Pravidla pro zpracování biometrických údajů

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:
- *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 záznam), pokud jsou spojeny s informací o přednášejícím, jsou biometrickým údajem a smí být zpracovávány pouze s jeho výslovným souhlasem.*

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 úkolů v rámci výkonu státní správy) **neexistují činnosti, kde by zpracování biometrických údajů bylo možné opřít o oprávněný zájem** a nebyl nezbytný svobodně udělený souhlas subjektů údajů.

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 souborů, 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 kurzů a přihlašující osoba je s tím seznámena před podáním přihlášky a zaplacením kurzovného.*
- *Uchovávání PDF souborů 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 výhradně se svobodným souhlasem – účastník by měl mít možnost mít průkazku bez osobní fotografie.*

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 subjektů údajů. 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.

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 subjektů 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, tzn. například údaje tzv. Pseudonymizovat.*

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 krom jiného také 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.

Zdůvodnění zpracování a související dokumentace

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

<u>Zdůvodnění musí obsahovat:</u>

- 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 osobních údajů.
- Balanční test je nezbytný vždy v případě systémů zpracovávajících audiovizuální obraz z veřejně přístupných prostor.
- Pro každou kategorii údajů musí existovat vymezení, kteří příjemci k nim musí mít přístup a v jaké části jejich zpracování.

<u>Dokumentace agendy zpracování musí zahrnovat:</u>

- Ověření, že biometrické údaje jsou zpracovávány pouze subjekty z Evropské unie.
- Podrobný účel zpracování jednotlivých kategorií osobních údajů. Nad rámec popisů agend tak musí být samostatně popsáno zpracování biometrických údajů, aby nemohlo dojít k mýlce, které kategorii osobních údajů, se které zpracování týká.
- Kategorii příjemců, kteří budou nebo mohou mít přístup k biometrickým údajům.
- Popis zabezpečení údajů samostatně pro každou kategorii údajů.

<u>Zabezpečení musí zahrnovat:</u>

- 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.
- Vyjádření, že dokumentace se vztahuje na zpracování u všech společných správců, pokud biometrické údaje zpracovávají společní správci. UK nesmí přenechat odpovědnost na jiném společném správci bez toho, aby se pracovníci ubezpečili o splnění 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. V případě rozsáhlého zpracování musí být součástí dokumentace i souhlasné stanovisko pověřence pro ochranu osobních údajů.

Příklad logování:

- *Laboratoř uchovávající vzorky hlasů pro testování 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 kdy. Záznam v tomto případě neobsahuje 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.*

Odpovědnost za zpracování

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

Příklady:

- *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.*

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. V rámci výsledků práce nesmí být biometrické údaje nikdy 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
- fungování nastavených principů ochrany biometrických údajů (např. oddělení biometrických dat od identifikačních osobních údajů)
- pravidlech zabezpečení v konkrétní práci/projektu
- zásadách, které musí student dodržovat při vlastní práci

Příklad:

- *Student se podílí na psychologických výzkumech, v rámci kterých jsou účastníci výzkumu nahráváni 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.*