Ochrana osobních údajů v Českém národním registru dárců dřeně o.p.s. ve vztahu k požadavkům GDPR

Účel a předmět

Nařízení (EU) 2016/679 (GDPR) představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich osobními údaji. Toto nařízení se nevztahuje na osobní údaje zesnulých osob. Český národní registr dárců o.p.s. (dále jen ČNRDD) je povinným subjektem, při zpracovávání osobních údajů se uvedeným nařízením řídí.

Toto SOP uvádí pravidla a povinnosti při zpracovávání osobních údajů fyzických osob a stanovuje obecné postupy pro zabezpečení osobních údajů, předejití náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Pojmy

Dokumentace GDPR
Dokumentace, která slouží k prokazování souladu s Nařízením dozorovému úřadu, je vedena v písemné i elektronické podobě a uložena u pověřence.

Dozorový úřad
Úřad pro ochranu osobních údajů (ÚOOÚ).

Incident
Za incident lze považovat jakoukoli událost, která představuje odchylku od zavedeného systému zabezpečení osobních údajů.

Osobní údaje
Pojem „Osobní údaje“ zahrnuje standardní kategorii osobních údajů a zvláštní kategorii osobních údajů.

Pověřenec pro ochranu osobních údajů (DPO)
Pověřenec pro ochranu osobních údajů slouží jako prvek, který dbá, aby zpracování osobních údajů u správce bylo v souladu s obecným nařízením GDPR.

Správce (ČNRDD)
Subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely, např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Standardní kategorie osobních údajů
Jakákoli informace týkající se identifikované či identifikovatelné fyzické osoby a skutečnost, že identifikace, resp. identifikovatelnost může nastat různými způsoby, ne vždy pouze podle jména, příjmení, adresy a data narození, ale i např. kódem, který je třeba zaměstnanci přidělen či IP adresou atd.

Subjekt údajů
Fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se výlučně k právnické osobě tak nejsou osobními údaji.

Zpracování
Jakákoli operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání,

uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zvláštní kategorie osobních údajů

Zvláštní kategorie osobních údajů, které zasluhují vyšší stupeň ochrany, jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. V případě ČNRDD jde o údaje získané ze zdravotních dotazníků, případně vyšetření provádění při náboru a v případě shody s potenciálním příjemcem.

Související externí a interní dokumenty

- Nařízení evropského parlamentu a rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Ochrana soukromí - prohlášení na webových stránkách ČNRDD
- Informování zaměstnance o zpracování osobních údajů
- Informovaný souhlas zaměstnance
- Smlouva o údržbě hardware a software, bod.č.3

Právní důvody zpracování OÚ

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

- ✓ zpracování je nezbytné pro splnění právní povinnosti, která se na ČNRDD, jako správce vztahuje,
- ✓ zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- ✓ zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je ČNRDD jako správce pověřena (tedy vyhledávání a identifikace nepříbuzného dárce pro daného pacienta)
- ✓ zpracování je nezbytné pro účely oprávněných zájmů ČNRDD či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů,
- ✓ zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- ✓ subjekt údajů udělil souhlas pro jeden či více konkrétních účelů.

Dokumentace GDPR

Záznamy o činnostech zpracování

Záznamy o činnostech zpracování jsou povinnou dokumentací ČNRDD a jsou určeny k doložení souladu s GDPR. Jedná se o přehled všech kategorií osobních údajů, které ČNRDD zpracovává a způsobů jejich zpracování. Vedení záznamů o zpracování a jejich aktualizace je v kompetenci pověřence. Záznamy o zpracování jsou vyhotoveny v písemné (počítá se i elektronická forma) podobě a na požádání jsou předkládány dozorovému úřadu. Záznamy o činnostech zpracování obsahují:

- jméno a kontaktní údaje ČNRDD a pověřence pro ochranu osobních údajů,
- účely zpracování,
- popis kategorií subjektu údajů a kategorií osobních údajů,

- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace,
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Záznamy o činnostech zpracování jsou průběžně aktualizovány. Vznik nového zpracování osobních údajů nebo změna či zánik již existujícího musí být osobou odpovědnou za zpracování neprodleně oznámeno pověřenci. Pověřenec dozoruje, aby zpracování osobních údajů pro nový či modifikovaný účel bylo v souladu s příslušnými ustanoveními GDPR.

Práva subjektu údajů

Přehled práv subjektu údajů

Přehled práv, jež mají fyzické osoby v postavení subjektů údajů k dispozici dle GDPR:
- Právo být informován o zpracování osobních údajů, čl. 13, 14
- Právo na přístup k osobním údajům, čl. 15
- Právo na opravu nepřesných osobních údajů, čl. 16
- Právo na výmaz (být zapomenut), čl. 17, odst. 1
- Právo na omezení zpracování, čl. 18
- Právo na přenositelnost údajů, čl. 20
- Právo vznést námitku, čl. 21

Omezení práv subjektu údajů

V následujících vyjmenovaných případech je právo subjektu údajů omezeno a žádosti subjektu údajů o uplatnění práv tak nelze vyhovět.
Právo být informován o zpracování osobních údajů (čl. 14), a to v případě, že osobní údaje nebyly získány od subjektu údajů – např. při zajištění návaznosti dalších zdravotních a sociálních služeb poskytovaných pacientovi ve smyslu ustanovení § 45 odst. 2 písm. g) zákona č. 372/2011 Sb., o zdravotních službách.
Právo na výmaz (čl. 17), a to v případě dodržení lhůty pro uchování osobních údajů stanovené právními předpisy (§ 53-69 zákona č. 372/2011 Sb., Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci).
Právo na přenositelnost (čl. 20) lze realizovat pouze za kumulativního splnění 2 podmínek: zpracování je založeno na souhlasu nebo smlouvě a jedná se o automatizované zpracování. Při poskytování zdravotních služeb a zpracování zdravotnické dokumentace v mezích platných právních předpisů se toto právo neuplatní.

Právo být informován o zpracování osobních údajů

Subjekt údajů má právo na určité informace o zpracování jeho osobních údajů (např. o účelu zpracování, totožnost správce, o jeho oprávněných zájmech, o příjemcích osobních údajů). Aktivitu musí vůči subjektu údajů vyvinout ČNRDD jako správce a požadované informace stanovené v GDPR subjektu údajů poskytnout, resp. zpřístupnit.

Žádosti subjektu údajů

Subjekt údajů uplatňuje svá práva s výjimkou práva být informován o zpracování osobních údajů na základě žádosti. Evidence a vyřizování žádostí o uplatňování práv subjektu údajů je v kompetenci

pověřence. Forma žádosti i jejího vyjádření je elektronická, pokud žadatel nepožádá o vyřízení jinou formou. Odpovědné osoby poskytují pověřenci potřebnou součinnost pro možnost řádného vyřízení žádostí.

Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je zaměstnanec ČNRDD jmenovaný ředitelem ČNRDD nebo nebo externí subjekt, který je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností. Pověřenec zajišťuje:

- poskytování informací a poradenství řediteli ČNRDD
- monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů, poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování,
- vyřizování žádostí subjektu údajů,
- spolupráci s dozorovým úřadem,
- hlášení narušení bezpečnosti osobních údajů dozorovému úřadu,
- kontakt s dozorovým úřadem v záležitostech týkajících se zpracování, včetně předchozí konzultace, a případně vedení konzultací v jakékoli jiné věci.

Pověřenec dále zajišťuje dohled nad zpracovatelskými operacemi:

- vede a dle potřeby aktualizuje záznamy o činnostech zpracování;
- při vzniku potřeby nové zpracovatelské operace, nebo změny již existující, spolupracuje při přípravě návrhu procesů a podkladů k rozhodnutí vedení ČNRDD související s:
    - dodržením zásad zpracování osobních údajů a zvláštních kategorií osobních údajů;
    - přípravou smlouvy o zpracování osobních údajů v případě, že zpracovatelskou operaci nebo její část bude provádět zpracovatel;
    - vyhodnocováním rizik pro práva a svobody subjektů údajů:
    - v případě, že riziko bude vyhodnoceno jako vysoké, posuzuje právní základ nového zpracování a vyjadřuje se k nutnosti, zda provést či neprovést posouzení vlivu na ochranu osobních údajů;
    - v případě kladného vyjádření ve spolupráci s odpovědnými zaměstnanci provádí posouzení vlivu zamýšlené operace zpracování na ochranu osobních údajů a případně zahájí konzultační činnost s dozorovým úřadem;
    - o rozhodnutí dozorového úřadu neprodleně informuje vedení ČNRDD;
    - požadavky na zabezpečení osobních údajů.
- při zániku zpracovatelské operace, nebo jakékoli její části, spolupracuje při přípravě návrhu procesů a podkladů pro rozhodnutí správce, související s:
    - dobou uchování osobních údajů za účelem archivace, pokud není určena platným skartačním plánem;
    - rozsahem a typy osobních údajů, které budou pro případnou archivaci uchovány.

Pravidla ochrany osobních údajů v ČNRDD

Všichni zaměstnanci ČNRDD jsou při zpracovávání osobních údajů fyzických osob povinni dodržovat pravidla a povinnosti stanovené interními předpisy pro používání a zabezpečení OÚ, předejití

náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
Při manipulaci a uchovávání dokumentů v listinné formě a s elektronickými nosiči obsahující OÚ musí být přijata opatření, která zamezí nahodilému či neoprávněnému přístupu k osobním údajům - uzamykatelné úschovné objekty např. trezory, skříně, kartotéky, kontejnery a uzamykatelné prostory s kontrolovaným vstupem pouze oprávněných osob. Při manipulaci a uchovávání dokumentů v elektronické formě obsahující OÚ musí být dodržována pravidla nakládání s přihlašovacími údaji (hesla, PIN apod.), zabezpečení PC v nepřítomnosti zaměstnance (odhlášení uživatele). Ukládání dat mimo WM je možné pouze na sdíleném úložišti příslušného ZOK.
Zaměstnanci jsou povinni k osobním údajům přistupovat jen tehdy, pokud je to nezbytné k výkonu jejich práce a využívat je pouze k výkonu práce. Zaměstnanci zejména nesmí používat osobní údaje pro soukromou potřebu, např. zjištění informací o blízkých osobách, sousedech či známých, zjištění informací na žádost známého apod. Zaměstnanci jsou dále povinni v maximální možné míře uplatňovat zásadu „prázdného stolu“ a nenechávat pokud možno žádné dokumenty nebo datová média obsahující osobní údaje volně na svém pracovišti v době nepřítomnosti. Při opuštění pracoviště je povinen uzamknout skříně, zásuvky stolů, ve kterých jsou dokumenty obsahující osobní údaje uchovávány.
Za zavedení konkrétních technických a organizačních opatření pro zabezpečení ochrany OÚ s přihlédnutím ke specifikům jednotlivých pracovišť zodpovídají vedoucí zaměstnanci. Nedodržení pravidel a postupů při nakládání s osobními údaji je bráno jako porušení pracovních povinností.

Hlášení narušení bezpečnosti osobních údajů

Za incident lze podle GDPR považovat jakékoli porušení zabezpečení, pokud vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění osobních údajů. Incident může z povahy věci vzniknout mnoha způsoby – v důsledku cíleného útoku, úmyslného či nedbalostního jednání ze strany zaměstnance (neoprávněné poskytnutí OÚ, ztráta USB-klíče, či jiného nosiče údajů, atd.), v důsledku pochybení třetí strany (zpracovatele), ale i při selhání techniky.

Školení zaměstnanců

S dodržováním zásad ochrany osobních údajů jsou zaměstnanci seznámeni v rámci adaptačního procesu při nástupu do ČNRDD. Povinné pravidelné školení zaměstnanců v oblasti ochrany osobních údajů je realizováno prostřednictvím pravidelných školení.

Kontrolní činnost

Kontrolní činnost zaměřenou na plnění požadavků GDPR provádí:
– pověřenec

Zaměření kontrolní činnosti:
- manipulace s dokumenty obsahující osobní údaje (zdravotnická dokumentace, osobní spisy zaměstnanců, klientské informace, ostatní písemnosti apod.) se zaměřením na jejich ukládání do úschovných objektů nebo určených prostor a uzamykání těchto úschovných objektů a prostor;
- zabezpečení počítačů v nepřítomnosti zaměstnance (odhlášení uživatele);
- dodržování pravidel nakládání s přihlašovacími údaji (hesla, PIN apod.);
- aktuálnost záznamů o činnostech zpracování;
- realizace technických a organizačních opatření.

Kontrolní činnost je prováděna průběžně tak, aby alespoň 1 x ročně byl zkontrolován celý rozsah zpracování osobních údajů.

ZMĚNY/REVIZE:

datum:	revidoval/schválil:	Podpis:	revize/změna*:
1.7.2018	Jindra/PJ, Pagáč/DP		Implementace SOP.
10.2.2020	Jindra/PJ, Pagáč/DP		**Výroční revize, beze změn, compliance se std WMDA 2020.**
1.10.2022.	Jindra/PJ, Pagáč/DP		**Výroční revize, beze změn.**

* silně vyznačeny pravidelné roční revize