V pátek 25. května 2018 nabyla účinnosti nová právní úprava ochrany osobních údajů – Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, zkráceně nazývaným GDPR. Nařízení je přímo použitelný předpis EU, a proto nebude transformován do žádného národního předpisu (v budoucnu má být vydán tzv. adaptační zákon, který má upravit náležitosti, které GDPR umožňuje řešit na národní úrovni).

GDPR, které je pro mnohé podnikatele strašákem, se vztahuje na zcela nebo částečně automatizované a neautomatizované zpracování osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Přičemž evidencí je míněn jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, až již centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska. Za osobní údaj jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tedy o fyzické osobě, kterou lze přímo nebo nepřímo identifikovat (subjekt údajů).

GDPR řeší ochranu osobních údajů při jejich zpracování. Tím je myšlena jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů (shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz či zničení).

Co má GDPR a BOZP společného

Vzhledem k tomu, že GDPR neobsahuje konkrétní pravidla pro nakládání s osobními údaji, je postup implementace o to složitější. Nemá být prokázáno plnění požadavků GDPR, ale soulad s ním. Každý správce (fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů) si musí vytvořit svá pravidla na základě konkrétních podmínek nakládání s osobními údaji, která poté musí dodržovat a tak zajišťovat soulad s GDPR.

GDPR je založeno na stejném základě jako BOZP, tedy na stanovení opatření na základě kvalifikovaného odhadu míry předpokládaných rizik spojených s nakládáním s osobními údaji. Ochrana je pojata abstraktně, obdobně jako v BOZP.

GDPR se vztahuje pouze na osobní údaje o živých fyzických osobách (při šetření smrtelného pracovního úrazu se GDPR neuplatní, to však neznamená, že se neuplatní ochrana osobních údajů podle jiných právních předpisů, např. občanského zákoníku).

Zásady zpracování osobních údajů

Základními „stavebními kameny“ GDPR (vodítky pro zajištění souladu) jsou zásady zpracování osobních údajů. Jejich dodržováním se vytváří soulad s GDPR. Jedná se o:

- zákonnost (zpracování nesmí být v rozporu se zákonem a pouze v odpovídajícím rozsahu při splnění některé z GDPR uvedených podmínek – právní důvody pro zpracování osobních údajů,

- korektnost a transparentnost (zajišťovat co největší míru informovanosti subjektů údajů a nezastírat účel zpracování),
- účelové omezení (osobní údaje nesmí být zpracovány k jinému účelu, než k jakému byly shromážděny [existují výjimky – pro účely archivace ve veřejném zájmu, vědeckého či historického výzkumu nebo pro statistické účely]),
- minimalizaci údajů (pouze údaje, které jsou pro dosažení účelu nezbytné, a to pouze v nutném rozsahu),
- přesnost (údaje musí být přesné a podle potřeby aktualizované; avšak správce nemá povinnost vyhledávat nepřesné údaje a opravovat je),
- omezení uložení (osobní údaje mají být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány, nepotřebné údaje musí být vymazány nebo anonymizovány [i zde platí výjimka – pro účely archivace ve veřejném zájmu, vědeckého či historického výzkumu nebo pro statistické účely]),
- integritu a důvěrnost (nutno přijmout vhodná technická a organizační opatření pro zajištění integrity a důvěrnosti osobních údajů),
- odpovědnost (zajištění souladu se všemi zásadami a být schopen to prokázat; odpovědný je vždy správce, nikoliv jeho zaměstnanec nakládající s osobními údaji [zaměstnanec ve smyslu GDPR není ani zpracovatelem osobních údajů]).

Právní důvody pro nakládání s osobními údaji

K legálnímu nakládání s osobními údaji musí být alespoň jeden právní důvod uvedený v GDPR (souběžně může být i více právních důvodů). Právní důvody úzce souvisí s účelem zpracování (účel ovlivňuje možný právní důvod, proto je primárně nezbytné stanovit účel, za kterým je s jednotlivým osobním údajem nakládáno). Právní důvody lze rozdělit do dvou základních skupin – bez souhlasu subjektu údajů a se souhlasem (souhlas je nutný). Všechny právní důvody jsou si rovny (souhlas není nadřazen ostatním). V případě právního důvodu k nakládání s osobním údajem bez souhlasu subjektu údajů se souhlas nepožaduje – souhlas by byl nejen nadbytečný, ale též by uváděl subjekt údajů v omyl, že je možné zpracování toho osobního údaje odvolat.

Právními důvody, kdy se souhlas nepožaduje, jsou případy, kdy:

- zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro přijetí opatření před uzavřením smlouvy na žádost subjektu údajů,
- zpracování je nezbytné pro plnění právní povinnosti,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
- zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy subjektu údajů vyžadující ochranu osobních údajů, zejména dítěte.

Pro zajištění BOZP a PO je v drtivém případě právním důvodem, že „zpracování je nezbytné pro plnění právní povinnosti“. Je-li však zájem nakládat s osobním údajem z důvodu, který nesplňuje, že zpracování je nezbytné pro plnění právní povinnosti, např. umístění fotografie znázorňující porušení požadavku k zajištění BOZP, na které je možné identifikovat konkrétní fyzickou osobu, na nástěnce nebo její prezentace v rámci školení zaměstnanců, je nutné si od

této osoby vyžádat souhlas splňující požadavky GDPR (jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, který subjekt údajů dává prohlášením nebo jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů).

Při nakládání s osobními údaji při zajišťování BOZP a PO je tedy zcela nezbytné rozlišovat, zda se jedná o plnění zákonné povinnosti (drtivá většina případů), či nikoliv. Dále je nutné mít na vědomí, že osobní údaje je možné zpracovávat pouze za předem jasně definovaným účelem (není možné je zpracovávat s tím, že se to může někdy k něčemu hodit apod.).

Zvláštní kategorie osobních údajů

GDPR kromě zajištění obecné ochrany osobních údajů definuje i ochranu pro zvláštní kategorii osobních údajů (dříve „citlivé údaje“). Jedná se o údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace a údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby. Jejich zpracování je, až na stanovené výjimky, zakázáno.

Zpracování je povoleno v případech:
- udělení výslovného souhlasu subjektu údajů,
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
- další případy uvedené v čl. 9 odst. 2 GDPR (zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů, zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance atd.).

Při zajišťování BOZP lze předpokládat nakládání s údaji o členství v odborech a s údaji o zdravotním stavu. Jak již bylo zmíněno, tyto údaje nesmí být zpracovávány, vyjma povolených případů. Z hlediska zajištění BOZP jím je případ: „zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany“. K jejich zpracovávání není nutné vyžadovat výslovný souhlas. Zároveň však nesmí být použity k jinému účelu, pokud nebudou upraveny tak, aby již nebylo možné identifikovat konkrétní fyzickou osobu (anonymizace [nevratné odstranění vazby mezi subjektem údajů a informací] apod.), tedy v případě, že osobní údaj není „přetvořen“ na anonymní údaj (údaj, který nelze vztáhnout k subjektu údajů).

Při zajišťování BOZP a PO je nutné dodržet pravidla stanovená správcem osobních údajů, např. nevyžadovat dokumenty obsahující osobní údaje, které nejsou potřebné, zamezit přístupu nepovolaných osob k dokumentům obsahujícím osobní údaje (uzamykání kanceláře apod.),

omezit přístup ke knize úrazů (přístup má pouze definovaný okruh osob), fyzickou likvidaci vícetisků dokumentů obsahujících osobní údaje (uchovat pouze potřebný počet výtisků), dodržovat mlčenlivost o zjištěných osobních údajích (např. neprozrazovat datum narození či velikost spodního prádla [v prostředí s nebezpečím výbuchu]) atd.

Zabezpečení osobních údajů

Zabezpečení osobních údajů má být provedeno s přihlédnutím ke stavu techniky, nákladům na provedení, povaze a rozsahu zpracování, jakož i jejich kategorii, kontextu a účelu zpracování a k různě pravděpodobným a různě závažným rizikům pro práva a svobody subjektů údajů (abstraktní pojetí ochrany osobních údajů jako při zajišťování BOZP). Záleží na správci údajů jaká konkrétní zabezpečení příjme. To je jeho právo i povinnost.

Je možné, nikoliv povinné, například provést pseudonymizaci, což znamená nahradit identifikační údaje kódem. Přitom databáze vazeb kód-identifikační údaj musí být uložena odděleně. Dále je možné provádět šifrování osobních údajů. Opět se nejedná o povinnost, ale o možnost použití v případě, kdy je to vhodné (správce usoudí, že je to potřebné).

Také by měla být přijata taková opatření, aby osobní údaje zpracovávala pouze fyzická osoba, která je zpracovává na pokyn správce nebo zpracovatele (fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce [nejedná se o zaměstnance správce!]). Jejich počet by měl být minimalizován.

Zajišťování BOZP a PO dodavatelským způsobem

Pro mnohé firmy je výhodné pro zajištění BOZP a PO si sjednat externí firmu. Tato firma, pokud v rámci smluvně sjednané činnosti nakládá s osobními údaji, což je pravděpodobné, je jejich zpracovatelem. Mezi správcem a zpracovatelem musí být uzavřeno písemné smluvní ujednání o způsobu zajištění ochrany osobních údajů. Zpracovatel je povinen řídit se požadavky správce údajů (údaje zpracovávat jen za základě pokynů správce) a umožnit mu kontrolu plnění této povinnosti. Bez písemného předchozího povolení správce, zpracovatel nesmí řetězit zpracovatelé osobních údajů, tedy předávat osobní údaje ke zpracování dalšímu zpracovateli.

Smlouva musí stanovit, že:
- zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce,
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo se na ně vztahovala zákonem stanovená mlčenlivost,
- příjme opatření k zabezpečení osobních údajů,
- dodržuje podmínky pro zapojení dalšího zpracovatele,
- zohledňuje povahu zpracování,
- je správci nápomocen v technických a organizačních opatřeních,
- vymaže nebo vrátí správci osobní údaje po ukončení poskytování služeb,
- poskytne správci informace potřebné k doložení toho, že byly splněny povinnosti podle čl. 28 GDPR (tedy především výše uvedené).

Jedná-li se o firmu, která k zajišťování BOZP a PO dodavatelským způsobem využívá zaměstnance, je zpracovatelem osobních údajů svých klientů (např. prezenční listiny školení, záznamy

o úrazu) a zároveň správcem osobních údajů svých zaměstnanců (mzdová agenta apod.), případně osobních údajů dalších osob (například smluvních partnerů).

Povinnosti správce

Správce primárně odpovídá za zpracování osobních údajů. Pro jejich ochranu je povinen zavést vhodná technická a organizační opatření odpovídající danému riziku (schopnost obnovit dostupnost osobních údajů, zajištění integrity údajů, mlčenlivost zaměstnanců atd.).

Správce je též povinen vést záznamy o činnostech zpracování (obdobně platí i pro zpracovatele). Ty mají především obsahovat:
- totožnost správce,
- účely zpracování,
- kategorie subjektů údajů a osobních údajů,
- dobu zpracování (plánované lhůty pro výmaz) – je-li to možné,
- obecný popis technických a organizačních bezpečnostních opatření – je-li to možné.

Povinnost vést záznamy se nevztahuje na správce, který má méně než 250 zaměstnanců. Tato výjimka se však neuplatní v případě, že zpracování pravděpodobně představuje riziko pro práva a svobody fyzické osoby, zpracování není příležitostné, nebo se zpracovávají zvláštní kategorie osobních údajů, případně osobní údaje týkající se rozsudků v trestních věcech. Tedy pokud správce (případně zpracovatel) provádí evidenci pracovních úrazů nebo zajišťuje náhrady škody a nemajetkové újmy jimi vzniklé, má povinnost o této činnosti zpracování záznamy, i když se jedná o firmu zaměstnávající méně než 250 zaměstnanců.

Nastane-li případ porušení zabezpečení osobních údajů, které je rizikové (např. citelná krádež dat), je správce povinen to ohlásit dozorovému orgánu (Úřadu pro ochranu osobních údajů). Ohlášení by mělo být provedeno do 72 hodin.

Práva subjektu údajů

Správcem nesmí být ignorována práva subjektů údajů – právo na informace, na přístup k osobním údajům, na opravu, na doplnění, na výmaz. Výkon těchto práv musí být bezplatný, vyjma případů zjevně nedůvodných žádostí (například neustále se opakujících). Uskutečněn má být bez zbytečného odkladu, resp. do třiceti dnů.

Kdokoliv, kdo v důsledku porušení GDPR utrpěl hmotnou či nehmotnou újmu, má právo od správce nebo zpracovatele obdržet náhradu utrpěné újmy.

Pokuty

Velkým strašákem se staly pokuty, které budou moci být podle GDPR uloženy. Pravdou však je, že budou moci být uloženy, jak Nařízení uvádí, podle okolností každého případu. Sankce, tedy nejen pokuty, mají mít především preventivní, odstrašující a donucující účinek, nikoliv však likvidační.

Nařízení nepožaduje, že v případě zjištění musí být pokuta uložena. Při rozhodování, zda správní pokutu uložit či nikoliv a případně v jaké výši bude zohledňována například povaha,

závažnost, délka porušení s přihlédnutím k povaze, rozsahu a účelu zpracování, jakož i k počtu dotčených subjektů údajů a jejich kategorie. Též bude brán zřetel na to, zda se jednalo o úmysl nebo nedbalost, na kroky podniknuté správcem ke zmírnění škod, předchozí porušení správce atd.

Stanovená pokuta do výše 20 000 000 EUR nebo do 4 % celosvětového obratu za předchozí finanční rok (podle toho, která hodnota je vyšší) se vztahuje pouze na závažnější porušení (porušení práv subjektu údajů, předávání osobních údajů atd.). Pro ta méně závažná (nenahlášení nebo neoznámení případu porušení zabezpečení osobních údajů atd.) jsou stanoveny poloviční hodnoty.

V souvislosti s výší pokut je nutné si uvědomit dva aspekty, a to že pokuta má být odstrašující i pro největší společnosti světa (proto tak vysoké částky), a že se budou ukládat podle okolností každého jednotlivého případu. Tedy u drobných živnostníků, kterým poskytovatelé služeb v zajištění BOZP a PO většinou jsou, se jistě nebude jednat o výše uvedené částky.

Dokumenty BOZP a PO obsahující osobní údaje

S osobními údaji se při zajišťování BOZP a PO nakládá zejména v případech:
- žádosti o pracovnělékařskou prohlídku,
- posudku o pracovnělékařské prohlídce,
- prezenčních listin školení BOZP a PO, jakož i dalších profesních školení a odborných příprav,
- evidence OOPP (jméno, příjmení, ale i tělesné rozměry atd.),
- evidence výkonu rizikové práce (rodné číslo atd.),
- evidence bezpečnostních přestávek,
- vydání příkazu na sváření (jméno a příjmení svářeče, číslo jeho svářečského průkazu atd.),
- knihy úrazů,
- evidence pracovních úrazů a nemocí z povolání,
- náhrad škody a nemajetkové újmy z důvodu pracovního úrazu nebo nemoci z povolání,
- zápisů z kontrol (včetně fotodokumentace, videí apod.),
- dokumentace požární ochrany (požárně poplachová směrnice, požární řád [jméno a příjmení vedoucího zaměstnance pracoviště, jména a příjmení členů preventivní požární hlídky, jméno, příjmení a odborná způsobilost zpracovatele] atd.).

Při zajišťování BOZP dochází i ke zpracování zvláštní kategorie osobních údajů, a to z důvodu plnění povinnosti v oblasti pracovního práva. Jedná se o nakládání s osobními údaji o zdravotním stavu, které jsou uvedeny v posudku o bolestném nebo o ztíženém společenském uplatnění. Posudek o pracovnělékařské prohlídce neobsahuje údaje spadající do této kategorie (neobsahuje údaj o zdravotním stavu, ale pouze o zdravotní způsobilosti k výkonu práce). To též platí o evidenci poskytovaných osobních ochranných pracovních prostředků – velikost oblečení a obuvi (jedná se o obecné osobní údaje, pokud je možné přímo nebo nepřímo identifikovat fyzickou osobu, což v tomto případě je).

Dalšími dokumenty obsahujícími osobní údaje, které se řadí do zvláštní kategorie, jsou kniha úrazů (údaje o zdravotním stavu – druh zranění, zraněná část těla), záznam o úrazu a záznam o úrazu – hlášení změn, které kromě údajů o zdravotním stavu mohou též obsahovat údaje o členství v odborech – jméno a podpis za odborovou organizaci. I v těchto případech platí, že

ke zpracování dochází z důvodu plnění povinnosti v oblasti pracovního práva (není nutné požadovat souhlas, tedy souhlas nemá být požadován).

Ve vztahu k posudku o bolestném, posudku o ztíženém společenského uplatnění, záznamu o úrazu a k záznamu o úrazu – hlášení změn navíc platí, že s těmito dokumenty nakládá více zaměstnanců (mzdová účetní, odborně způsobilá osoba k zajišťování úkolů v prevenci rizika atd.), čímž dochází k zvýšení rizika ochrany osobních údajů (přeposílání dokumentů mezi nimi atd.). Z tohoto důvodu je nezbytné zajistit v maximálně možné míře omezení počtu těchto zaměstnanců (v interním předpise, např. pracovnímu postupu při vzniku pracovního úrazu, by měl být definován koloběh uvedených dokumentů).

GDPR nebrání v poskytnutí výtisku záznamu o úrazu, resp. záznamu o úrazu – hlášení změn odborové organizaci bez udělení souhlasu subjektem údajů, tedy postiženým. Jedná o možnost plnění zákonné povinnosti zpřístupnit jim doklady o evidenci a hlášení pracovních úrazů [viz § 108 odst. 6 písm. b) zákoníku práce], tedy o případ, kdy zpracování je nezbytné pro plnění právní povinnosti. Navíc, jejich zástupce tyto dokumenty podepisuje, tedy opět se jedná o zpracování osobních údajů nezbytných pro plnění právní povinnosti.

Jiné to však je se zasíláním výtisku České správě sociálního zabezpečení. Zde se nejedná o zpracování, které je nezbytné pro plnění právní povinnosti, neboť zaslání nevyžaduje žádný právní předpis (ani zákon č. 187/2006 Sb., ve znění pozdějších předpisů). K doložení, že pracovní neschopnost nevznikla z důvodů uvedených v § 25 písm. a) a § 31 uvedeného zákona, neslouží záznam o úrazu ve smyslu nařízení vlády č. 201/2010 Sb., ve znění pozdějších předpisů, ale speciální formulář „Záznam o úrazu“ ČSSZ, který vyplňuje zraněný zaměstnanec. Zasláním záznamu o úrazu podle nařízení vlády by došlo k porušení souladu s GDPR, neboť by došlo k porušení zásady minimalizace údajů.

Zveřejnění jmen a příjmení členů preventivní požární hlídky vyvěšením požárního řadu na pracovišti, na které se vztahuje, není porušením souladu s GDPR, neboť se jedná o požadavek právního předpisu (§ 31 odst. 4 vyhlášky č. 246/2001 Sb., ve znění pozdějších předpisů). Avšak vyvěšení pouhého seznamu členů hlídky s uvedením pracoviště jejich působnosti, bez jejich udělení souhlasu k tomu, by bylo nedodržení souladu s GDPR.

Uchování dokumentů

S ochranou osobních údajů úzce souvisí i doba uchovávání jednotlivých dokumentů obsahujících osobní údaje (naplnění zásady omezení uložení). Je jedno, zda se jedná o dokumenty v listinné nebo elektronické podobě. Z hlediska zajištění souladu s GDPR osobní údaje mohou být v dokumentech uvedené pouze po dobu trvání účelu, pro který byly osobní údaje získány a zpracovávány (doba uchování dokumentů).

Dobu uchovávání dokumentů mnohdy řeší Spisový a skartační řád. V některých případech je doba uchování upravena právními předpisy. V oblastech BOZP a PO se jedná například o:

- § 40 zákona č. 258/2000 Sb. (evidence rizikové práce) – 10, resp. 40 let,
- § 44a odst. 6 zákona č. 258/2000 Sb. (školení o nakládání s toxickými látkami) – 3 roky,
- § 31 odst. 2 zákona č. 563/1991 Sb. (účetní doklady, např. doklad o doplatcích za léky, pokud je možné přímo nebo nepřímo identifikovat fyzickou osobu [např. doklad je součástí spisu zaměstnance o náhradě škody a nemajetkové újmy]) – 5 let,

- § 35a odst. 4 zákona č. 582/1991 Sb. (záznamy potřebné pro účely důchodového pojištění, mimo jiné záznamy o pracovním úrazu a nemoci z povolání [jen ten výtisk sloužící pro účely důchodového pojištění]) – 30 let.

Jak bylo uvedeno, výčet není konečný. Záleží především na zaměstnavatelem provozovaných činnostech a z toho plynoucích zpracovávaných dokumentech, jakož i s BOZP dalších souvisejících činností, např. jednání s odborovou organizací o zajištění BOZP.

Závěrem

Vzhledem k tomu, že při zajišťování BOZP je nakládáno se zvláštní kategorií osobních údajů, mělo by být pracoviště odborně způsobilé osoby vybaveno skartovacím přístrojem (fyzická likvidace vícetisků atd.). Její pracoviště by nemělo být volně přístupné (uzamykatelné a při opuštění pracoviště uzamčené). Podle požadavků správce osobních údajů je možné, že skříně, v kterých jsou uloženy dokumenty obsahující osobní údaje, zvláště ty ze zvláštní kategorie budou muset být uzamykatelné, případně jinak zabezpečený, případně bude nastaven režim pro předávání dokumentů obsahujících zvláštní kategorie osobních údajů jednotlivými pracovišti apod. Též by odpovídajícím způsobem měla být zajištěna ochrana osobních údajů „v terénu“ – převoz osobních údajů v notebooku, na flash disku apod.

Problém příliš obecných požadavků GDPR na zajištění ochrany osobních údajů by měly řešit kodexy chování vydané jednotlivými oborovými sdruženími. V oblasti BOZP zatím není známa žádná taková iniciativa. Komora BOZP a PO ČR, ani Asociace techniků bezpečnosti práce a požární ochrany České republiky, z. s. zatím nevydaly žádná stanoviska k zajištění souladu s GDPR (asociace bude problematiku GDPR řešit na svém semináři).

Na úplný závěr

Udělat konkrétní návod, jak postupovat pro vytvoření souladu s Obecným nařízením k ochraně osobních údajů (GDPR) pro různé správce je prakticky nemožné. Přístup musí být vždy individuální u každého jednotlivého správce. V žádném případě nelze zajišťovat podle univerzálního řešení (opět obdoba BOZP).

Lze však doporučit určitý postup pro vytvoření souladu s GDPR.

Systém ochrany osobních údajů v souladu s GDPR je možné vytvořit pomocí těchto kroků:

1. Provést analýzu současného stavu. To znamená vyhodnotit jakým způsobem je v současné době zajištěna ochrana osobních údajů (především vyhodnocení systému a jeho funkčnosti).
2. Provést analýzu kde a jakým způsobem ve firmě nebo společnosti dochází ke zpracování osobních údajů, včetně, zda jsou zpracovávány údaje spadající do zvláštní kategorie osobních údajů.
3. Provést analýzu k jakému účelu vyhledané osobní údaje se používají a které osoby se s nimi seznamují.
4. Vyhodnotit, zda zjištěné osobní údaje jsou pro provozovanou činnost nutné. Pokud ne, zrušit je, jakož i jejich další získávání. U těch, které jsou potřebné, vyhodnotit oprávněnost zpracování (z jakého důvodu je možné je zpracovávat ve smyslu GDPR – splnění

jedné ze stanovených podmínek – viz závorka v bodě 5. nebo udělení souhlasu subjektem údajů) a nutnost rozsahu osob, které se s nimi seznamují.

5. U osobních údajů, které je možné zpracovávat pouze na základě souhlasu subjektu údajů, vyhodnotit, zda souhlas byl udělen, a pokud ano, zda odpovídá požadavkům, které vyplývají z GDPR (souhlas není nutné zajišťovat v případě, že zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro přijetí opatření před uzavřením smlouvy na žádost subjektu údajů, pro plnění právní povinnosti, ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy subjektu údajů vyžadující ochranu osobních údajů, zejména dítěte).
6. Vytvořit souhlasy pro zpracování osobních údajů, u kterých je to nutné a požádat o udělení souhlasů subjekty údajů.
7. Vytvořit systém pro poskytování souhlasů, kde je to nutné, při přijímání nových osobních údajů.
8. Vyhodnotit jaká při zpracování osobních údajů vznikají rizika.
9. Stanovit podmínky ochrany osobních údajů (**technické** [způsob ukládání dokumentů, způsob zajištění elektronické dokumentace, šifrování, je-li to nutné, zajištění při předávání údajů třetím osobám atd.], **organizační** [jak dlouho se které údaje uchovávají, možnost zapomenutí, zajištění při předávání údajů třetím osobám atd.], **personální** [kdo s kterými údaji smí pracovat, školení zaměstnanců, ustanovení pověřence, je-li to nutné atd.]).
10. Vytvořit interní předpis (směrnice apod.), který stanoví pravidla systému zajištění ochrany osobních údajů ve vaší firmě, včetně poskytování informací subjektům údajů a kontrolní činnosti.
11. Prověřit, zda nově vytvořeným systémem (interním předpisem) jsou naplněny požadavky všech zásad zpracování osobních údajů.
12. Plnit požadavky stanovené si v interním dokumentu a vést dokumentaci prokazující soulad s GDPR.

červen 2018