůty).

[11] Informace, že porušení bezpečnosti zahrnuje i biometrické údaje je i součástí hlášení Úřadu pro ochranu osobních údajů ([GDPR] čl. 33, odst. a)

kdy. Záznam v tomto případě neobsahuje obsahovat identifikace konkrétních osob (aby nevznikala další evidence osobních údajů), ale identifikátory použitých vzorků, které samy o sobě nevytváří evidenci osobních údajů. Přehled identifikátorů může být nahrazen informací, že byl použit celý soubor zkušebních biometrických šablon.

2.3 Odpovědnost za zpracování

UK nese plnou odpovědnost za zpracování údajů i v případě, že ji vykonává zpracovatel na základě smlouvy s UK.

Poznámka: Viz bod 3.1.4 pro zajištění odpovědnosti při společném výzkumu

Příklad:

Externí zpracovatel – bezpečnostní agentura – zajišťuje ostrahu objektu UK. Činí tak na základě smlouvy s UK. Pokud mají pracovníci agentury přístup k záznamům kamerového systému, nesmí v rámci zpracování využít data k identifikaci osob (AV údaje by se staly biometrickými údaji).

Pokud by celý kamerový systém byl majetkem bezpečnosti agentury a veškeré zpracování probíhalo jejich prostředky a pracovníky, je správcem dat agentura, nikoli UK. Pokud by byly údaje současně biometrickými údaji, musí splnění podmínek legislativy zajistit správce, tedy bezpečnostní agentura.

2.3.1 Biometrické údaje v rámci studentské práce

Pokud jsou studenti zapojeni do vědecké práce, která pracuje s biometrickými údaji, vztahují se na ně stejná pravidla, jako na jakéhokoli jiného člena týmu, viz bod 3.1.4.

V rámci výsledků práce nikdy nesmí být biometrické údaje zveřejňovány.

Vedoucí práce je odpovědný za poučení studenta o:

- Obecných pravidlech ochrany osobních údajů
- Zvláštní kategorii biometrických údajů
- Vymezení kategorie biometrických údajů v rámci osobních údajů
- Jak fungují nastavené principy ochrany biometrických údajů (např. oddělení biometrických dat od identifikačních osobních údajů)
- Jaká jsou pravidla zabezpečení v konkrétní práci / projektu
- Jaké zásady musí dodržovat student při vlastní práci

Příklad:

Student se podílí na psychologických výzkumech, v rámci kterých jsou účastníci výzkumu nahrávání videokamerou. Student musí být poučen, že např. nesmí pro videonahrávky využít vlastní mobilní telefon nebo si nahrávky ukládat na notebook a to ani v případě, že má např. šifrovaný disk.

3. Zabezpečení biometrických údajů

Uchovávání biometrických údajů musí být zajištěno tak, aby byly maximálně omezeny možnosti jejich zneužívání. Do kategorie zneužívání patří jakékoli využívání mimo důvody, pro které byly pořízeny, a které byly výslovně uvedeny v souhlasu, který subjektu udělil.

3.1.1 Šifrování

Uložené údaje musí být uchovávány šifrované tak, aby nebyly využitelné bez znalosti nebo nástroje, který není spolu s údaji dostupný.

Pro autentizaci jsou uchovávány biometrické šablony. Ty by měly být uchovávány tak, aby z nich nebylo možné zpětně získat ucelený biometrický údaj nebo jeho podstatnou část (tzv. hash). I hash musí být uchováván jako osobní údaj s dostatečnou mírou ochrany.[12]

3.1.2 Minimalizace kopií

Biometrické údaje mohou být zpracovány výhradně s účelem, ke kterému byly pořízeny. Proto mohou být uloženy pouze v místě (typicky v systému), který je zpracovává a nesmí být sdíleny s jinými systémy. Konkrétně nesmí být do jiných míst přenášeny nebo jiným systémům umožněno, aby biometrické údaje využívány, nebo využívaly služby systému, který data zpracovává a který je pro služby poskytnuté jiným systémům využije.

> *Příklady:*
>
> Fakulta má fotografii studenta pořízenou za účelem vytvoření přístupové karty na pracoviště. (Pozor: Pro uchovávání musí mít svobodný souhlas, který uchovávání uvádí!) Tuto fotografii nesmí pracoviště poskytnout jinému pracovišti k žádnému účelu.
>
> Systém fakulty uchovává šablonu biometrického podpisu používaného pro ověření dokumentu. Tento systém nesmí nabízet službu ověření biometrického podpisu jiným systémům (např. na jiných fakultách), pokud výslovnou součástí souhlasu nebylo sdílení tohoto údaje mezi fakultami.
>
> Docházkový systém uchovává hashe otisků prstů. Tento hash nesmí být součástí dat, které docházkový systém sdílí s jinými systémy, a to ani v případě, že by tyto jiné systémy hash nevyužívaly.

[12] Bylo opakovaně prokázáno, že i z tzv. „hashe“ je současnými technickými možnostmi získat dostatek informaci na vytvoření takové náhrady původních biometrických údajů, které umožňují falešné prokázání identity. Viz např. [ÚOOÚ 1]. „Hashem“ se rozumí provedení takové matematické operace, kterou není možné inverzní operací získat zpět původní biometrické údaje, ale při provedení stejné operace s jinými údaji je možné porovnat, zda nové údaje jsou dostatečně podobné šabloně.“

3.1.3 Logování přístupů

Pokud jsou někde uchovávány biometrické údaje, musí být veškeré přístupy k místu jejich uložení logovány[13].

Příklady:

Pokud jsou uloženy někde např. fotokopie osobních dokladů, musí být každý konkrétní přístup k nim zaznamenán. Není proto např. možné, aby fotokopie dokladu byla v papírové složce v zamčené skříni, jejíž klíč je pracovníkům pracoviště dostupný. (Upozornění: Pro fotokopii musí být doložitelný také výslovný souhlas).

Pokud je kopie vlastnoručního podpisu součástí smlouvy, smlouva nesmí být zveřejněna na internetu, ani nesmí být volně přístupná v rámci interních informačního systému tak, aby k její fotokopii s podpisem měli přístup pracovníci, kteří nepotřebují autentizovat podepisující osobu.

Další příklady viz bod 2.2.

3.1.4 Zabezpečení v rámci výzkumu vedeného více pracovišti

Pokud jsou biometrické údaje zpracovávány v rámci výzkumu více pracoviště, vždy musí být maximálně uplatněna možnost jejich anonymizace před předáním jinému pracovišti.

Příklad:

Nemocnice sbírá osobní údaje i biometrická data o pacientech na základě souhlasu o zapojení do výzkumu. Data jsou analyzována na pracovišti UK. Toto pracoviště přímo osoby nekontaktuje a nepotřebuje proto znát identifikační údaje osob, kterých se data týkají. Osobní údaje včetně biometrických proto jsou vždy předávány anonymizované.

Pokud jsou předávány opakovaně údaje o stejných pacientech, jsou anonymizovány tak, aby pracoviště mohlo sledovat, které vzory patří ke stejné osobě, ale přesto není důvod, aby znalo jejich identitu.

Je-li nezbytné, aby pracovníci různých pracovišť spolupracovali na využívání osobních údajů včetně biometrických dat, mělo by být využito vzdáleného přístupu ke sdílenému úložišti spravovaného jednou organizací, aby byla dodržena zásada minimalizace dat i jejich kopií.

Úroveň zabezpečení vzdáleného přístupu musí být adekvátní citlivosti zpracovávaných údajů a požadavku na ověření přistupujících osob, logování jejich přístupů a dokumentace

[13] Viz příkaz [ÚOOÚ 6], kde Úřad vytýká nedostatek: Správní orgán k dané věci dále uvádí, že logování přístupů k osobním údajům je jedním z nejzákladnějších prvků zabezpečení zpracovávaných osobních údajů v informačních systémech a zcela běžným prvkem, který automatizované systémy obsahují. V případě, že se jedná o rozsáhlé zpracování osobních údajů a bez řádného logování tak nelze zajistit, aby nedošlo k neoprávněným přístupům a jinému nedovolenému zpracování, resp. zjistit, kdo případnou změnu provedl, musí správce zajistit, aby i oprávněné osoby (v tomto případě oprávnění zaměstnanci příslušného služebního úřadu) přistupovaly k osobním údajům pouze tehdy, mají-li k tomu relevantní důvod. Oprávněnost přístupu však nelze zpětně ověřit, pokud není systém vybaven logováním.

důvodů, proč se k biometrickým údajům přistupovalo. Doporučeným postupem zabezpečení jsou osobní certifikáty členů týmu nebo dvoufaktorová autentizace.

3.2 Rozsah a doba uchovávání údajů

V případě biometrických (i ostatních osobních údajů) musí být zajištěno, že údaje jsou zpracovávány (zahrnuje i uchovávání bez aktivního využívání) výhradně po dobu, kdy jsou nezbytně nutné pro účel, ke kterému byly pořízeny.

Příklad:

Fotografie pracovníka byla pořízena pro přístupový systém. Fotografie nesmí být uchovávána, pokud pracovník už na střežené pracoviště nechodí a jeho fotografie proto již pro identifikaci neslouží. Pokud je známo nebo existuje důvodný předpoklad, že se pracovník na pracoviště zase vrátí (např. po ukončení studijního pobytu v zahraničí), je možné jeho fotografii v systému uchovat, ale pouze v případě, že toto uchování pro budoucí znovuvyužití bylo výslovnou součástí souhlasu, který pracovník udělil. Uchování pro budoucí opakované využít je jiným způsobem využití údajů, navíc má pracovník důvod předpokládat, že údaje jsou odstraněny po ukončení jeho působnosti automaticky na základě principu minimalizace údajů.

UK smí uchovávat jenom nejmenší množství osobních údajů nezbytných pro identifikaci osoby. Nesmí uchovávat více údajů, než je nezbytné.

Příklad:

Pokud se na základě souhlasu pořizuje např. kopie osobního dokladu a není nezbytné uchovávat kopii podpisu, nesmí být podpis součástí kopie.

Pokud přístupové zařízení využívá výhradně otisku prstu pro identifikaci osoby, nesmí být součástí záznamu osoby jiné biometrické údaje, např. fotografie.

Biometrické údaje nesmí být uchovávány pro účely, pro které není nezbytné uchovávat biometrické údaje, a postačily by údaje nespadající do zvláštní kategorie.

Příklad:

Nesmí být uchovávána kopie osobního dokladu subjektu za účelem možnosti ověřit údaje z něj opsané (typicky jméno příjmení, místo a datum narození). Pokud by se taková kopie uchovávala, smí obsahovat pouze uvedené ověřované osobní údaje a nikoli údaje další (fotografie, podpis nebo jakékoli další údaje, např. pohlaví). Fotokopie by musela být začerněna nebo jinak omezen obsah informací, které jsou na ní dostupné.

3.2.1 Zpracování z důvodu oprávněného zájmu

Bez souhlasu zaznamenaných osob může být AV záznam zpracováván výhradně na základě oprávněného zájmu. V takovém případě je třeba zpracovat balanční test a vyhodnotit, zda oprávněný zájem UK je důležitější než právo osob na ochranu soukromí.

Oprávněný zájem nikdy nemůže být důvodem ke zveřejnění záznamu širší skupině osob, např. na internetu. Výjimka z tohoto pravidla může být povolena výhradně po konzultaci s pověřencem pro ochranu osobních údajů.

> *Poznámka:* V podobných případech, kdy data nejsou přímo součástí vědeckého výzkumu, by neměl být vědecký výzkum používán pro zdůvodnění zpracování; ten je možné výhradně ve svém významu. V opačném případě může subjekt oprávněně požadovat odstranění údajů, protože jejich odstranění neohrožuje významně splnění cíle.

4. Použité zdroje a podklady

Pokyny metodického pokynu se kromě legislativy opírají zejména o již vydané výroky a rozhodnutí Úřadu, které jsou pro aplikaci v rámci ČR rozhodující:

[GDPR] Nařízení EP a rady EU 2016/679 včetně následných doplnění https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6607&n=uplne%2Dzneni%2Dgdpr

[MKG2019] Biometrické údaje a jejich právní režim, Revue pro právo a technologie, ročník 8, číslo 2, rok 2019, dostupné online: https://journals.muni.cz/revue/article/view/8801/pdf

[ÚOOÚ 1] Čtrnáct nedorozumění ohledně biometrické identifikace a autentizace https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=43934

[ÚOOÚ 2] Kontrola využití biometriky u klientů (UOOU-09654/18) https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6546&n=kontrola%2Dvyuziti%2Dbiometriky%2Du%2Dklientu%2Duoou%2D09654%2D18

[ÚOOÚ 3] Kontrola používání technologie FaceID https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5677&n=kontrola%2Dpouzivani%2Dtechnologie%2Dfaceid%2Dspolecnost%2Dmetrostav%2Da%2Ds

[ÚOOÚ 4] Kontrola používání hlasové biometrie https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5691&n=kontrola%2Dpouzivani%2Dhlasove%2Dbiometrie%2Dspolecnost%2Dceska%2Dsporitelna%2Da%2Ds

[ÚOOÚ 5] Kontrola zpracování osobních údajů včetně zvláštních kategorií (otisků prstů) při provozování hazardních her https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=6289&n=kontrola%2Dzpracovani%2Dosobnich%2Dudaju%2Dvcetne%2Dzvlastnich%2Dkategorii%2Dotisku%2Dprstu%2Dpri%2Dprovozovani%2Dhazardnich%2Dher

[ÚOOÚ 6] Příkaz ÚOOÚ o neoprávněném uchovávání kopií osobních dokladů https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=41094

[eprávo 1] Zpracování biometrických údajů zaměstnanců https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html

[WP29 1] Pokyny týkající se pověřenců pro ochranu osobních údajů https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34787