Andrea Nedvědová, Laktační poradenství,
Vyšehrad 681, 549 41 Červený Kostelec
Tel.: 773 930 255
e-mail: nedvedova@kojenideti.cz
IČO: 048 61 108

Bezpečnostní směrnice
na ochranu osobních údajů

Obsah

Účel a cíl bezpečnostní směrnice

Táto bezpečnostní směrnice stanovuje pravidla pro zpracování osobních údajů fyzických osob a popisuje základní požadavky, povinnosti a opatření při zpracování osobních údajů. Cílem je zabezpečit ochranu osobních údajů při manuálním a automatizovaném zpracování v souladu se zákonem č. 101/2000 Sb. o ochraně osobních údajů a v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Rozsah platnosti

Směrnice je závazná pro ty zaměstnance a spolupracovníky, kteří při své činnosti přicházejí do styku s osobními údaji fyzických osob zpracovávaných ve jménu provozovatele. Porušení směrnice se považuje za závažné porušení pracovní disciplíny a závažné porušení spolupráce.

Směrnice je určená:

- Zaměstnancům provozovatele, pokud provozovatel zaměstnance má,
- smluvním a jiným partnerům majícím možnost přístupu k osobním údajům

Definice pojmů

Osobní údaje – údaje týkající se určené anebo určitelné fyzické osoby, přičemž takovou osobou je osoba, kterou možno určit přímo anebo nepřímo, zejména na základě všeobecně použitelného identifikátoru anebo na základě jedné či vícerých charakteristik anebo znaků, které tvoří její fyzickou, fyziologickou, psychickou, mentální, ekonomickou, kulturní anebo sociální identitu. Může to být například jméno, příjmení, rodné číslo, adresa, fotografie, email,…

Zpracováni osobních údajů – vykonávání jakýchkoliv operací anebo souborů operací s osobními údaji, např. jejich získávání, shromažďování, zaznamenávání, uspořádávání, přepracováni anebo změna, vyhledávání, prohlížení, přeskupování, kombinování, přemísťování, využívání, uchovávání, likvidace.

Provozovatel – Andrea Nedvědová

Laktační poradenství

Vyšehrad 681

549 41 Červený Kostelec

Oprávněná osoba – každá fyzická osoba, která přichází do styku s osobními údaji v rámci svého pracovního poměru s provozovatelem anebo osoba, která přichází do styku s osobními údaji v rámci své činnosti ve jménu provozovatele.

Dotčená osoba – každá fyzická osoba, které osobní údaje se zpracovávají. Může to být osoba, které bylo poskytnuté poradenství při kojení anebo osoba, které osobní údaje se zpracovávají na účely mzdové agendy provozovatele v případě, pokud má provozovatel zaměstnance.

Účel zpracováni – předem jednoznačně vymezený anebo ustanovený záměr zpracování osobních údajů, který se váže na určitou činnost. Účelem může být dokumentace z poradenství včetně komunikace přes internet, daňové doklady/fakturace, reference na webových stránkách, přihlašování na podpůrnou skupinu kojících matek, přihlašování na kurz přípravy na kojení.

Automatizovaný informační systém – (dále jen „AIS“) souhrn technických prostředků výpočtové techniky, programové a aplikační vybavení, údajová základna, paměťové média s údaji, instalační média, dokumentace související s technickým a programovým vybavením určeným na automatizované zpracování údajů.

Uživatelský účet – slouží na identifikaci používatele v automatizovaném informačním systému, tvoří jej název účtu a heslo.

Oprávněný používatel – zaměstnanec anebo osoba vykonávající činnost ve jménu provozovatele, který byl poučený o zásadách zpracování osobních údajů a kterému byl zřízený uživatelský účet a přidělené příslušné přístupové práva umožňující plnění jeho pracovních povinností.

Likvidace osobních údajů – zrušení osobních údajů rozložením, vymazáním anebo fyzickým zničením hmotných nosičů tak, aby se z nich osobní údaje nedali reprodukovat.

Bezpečnostní opatření – vykonávaná praxe, pracovní postup anebo zařízení, které snižují riziko zneužití osobních údajů.

Bezpečnostní incident – událost, které přetrvávání anebo opakování by mohlo způsobit ohrožení zájmů provozovatele a snížení úrovně ochrany zpracovaných osobních údajů.

Všeobecní zásady zpracování osobních údajů

Zpracovat možno jen také údaje, které svým rozsahem zodpovídají účelu jejich zpracování podle zákonem stanovených podmínek na základě souhlasu dotčené osoby, s ohledem na výjimky ze zákona, kdy není potřebný souhlas dotčené osoby.

Souhlas dotčené osoby si provozovatel nesmí vynucovat.

Při zpracování osobních údajů je potřebné dodržovat zásady:

- zásada omezení účelu - osobní údaje se mohou získávat jen na konkrétně určený, výslovně uvedený a oprávněný účel a nesmí se dále zpracovat způsobem, který není slučitelný s tímto účelem
- zásada minimalizace osobních údajů - zpracovat jen ty osobní údaje, které jsou nevyhnutné pro daný účel
- zásada správnosti - zpracované osobní údaje musí být správné a podle potřeby aktualizované
- zásada minimalizace uchovávání - osobní údaje se zpracovávají nejpozději do té doby, dokud je to potřebné na účel, na který se osobní údaje zpracovávají
- zásada integrity - zpracování osobních údajů takovým způsobem, který zaručí jejich přiměřenou bezpečnost
- zásada zodpovědnosti - provozovatel je zodpovědný za dodržování základních zásad při zpracování osobních údajů
- zásada mlčenlivosti - provozovatel a oprávněná osoba jsou povinní dodržovat mlčenlivost o osobních údajích, se kterými přijdou do styku. Osobní údaje se nesmí využít pro osobní potřebu, bez souhlasu dotčené osoby se nesmí zveřejňovat ani nikomu poskytovat a zpřístupňovat, kromě zákonných výjimek (např. Sociální a zdravotní pojišťovna v případě, že má provozovatel zaměstnance).

Vymezení osobních údajů

Oprávněná osoba zpracovává osobní údaje jen v rozsahu a způsobem vymezeným účelem:

1. vedení záznamů z poradenství při kojení osobním i virtuálním. Na tento účel zpracovává osobní údaje: Jméno, příjmení, e-mail, adresa, tel. číslo, osobní údaje a fotky z komunikace přes email, zprávy, aplikace messenger, whatsapp nebo jiné aplikace určené ke komunikaci, jméno dítěte, věk/datum narození dítěte, zdravotní stav dítěte či matky
2. účetní doklady - na tento účel se zpracovávají osobní údaje: jméno, příjmení, adresa
3. reference zveřejněné na webových stránkách – na tento účel se zpracovávají osobní údaje, které dotčená osoba sama poskytne, obvykle Jméno, Město, email (není zveřejněný) a reference k poradenství při kojení, která může zahrnovat zdravotní stav dotčené osoby a dítěte dotčené osoby, popřípadě fotografie
4. informovaný souhlas – na účel souhlasu se zpracováním osobních údajů se zpracovávají osobní údaje poskytnuté dotčenou osobou
5. přihlašování na podpůrnou skupinu kojících matek nebo předporodní kurz přípravy na kojení – zpracovávají se osobní údaje jméno, příjmení, email, telefonní číslo, adresa

Oprávněné osoby jsou povinné po poučení dodržovat zásady pro zpracování osobních údajů podle této směrnice.

Práva dotčených osob

Dotčená osoba má právo:

- právo požadovat od provozovatele přístup k svým osobním údajům
- právo na opravu osobních údajů
- právo na vymazání osobních údajů
- právo na omezení zpracování osobních údajů
- právo namítat proti zpracování osobních údajů
- právo na přenosnost svých osobních údajů
- právo odvolat souhlas (pokud je souhlas právním základem zpracování)
- právo podat stížnost dozornému orgánu, tj. Úřad pro ochranu osobních údajů České republiky.

Dotčená osoba může tyto práva vyžadovat od provozovatele ústně, písemně anebo elektronickou formou. Provozovatel musí tomuto právu vyhovět, obvykle ve formě, v jaké se dotčená osoba svého práva dožaduje. Pokud se dotčená osoba dožaduje svých práv ústně, má provozovatel právo požadovat od něj dodatečné informace potřebné na potvrzení totožnosti.

Provozovatel je povinný poskytnout informace do jednoho měsíce od doručení žádosti. V odůvodněných případech může prodloužit lhůtu o další dva měsíce, a to i opakovaně. O každém takovém prodloužení musí informovat dotčenou osobu do jednoho měsíce od doručení žádosti s důvody prodloužení lhůty.

Informace provozovatel poskytuje bezplatně, kromě důvodů, kdy je žádost dotčené osoby zjevně neopodstatněná anebo nepřiměřená, zejména pro její opakující se povahu. V takovém případě může provozovatel požadovat přiměřený poplatek anebo odmítnout konat na základě žádosti dotčené osoby.

Bezpečnostní opatření

Bezpečnostní opatření slouží na zabezpečení důvěrnosti a dostupnosti chráněných osobních údajů.

Oprávněné osoby jsou povinné:

- chránit zpracované osobní údaje
- chránit informační a technologické zdroje s údaji
- zpracovat osobní údaje v souladu s touto směrnicí
- informovat provozovatele, pokud zjistí porušení anebo nedodržení principů této směrnice.

Provozovatel před započetím zpracování osobních údajů a během jejich zpracování průběžně kontroluje, zda jejich zpracováním nevzniká nebezpečenství narušení práv a svobod dotčených osob. Kontrolu vykonává minimálně raz ročně, podle potřeby může i častěji. Výstupem kontroly je zápis, ve kterém jsou popsané zjištění z kontroly. V případě nedostatků jsou následně přijímané opatření na zabezpečení bezpečnosti zpracovaných osobních údajů.

Postupy při bezpečnostních incidentech, haváriích, poruchách a jiných mimořádných situacích

Incidentem týkajícím se zpracováni osobních údajů jsou jakékoliv události, při kterých dochází k narušení bezpečnosti zpracováni osobních údajů, např.:

- ztráta anebo krádež nosičů informací obsahujících osobní údaje
- selhání informačních systémů obsahujících osobní údaje
- výskyt škodlivého kódu v počítačových zařízeních anebo na serveru
- podezření na neoprávněný přístup do informačních systémů
- narušení důvěrnosti osobních údajů
- zneužití údajů na jiné jako vymezené účely
- požár v chráněných prostorech provozovatele
- živelné pohromy, resp. jiné nepředvídatelné mimořádné události

Provozovatel přijme přiměřené dostupné opatření na předcházení vzniku bezpečnostních incidentů.

Pokud provozovatel zjistí porušení ochrany osobních údajů a toto porušení ochrany povede k riziku pro práva dotčené osoby, je povinný přijmout přiměřené opatření na nápravu a do 72 hodin od zjištění skutečnosti o porušení ochrany osobních údajů informovat Úřad pro ochranu osobních údajů o tomto porušení.

Seznam bezpečnostních opatření

Technické opatření

Zabezpečení objektu pomocí mechanických zábranných prostředků

Objekty, ve kterých se nacházejí osobní údaje zaznamenané na fyzických nosičích anebo výpočtová technika, ze které se přistupuje do systémů na zpracování osobních údajů, musí být zabezpečené proti neoprávněnému vniknutí.

Výpočtová technika při zpracování osobních údajů musí být umístněná tak, aby nebylo možné nepověřenými osobami odpozorovat z monitoru zpracované osobní údaje dotčených osob.

Osobní údaje v tištěné formě - např. ve formě zápisu z poradenství, daňové doklady jsou skladované v sídle provozovatele v uzamykatelném trezoru anebo uzamykatelné skříni.

Pokud oprávněná osoba pracuje s osobními údaji na listinných nosičích, tyto nesmí být ponechané např. volně na stole na místě, kde mají přístup cizí osoby. Pokud je potřebné přenést listinné dokumenty, musí být celou dobu pod dozorem, nesmí být např. ponechané samotné v autě, ani pokud je uzamčené.

Ochrana před neoprávněným přístupem

Počítačové zařízení, ze kterého se přistupuje k osobním údajům dotčených osob, musí být zabezpečené heslem. Pokud je potřebné použít přenos údajů prostřednictvím počítačových sítí, je potřebné přenášené data zabezpečit pomocí hesla, bez kterého se nedá soubor s osobními údaji otevřít.

Autorizace osob v automatizovaném informačním systému

Oprávněné osoby mají na vstup do AIS vytvořené osobité přihlašovací údaje s bezpečným heslem, které pravidelně musí měnit 1 x 3 měsíce. Heslo musí byť "silné" - musí obsahovat kromě malých znaků abecedy také minimálně jeden velký znak a speciální znak, případně číslo. Heslo musí obsahovat náhodné znaky, ne celé slova. Příkladem silného hesla je A47Z@iYpet, příkladem slabého hesla je kojeni10. Oprávněná osoba nesmí heslo uchovávat v počítači ani mobilním zařízení, ale v písemné formě na takovém místě, kde nemají mít přístup neoprávněné osoby.

Ochrana proti škodlivému kódu

Počítačové zařízení, ze kterého se přistupuje do informačního systému, je zabezpečené pravidelně aktualizovaným antivirovým programem. Pravidelná rychlá kontrola počítače antivirovým programem je spuštěná automaticky každý den, hloubková kontrola 1 x týdenně, vždy ve stejném čase.

Provozovatel v počítači používá jen legální software se zapnutým firewall-em. Připojení na počítačovou síť je zabezpečené šifrovaným spojením s heslem, nikdy přes veřejně přístupné počítačové sítě. Úroveň ochrany je nastavená na "střední" - upozornění, pokud se stránky pokoušejí instalovat doplňky, blokování nahlášených útočných stránek, blokování nahlášených podvodních stránek, nepamatování si uložených hesel.

Software počítačů je pravidelně aktualizovaný.

Zálohování zpracovaných osobních údajů

Zálohování zpracovaných osobních údajů se uskutečňuje 1 x měsíčně.

Osobní údaje uložené na pevném disku počítačového zařízení se zálohují na datový nosič určený výlučně na tyto potřeby.

Likvidace osobních údajů

Pokud je potřebné vykonat likvidaci fyzických nosičů s osobními údaji, tyto třeba skartovat, případně jinak fyzicky zničit, aby nebylo možné zpětné zjištění osobních údajů z těchto nosičů. Za bezpečnou likvidaci nosiče se nepovažuje vyhození celého nosiče do koše!

Osobní údaje se z počítačového zařízení likvidují vymazáním z pevného disku počítačového zařízení a vymazáním z datového nosiče určeného na zálohování osobních údajů.

Osobní údaje je oprávněná likvidovat jen oprávněná osoba.

Organizační bezpečnostní opatření

Před prvním uskutečněním zpracovatelské operace s osobními údaji provozovatel poučí oprávněnou osobu o právech a povinnostech vyplývajících ze zákona a vyhotoví o tom písemný záznam o poučení.

Postupy při zpracování osobních údajů

Oprávněné osoby mají neomezený přístup k osobním údajům dotčených osob a mohou vykonávat všechny zpracovatelské operace:

A - oprávnění obeznamovat se s osobními údaji
B - oprávnění získávat osobní údaje ve jménu provozovatele
C - oprávnění zaznamenávat osobní údaje
D - oprávnění vykonávat změny a opravy osobních údajů
E - oprávnění likvidovat osobní údaje
F - neomezený přístup k zpracovaným osobním údajům

Zakázané postupy při zpracování osobních údajů:

- zveřejňování osobních údajů, kromě případů, že dotčená osoba výslovně souhlasila se zveřejněním osobních údajů
- poskytování osobních údajů třetím stranám, o kterých nebyla dotčená osoba předem informovaná
- zpřístupňování osobních údajů
- přeshraniční přenos osobních údajů

Zodpovědnost za porušení zákona o ochraně osobních údajů

Oprávněná osoba poučením přebírá na sebe zodpovědnost za zpracování osobních údajů podle této bezpečnostní směrnice. V případě, že okolnosti nedovolují dodržet všechny uvedené bezpečnostní opatření, bezodkladně informuje o této skutečnosti provozovatele.

Vzdělávání

Oprávněná osoba je před první zpracovatelskou operaci s osobními údaji důkladně obeznámená se systémem na zpracování osobních údajů. Oprávněná osoba je taky obeznámená s pravidly používání počítačových zařízení a možnými riziky spojenými s jejich používáním v rámci sítě Internetu.

Postup při ukončení případného pracovního poměru oprávněné osoby anebo spolupráce s oprávněnou osobou

Provozovatel při ukončení pracovního poměru oprávněné osoby anebo ukončení spolupráce s oprávněnou osobou zruší této osobě přístupové práva do správy informačních systémů. I po ukončení pracovního poměru anebo ukončení spolupráce je oprávněná osoba povinná dodržovat mlčenlivost o osobních údajích zpracovávaných během trvání jejího pracovního poměru anebo trvání spolupráce s provozovatelem.

Postup při poruše počítačového zařízení

Pokud je potřebné vykonat opravu počítačového zařízení, ve kterém jsou osobní údaje, mimo sídla provozovatele, je potřebné osobní údaje z počítačového zařízení zálohovat na datový nosič, vymazat z počítačového zařízení a až tak umožnit opravu zařízení.

Táto bezpečnostní směrnice je závazná a platná od 25. 5. 2018