39.49. Bezpečnost práce, požární ochrana a GDPR

http://www.guard7.cz/gdpr/bezpecnost-prace-pozarni-ochrana-a-gdpr

Představovat Nařízení Evropského parlamentu a rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,– General Data Protection Regulation je jistě zbytečné. Co GDPR a BOZP a PO?

GDPR se bezpečnosti práce a požární ochrany dotýká v oblastech:

1. vyšetřování, evidence a likvidace pracovních úrazů
2. školení zaměstnanců,
3. pracovnělékařské péče,
4. evidence rizikové práce,
5. kontrolní činnost,
6. evidence pracovní doby – bezpečnostních přestávek,
7. povolování prací, které s představují zvýšené riziko – například povolení ke sváření apod.,
8. evidence OOPP,
   tedy všude tam, kde zaměstnavatel zpracovává osobní údaje zaměstnanců (subjektů údajů) a v případě pracovních úrazů také zvláštní kategorii osobních údajů.

Jak již bylo uvedeno, pro zpracování osobních údajů musí mít zpracovatel právní důvod. V tomto případě to jsou:

1. zpracování je nezbytné pro **splnění smlouvy**, jejíž smluvní stranou je subjekt údajů – základem je smlouva mezi zaměstnavatelem a zaměstnancem o uzavření pracovněprávního vztahu,

2. zpracování je nezbytné pro **splnění právní povinnosti**, která se na správce vztahuje – například povinnosti zaměstnavatele zajistit bezpečnost a ochranu zdraví zaměstnanců při práci, provádět evidenci a odškodnění pracovních úrazů apod..
3. zpracování je nezbytné pro **účely oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.
4. subjekt údajů udělil **souhlas** pro jeden či více konkrétních účelů – jako jediný právní důvod je odvolatelný. Zde platí například při zveřejňování osobních údajů (fotografie, video ….) na sociálních sítích (profilech, které jsou provozovány jménem organizace apod.) a všude tam, kde pro účel použití neexistuje právní důvod. Pro jeden účel zpracování může být více právních důvodů.

Zaměstnavatel tedy nepotřebuje ke zpracování agendy BOZP a PO, kde jsou uvedeny osobní údaje souhlas zaměstnanců, ale musí je informovat v rozsahu požadovaném GDPR.
Dokumenty, kde jsou uvedeny osobní údaje zaměstnanců, musí být chráněny a musí být stanoveno, kdo a v jakém rozsahu k nim má přístup. Není je tedy možné ukládat volně, aby se s nimi mohl seznámit „každý“.

Záznamy o BOZP a PO

Při pohybu záznamů týkajících se BOZP a PO, které obsahující osobní údaje je nutné stanovit pravidla a postupy:

1. záznamy v tištěné podobě (záznamy o pracovních úrazech, prezenční listiny školení) by se měly předávat skrytě tj. nepoužívat průhledné obaly, předávat proti podpisu (pokud je to vhodné a odpovídající riziku). Je nutné stanovit pravidla pro jejich skartaci včetně postupu pro „zkažené“ záznamy.
2. elektronickou podobu záznamů jako např. vyplněné předlohy pro

vytištění, naskenované prezenční listiny, záznamy o úrazech apod. je nutné podrobit jasně stanovenému režimu, pokud jsou rozšiřovány prostřednictvím elektronické pošty, ukládány na vnitrofiremní i venkovní úložiště apod.. To spočívá ve stanovení oprávnění pro zpracování těchto údajů a technické a softwarové zabezpečení.

3. Vše začlenit do systému ochrany osobních informací v souladu s nařízením GDPR.

Pracovnělékařská péče

Záznamy o zdravotních prohlídkách (nástupní, periodické, mimořádné a výstupní) tj. lékařské posudky o zdravotní způsobilosti k práci obsahují osobní údaje zaměstnanců:
1. jméno a příjmení,
2. bydliště,
3. datum narození,
4. popřípadě, telefonický a emailový kontakt.

Na posudku by mělo být od poskytovatele pracovnělékařských služeb uvedeno pouze, zda je zaměstnanec po zdravotní stránce schopen, schopen s omezením nebo neschopen. Pokud by zde byly uvedeny informace o zdravotním stavu, dostává se osobní údaj do zvláštní kategorie údajů a do režimu zvláštní ochrany stanovené v každé organizaci v rámci implementace GDPR.

Pracovní úrazy

Knihy úrazů a záznamy o úrazu nesmí být volně dostupné, jsou v nich jednoznačně uvedeny osobní údaje zařazené do zvláštní kategorie osobních údajů. Kniha úrazů (v tištěné podobě) musí být například uzamčena u vedoucího pracoviště, který ji použije až v případě nutnosti provedení zápisu a v případě potřeby zpřístupní dalším oprávněným osobám.

V případě elektronické formy knihy úrazů a záznamů o úrazu musí být tyto zabezpečené proti přístupu neoprávněných osob, stanoven systém oprávnění, rozdělení úkolů a pravomocí a zajištěna ochrana ve firemní počítačové síti, proti útokům zevnitř i zvenčí.
Celý proces pracovního úrazu od vyšetření až po likvidaci a přijetí opatření proti jejich opakování by měl být zdokumentován tak, aby bylo jasně stanoveno, kdo a k jakým informacím a za jakým účelem má přístup a jak s nimi může zacházet a jaká další ochranná opatření jsou stanovena.

Evidence rizikových prací

I zde se zpracovávají osobní údaje zvláštní kategorie a platí pro jejich zpracovávání shodné zásady jako pro záznamy o pracovních úrazech. Povinnost zaměstnavatele evidovat rizikové práce stanoví § 40 Zákona č. 258/2000 Sb. o veřejném zdraví.

Evidence rizikových prací musí obsahovat u každého zaměstnance údaje:

- jménu, příjmení a rodném čísle,
- počtu směn odpracovaných při rizikové práci, s výjimkou rizika infekčního onemocnění,
- datech a druzích provedených lékařských preventivních prohlídek a jejich závěrech,
- zvláštních očkováních souvisejících s činností na pracovišti zaměstnavatele nebo o imunitě (odolnosti) k nákaze,
- o výsledcích sledování zátěže organismu zaměstnanců faktory pracovních podmínek a naměřených hodnotách intenzit a koncentrací faktorů pracovních podmínek a druhu a typu biologického činitele, s výjimkou údajů o zdravotním stavu zaměstnanců.

Evidence se ukládá po dobu 40 let po ukončení expozice, jde-li o práce:

- s chemickými karcinogeny,
- s azbestem,
- v riziku fibrogenního prachu,
- s biologickými činiteli, které mohou vyvolat latentní onemocnění, onemocnění, která mají velmi dlouhou inkubační dobu nebo způsobují onemocnění, které se opakovaně projevují remisemi či mohou mít závažné následky.

Více o evidenci rizikových prací.

Školení zaměstnanců

Zaměstnavatel je povinen prokázat, že provedl stanovená školení a výcvik. Zpravidla se jedná o prezenční listiny (hromadné) a certifikáty o absolvování školení pro jednotlivce. Ty by měly být uloženy tak, aby k nim nebylo možné bez oprávnění přistupovat – např. zamčené. Elektronické kopie opět podléhají chráněnému uložení a přístupu v rámci řešení počítačové sítě a její ochrany.
Další viz výše – Záznam o BOZP a PO.

Sledování lhůt zaměstnanců

Osobní údaje zaměstnanců jsou uvedeny v dokumentaci nebo softwarových aplikacích pro sledování a řízení lhůt školení a v dokumentaci, která prokazuje jejich provedení.V současnosti se zpravidla preferuje softwarové řešení. To je ale v řadě případů „improvizované“ tj. nepoužívá speciální software, ale např. MS Excel, Access apod. Zde je třeba vyhodnotit riziko a přijmout ochranu proti neoprávněnému přístupu a zneužití.

Dokumentace BOZP a PO

Další osobní údaje se mohou objevit v dokumentaci BOZP a PO –

oprávněné a odborně způsobilé osoby, odpovědní zaměstnanci za určité oblasti (např. technická zařízení, odpovědnost za pracoviště…) záznamech o kontrolní činnosti. Jméno a příjmení, je v dokumentaci vhodné nahradit pracovní funkcí zaměstnance. To ale není vždy možné. Pokud odpovědná osoba ukončí pracovněprávní poměr s organizací, je nutné bezodkladně dotčenou dokumentaci aktualizovat odstranit (změnit jméno a příjmení nové odpovědné osoby) osobní údaje (jméno a příjmení). Již netrvá právní důvod (dodržování požadavků pro splnění právních povinností) a organizace v tomto případě nemá dále právo zpracovávat osobní informace bývalého zaměstnance.

Pro příklad – požární řád pro pracoviště se zvýšeným a vysokým požárním nebezpečím, kde jsou ustanoveny preventivní požární hlídky (PPH), musí obsahovat jako přílohu pokyny pro činnost PPH. Ty obsahují jmenný seznam velitele a členů PPH a vlastní požární řád obsahuje jméno a příjmení odpovědného vedoucího zaměstnance. Požární řád se zveřejňuje tak, aby byl dobře viditelný a trvale přístupný pro všechny osoby vyskytující se v místě provozované činnosti, což jsou i návštěvníci a další osoby. V tomto případě je právním důvodem pro zpracování osobních údajů plnění právní povinnosti.
Stejně jako v předešlém případě musí být dokumentace aktualizována pokud dojde ke změně členů PPH nebo vedoucího zaměstnance odpovědného za pracoviště.

Fotografie a videa

Fotografie a videa pořizovaná na pracovištích za účelem dokládat stav (shodu či neshodu s požadavky BOZP a PO) je možné pořizovat i pokud jsou na nich zaměstnanci, ale pouze pokud je to nutné k účelu pro který jsou pořizovány. Například nepoužívání OOPP, nebezpečná manipulace atd.. Pro další účely zpracování je ale třeba souhlasu zaměstnanců. Tyto záznamy je třeba zpracovávat a ukládat opět tak, aby byly chráněny proti zneužití a přístupné pouze oprávněným

osobám.

E-learning

Pokud používáte e-learningová školení, kde jsou osobní údaje ukládány mimo vaše úložiště, stává se z poskytovatele e-learningu **zpracovatel**. Vzájemné vztahy a pravidla pro zpracovávání osobních dat vašich zaměstnanců musíte vymezit ve smlouvě popř. dodatku ke stávající smlouvě tak, aby zahrnovala všechny požadavky GDPR.
Minimálně by poskytovatel e-learningu (zpracovatel) měl v rámci prováděného školení:

1. informovat uživatele v rozsahu požadavků GDPR,
2. zpracovávat jejich osobní údaje pouze v nejnutnějším rozsahu,
3. poskytnout jim na požádání výpis,
4. po pominutí právního důvodu vymazat ze svých databází. Pominutím právních důvodů zde není ukončení pracovního poměru zaměstnancem, ale uplynutí zákonné lhůty pro doložení důkazů.

Související legislativa

Zákon č. 101/2000 Sb., o ochraně osobních údajů.
Zákon č. 89/2012 Sb., občanský zákoník.
Zákon č. 127/2005 Sb. ,o elektronických komunikacích.
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.
Nařízení GDPR

Další

- **Pojmy a definice GDPR**
- **Zásady zpracování osobních údajů**
- **Právní důvody pro zpracování osobních údajů**
- **Souhlas se zpracováním osobních údajů**
- **Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů**
- **Podmínky vyjádření souhlasu se zpracováním osobních údajů**
- **Odvolání souhlasu se zpracováním osobních údajů**
- **Platnost souhlasu uděleného před účinností GDPR**
- **Osobní údaje**
- **Zvláštní kategorie osobních údajů**
- **Použití již zveřejněných osobních údajů**
- **Informační povinnost správce vůči subjektu údajů**
- **Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů**
- **Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**

- Přístup k osobním údajům
- Právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném rozhodování
- Právo být zapomenut
- Právo na přenositelnost údajů
- Zaměstnavatel a zpracování osobních údajů
- Správce
- Hlavní povinnosti správce
- Zpracovatel
- Zabezpečení osobních údajů
- Porušení zabezpečení osobních údajů
- Pověřenec pro ochranu osobních údajů
- Postavení pověřence pro ochranu osobních údajů
- Úkoly pověřence pro ochranu osobních údajů
- Záznamy o činnostech zpracování
- Posouzení vlivu na ochranu osobních údajů
- Kodex chování a osvědčení
- Transparentnost a postupy
- Práva subjektů údajů
- Právo subjektu údajů na transparentní informace
- Právo subjektu údajů na informace
- Právo subjektu údajů na přístup k osobním údajům
- Právo subjektu údajů na opravu
- Právo subjektu údajů být zapomenut
- Právo subjektu údajů na omezení zpracování
- Právo na oznámení při opravě nebo výmazu údajů nebo při omezení zpracování
- Právo na přenositelnost údajů
- Právo vznést námitku
- Právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném rozhodování
- Pracovní skupina WP29
- Pravidelné a systematické monitorování

- **Profilování**
- **Pseudonymizace**
- **Zpracování osobních údajů prováděné ve velkém rozsahu**
- **Sužba informační společnosti**