

GDPRstart.cz



9 PRAKTICKÝCH KROKŮ K ZAJIŠTĚNÍ SOULADU S GDPR

(návod, jak si sami, snadno a rychle vyřešíte GDPR)

Příručka pro živnostníky, poradce, trenéry, malé firmy, spolky, sportovní kluby, zájmová sdružení, kulturní organizace, gastro provozy, ubytovací zařízení a vůbec všechny ty menší, kterých se GDPR také týká

Pro koho je tato příručka určena a jak ji používat

Na úvod několik faktů:

- **GDPR** je nové byrokratické obecné **nařízení EU** o ochraně osobních údajů (*dále OÚ*)
- Platí již 2 roky a vstoupí v účinnost bez výjimky **25. května 2018**
- Týká se **úplně každého** živnostníka, firmy, spolku, organizace, kteří zpracovávají OÚ
- Každý subjekt je **povinen doložit a prokázat**, že OÚ zpracovává v souladu s GDPR
- Za nerespektování nařízení **hrozí likvidační sankce**, žaloby a mnohamilionové pokuty
- Rozhodně se tedy nevyplatí nařízení ignorovat, **je potřeba se na něj připravit**

Ano, budete se tím muset zabývat... To jsou ty špatné zprávy. Ale je tu i několik lepších:

- Asi se shodneme v tom, že **je třeba naše OÚ chránit** a v tom nám všem GDPR pomůže
- Nařízení je napsáno poměrně obecně (musí být univerzální), umožňuje **volnější výklad**
- Přesto v něm jsou ty **nejpodstatnější věci jasně a důrazně popsány** → to je vodítko
- GDPR veškerá rozhodnutí o bezpečnosti OÚ přenáší **na vás**, stejně tak i všechna rizika
- Je zdůrazněna **zásada přiměřenosti** přijatých opatření → rozdíl mezi korporací a např. OSVČ

Shrnutí a doporučení: Pokud zpracováváte jakékoliv OÚ, nařízení se nevyhýbejte. K zajištění souladu vaší práce s GDPR přistupte zodpovědně a se zdravým „selským“ rozumem tak, abyste minimalizovali zpracovávané OÚ a zajistili jejich bezpečnost přiměřeně vaší velikosti a objemu zpracovávaných informací.

Celý proces přípravy na GDPR můžete svěřit dodavatelské firmě a zaplatit jí za to desítky tisíc - stejně tak ale ten největší objem práce zůstane na vás.

Nebo si vyhradte několik hodin času a základní přípravu si zpracujete sami. Právě v tom vám pomůže tato příručka. Srozumitelně vás v několika krocích provede přípravou na GDPR - bez zbytečností, složitostí a komplikací. Nabídne vám potřebné formuláře a podklady. Vyřešíte to podstatné, ušetříte čas, peníze a nervy.

Je pouze na vás, jestli zrealizujete všechny následující kroky, nebo si vyberete jen ty podle vás podstatné. Popsán je ideální postup, ale jak bylo uvedeno výše, zodpovědnost je na vaší straně.

Samozřejmě se může stát, že přijde kontrola a zjistí u vás nějaké nedostatky – v tom případě vás zřejmě **vyzve k jejich odstranění**, místo **pokuty nebo zákazu činnosti**, tak jak by to nejspíše bylo v případě ignorování GDPR a neexistence přípravy na něj.

Pro koho tato příručka není: pro střední a velké firmy, státní instituce, zpracovatele velkých objemů OÚ, zpracovatele citlivých a specifických údajů, jakékoliv nestandardní situace atd.

Přátelé, příručka je zpracována na základě mých praktických zkušeností, získaných při přípravě na GDPR pro subjekty z různých oborů a různých velikostí. Tato příručka je informační produkt, jejím stažením souhlasíte a potvrzujete, že jste si vědomi, že jakékoliv použití informací z příručky nebo jejích částí je plně na vaší zodpovědnost, ve vaší kompetenci a autor nenese žádnou zodpovědnost za případné důsledky.

Rozumíme si? Tak pojďme na to...

Krok 1: Začínáme...

Seznámíte se s GDPR, základními termíny, principy a povinnostmi

GDPR = General Data Protection Regulation, česky Obecné nařízení o ochraně OÚ

GDPR je již platné a v celé Evropské unii nabývá účinnosti dne **25. května 2018**

GDPR nahrazuje veškerou dosavadní právní úpravu v oblasti nakládání s OÚ

GDPR sjednocuje pravidla práce s OÚ, vymahatelnost a sankce jednotně v celé EU

Slovníček:

Subjekt údajů je jakákoliv identifikovaná nebo identifikovatelná fyzická osoba s nějakými OÚ.

Osobní údaj (OÚ) je jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě.

Co všechno může být osobní údaj? Příklady nejběžnějších OÚ najdete na straně 5.

Zpracování OÚ je jakákoliv operace nebo soubor operací s osobními údaji.

Správce údajů = VY – jakákoliv fyzická nebo právnická osoba, která spravuje nebo zpracovává OÚ.

Zpracovatel je fyzická nebo právnická osoba, která pro správce zpracovává OÚ (např. účetní atd.).

Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt dává svolení správci se zpracováním svých OÚ.

Porušení zabezpečení OÚ je protiprávní nebo náhodné zničení, ztráta, změna nebo poskytnutí OÚ.

Zvláštní kategorie OÚ jsou údaje o rasovém nebo etnickém původu, zdravotním stavu, politických názorech, náboženském vyznání, členství v odborech, genetické údaje, biometrické údaje atd.

Dozorový úřad je u nás Úřad pro ochranu osobních údajů.

Základní principy zacházení s osobními údaji:

Princip odpovědnosti = jen a pouze správce a nikdo jiný je odpovědný za dodržení zásad zpracování OÚ v souladu s GDPR a zároveň správce je povinen soulad s GDPR doložit.

Princip přístupu založeného na riziku = správce je povinen od začátku a neustále brát na vědomí a vyhodnocovat míru rizika při sběru a zpracování OÚ

Zásady zpracování osobních údajů:

Zákonnost – zpracování nesmí být v rozporu se zákonem a musí být prováděno z jednoho konkrétního a přesně vymezeného důvodu (pro splnění právní povinnosti; pro splnění smlouvy nebo opatření před přijetím smlouvy; pro ochranu životně důležitých zájmů; pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci; pro účely oprávněných zájmů správce; s uděleným souhlasem subjektu údajů).

Korektnost a transparentnost – zajišťovat co největší míru informovanosti subjektu údajů.

Účelové omezení – OÚ nesmí být zpracovávány k jinému účelu, než k jakému byly shromážděny.

Minimalizace údajů – zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah.

Přesnost – zpracovávané OÚ musí být přesné a podle potřeby aktualizované.

Omezení uložení – uložení OÚ může být realizováno pouze po dobu ne delší, než je nezbytně nutné pro účel zpracování (s ohledem na právní předpisy, promlčecí lhůtu atd.).

Integrita a důvěrnost – povinnost přijmout vhodná technická a organizační opatření zajišťující ochranu před neoprávněným nebo protiprávním zpracováním, ztrátou, zničením, poškozením.

Odpovědnost – dodržování všech uvedených zásad je na správci a musí být schopen to doložit.

GDPR se vztahuje na jakékoliv zpracování OÚ – na automatizované (data) i manuální (papírové)!

Krok 2: Zpracováváme...

Určete odpovědnou osobu a zjistěte, kde všude pracujete s osobními údaji

Právě teď se dostáváte do okamžiku, kdy začínáte pracovat na prokázání vašeho souladu s GDPR. Jak již víte, musíte být schopni **prokázat dodržování pravidel a souladu s GDPR. Ved'te si proto potřebnou dokumentaci – ideálně v písemné podobě – šanon, složku. Sem zakládejte všechny vyplněné formuláře a dokumenty.** Formuláře a dokumenty si můžete vytvořit sami (dejte pozor na to, aby obsahovaly všechny potřebné údaje).

Pokud dokumenty nechcete vymýšlet a tvořit, doporučuji vám stáhnout si je z webu:

www.GDPRstart.cz/dokumenty/

Zde najdete všechny dokumenty zmiňované v tomto návodu + spoustu dalších pomůcek, které vám vaši práci usnadní. Formuláře jsou pečlivě připravené, zkontrolované právní kanceláří a otestované v praxi. **Cena za kompletní sadu všech dokumentů, formulářů a bonusů je 1.990 Kč. Při objednání do 7-mi dní od stažení této příručky platí zvýhodněná cena 990 Kč.**

DPO – Data Protection Officer (pověřenec pro ochranu osobních údajů)

Vzhledem k určení této příručky zřejmě nemáte zákonnou povinnost DPO jmenovat (DPO musí mít orgán veřejné moci či veřejný subjekt, nebo subjekt, který provádí rozsáhlé, pravidelné a systematické monitorování občanů). Přesto můžete DPO jmenovat dobrovolně, jako další důkaz a podporu realizování souladu s GDPR. Bližší informace o DPO najdete na www.GDPRstart.cz/DPO/.

Vyplňte **Formulář A – Úvodní list**

(použijte formulář stažený z webu www.GDPRstart.cz/dokumenty/, nebo vytvořte vlastní)

Slouží jako úvodní list dokumentace GDPR, obsahuje všechny identifikační údaje správce (pro kterého se GDPR zpracovává), kontaktní osobu zodpovědnou u vás za dodržování nařízení, kontaktní údaje.

Vyplňte **Formulář B – Definice skupin subjektů a činností**

(použijte formulář stažený z webu www.GDPRstart.cz/dokumenty/, nebo vytvořte vlastní)

1. Vezměte si papír a tužku a vyznačte jakékoliv skupiny subjektů údajů, se kterými přicházíte do kontaktu (pomůže vám předpřipravený seznam stažený z webu): zaměstnanci, uchazeči o zaměstnání, dodavatelé – fyzické osoby, zákazníci, potenciální zákazníci, klienti, členové, uživatelé, pacienti atd.
2. Pro každou takovou u vás využívanou skupinu vyjmenujte všechny činnosti, při kterých dochází ke zpracování osobních údajů (opět vám může pomoci seznam z webu). Příklad: zaměstnanci – personální agenda, zaměstnanci – mzdová agenda, zaměstnanci – služební cesty atd.; zákazníci – objednávky, zákazníci – smlouvy, zákazníci – newsletter atd.

Bud'te důkladní, na nic nezapomeňte, toto je základ a podklad k realizaci dalších kroků!

Krok 3: Likvidujeme...

Vytrídíte, zrušíte a smažete osobní údaje, které nutně nepotřebujete

Díky předchozímu bodu máte před sebou seznam všech činností, při kterých u vás dochází ke zpracování osobních údajů.

Ted' se u každé vyjmenované činnosti zamyslete, jestli ji ke své práci opravdu nutně potřebujete, a jestli existuje alespoň jeden zákonný důvod pro zpracování OÚ během této činnosti – viz zásady zpracování OÚ ze stránky 3.

Zákonným důvodem může být (vždy je třeba vybrat pouze jeden):

- Splnění právní povinnosti
- Splnění smlouvy nebo opatření před přijetím smlouvy
- Ochrana životně důležitých zájmů
- Splnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci
- Ochrana oprávněných zájmů správce
- Udělený souhlas subjektu údajů (berte jako poslední možnost, snažte se využívat předchozí)

Ze svého seznamu vyškrtněte činnosti, které nejsou nezbytně nutné, ke kterým nemáte ani jeden zákonný důvod, nebo u kterých nemůžete zajistit náležitou bezpečnost OÚ (stále myslíte na to, že za používané OÚ zodpovídáte). Tyto činnosti budete muset zrušit.

U činností, které na vašem seznamu zůstaly a budete je nadále využívat, co nejvíce omezte zpracovávané OÚ (viz zásada minimalizace). Všechny nepotřebné a nedůležité údaje smažte.

Úplně stejně nemilosrdně postupujte při likvidaci starých a neaktuálních souborů osobních údajů, jako například zálohy na CD, síti, externích a cloudových úložištích, starých archivů a dokumentů, výkazů, jak v elektronické, tak v listinné podobě.

Pomůcka – co všechno může být osobní údaj:

*jméno, příjmení, trvalé bydliště, doručovací adresa, datum narození, místo narození, věk, rodné číslo, osobní stav, **zdravotní stav, zdravotní znevýhodnění**, fotografický záznam, video záznam, audio záznam, e-mailová adresa, soukromé i pracovní telefonní číslo, IP adresa, identifikační číslo, daňové číslo, číslo OP, číslo řidičského průkazu, číslo pasu, číslo bankovního účtu, vzdělání, příjem ze zaměstnání, příjem z důchodu, výkonnost, zdravotní pojišťovna, počet dětí, mateřská, nemocenská, benefity, plán a výkaz práce, **národnost, rasový a etnický původ, politické názory, náboženské a filozofické vyznání, členství v odborech, sexuální orientace, trestní delikty, pravomocná odsouzení, DNA, krevní skupina, Rh faktor krve, snímek obličeje, otisk prstu, snímek oční duhovky, snímek sítnice**, podpis, hlas, jméno, příjmení a pohlaví člena rodiny, adresa člena rodiny a vlastně úplně všechno týkající se člena rodiny....*

Červeně a tučně jsou vyznačeny OÚ zvláštní kategorie, při jejichž zpracování je nutné dbát zvýšené pozornosti, k jejich zpracování se vztahují další povinnosti a prakticky pokud nemáte zákonný důvod pro jejich zpracování, vždy si od subjektu údajů vyžádejte souhlas s jejich zpracováním.

Nyní máte aktualizovaný seznam všech činností a osobních údajů, které budete nadále při své práci využívat. V dalším kroku si každou činnost detailně projdeme a navrhujeme opatření pro zajištění souladu s GDPR.

Krok 4: Přemýšlíme & plánujeme...

Každé zpracování OÚ prověříte a navrhnete opatření zajišťující soulad s GDPR

Každý správce OÚ – tedy i vy - je povinen s přihlédnutím ke stavu techniky, nákladům, povaze, rozsahu, kontextu, rizikům a účelu zpracování provést vhodná technická a organizační opatření pro zabezpečení zpracovávaných OÚ. Je tedy pouze na vašem rozhodnutí, jaká opatření provedete, vždy ovšem s vědomím principu odpovědnosti a přístupu založeného na riziku (viz stránka 3).

Pro každou činnost a skupinu subjektů vytvořte záznam o činnostech zpracování – dokument, kde jsou přesně a přehledně uvedeny následující údaje:

- Jméno a kontaktní údaje správce (vás)
- Zákonné důvody a účely zpracování
(příklad: poskytování konzultací, ubytování hostů, prodej zboží, ...)
- Popis kategorií subjektů údajů a kategorií zpracovávaných osobních údajů
(příklad: klienti, ubytovaní návštěvníci, maloobchodní zákazníci, ...)
- Příjemci zpracovaných OÚ
(příklad: spolupracující subjekty, hotelová restaurace, rozvážková služba, ...)
- Informace o případném předání OÚ třetím stranám
- Lhůty pro výmaz jednotlivých OÚ
(příklad: po dobu trvání smluvního vztahu a tři roky po jeho ukončení)
- Popis technických a organizačních bezpečnostních opatření
(příklad: písemné záznamy – uzamčená skříň nebo trezor, PC – ochrana heslem a otisk prstu)

Ukázky a vzor vyplněného záznamu najdete na webu www.GDPRstart.cz/dokumenty/
Součástí jsou také seznamy usnadňující doplnění s nejčastěji používanými možnostmi.

Vyplňte **Formulář C – Záznam o činnostech zpracování** tolikrát, kolik druhů činností provádíte.
(použijte formulář stažený z webu www.GDPRstart.cz/dokumenty/ , nebo vytvořte vlastní)

Věnujte tomuto dokumentu velkou pozornost, u každé činnosti zvažte míru rizika, promyslete, jak můžete zabezpečit zpracovávané OÚ a co můžete udělat proto, aby nedošlo k jejich ohrožení nebo zneužití.

Opatření budou organizační a technická. Organizační upravují způsob zpracování, umístění, přístupy, pracovní postupy, omezení atd. Technická opatření se zabývají využitím technických prostředků a jejich nastavení tak, aby co nejlépe splňovaly požadavky ochrany OÚ. Všechna zvolená opatření a zajištění vyjmenujte v dokumentu a také je zrealizujte. Jak již bylo uvedeno výše, vše je na vašem zvážení a posouzení, na jaké úrovni je třeba OÚ ochránit.

Zároveň je toto také klíčový dokument, kterým můžete prokázat, že OÚ zpracováváte v souladu s GDPR. Buďte připraveni tyto dokumenty poskytnout v případě potřeby dozorovému úřadu.

Krok 5: Zamykáme & heslujeme...

Přijmete a provedete opatření také u používaných technických prostředků

V tomto kroku se budeme věnovat zajištění OÚ z pohledu používaných technických prostředků – sem patří budovy, dveře, kanceláře, skříně, trezory, zámky, klíče, zejména ale prostředky zajišťující automatizované zpracování údajů – IT technologie, hesla, počítače, sítě, telefony, tiskárny, software, hardware, data, cloudy atd.

Velkou pomůckou nám budou v předešlém kroku vytvořené záznamy o činnostech zpracování. Cokoliv uvedete v kolonce „Ochranná a bezpečnostní opatření“, zde byste měli popsat – jak to pomůže v ochraně OÚ, jaké je použito zabezpečení, co je potřeba udělat a zajistit, aby byl technický prostředek správně použit.

Aby to pro vás bylo co nejjednodušší, použijte připravený dotazník s různými variantami odpovědí:

Vyplňte **Formulář D – Popis technických opatření**

(použijte formulář stažený z webu www.GDPRstart.cz/dokumenty/ , nebo vytvořte vlastní)

Povinné ohlašování případů porušení zabezpečení OÚ dozorovému úřadu

Každý správce údajů, který se dozví o porušení zabezpečení zpracovávaných OÚ, musí nejpozději do 72 hodin od okamžiku, kdy se o porušení dozvěděl, tento incident ohlásit Úřadu pro ochranu osobních údajů a také incident zaevidovat. Porušení není třeba hlásit, jestliže je nepravděpodobné, že by toto porušení mělo za následek rizika pro práva a svobody subjektů údajů. Nahlásit je třeba popis daného porušení, jméno a kontaktní údaje správce, popis důsledků porušení a popis přijatých opatření.

Porušení je také třeba oznámit dotčenému subjektu údajů, pokud je pravděpodobné, že bude mít za následek vysoké riziko pro práva o svobody subjektu údajů.

Příklady technických prostředků a použitých opatření:

Data zpracovává:

- Informační systém, účetní systém, objednávkový systém, apod.
- Osoby pomocí tabulek, například v Excelu.
- Osoby ručně výpisem z databáze, apod. v papírové formě.
- Externí společnost na Vaši žádost.

Bezpečnostní opatření:

- Máte instalovány v objektu kamery.
- Máte instalován EZS a EPS.
- Váš objekt je střežen 24 hodin ostrahou.
- Objekt je rozdělen na zóny s omezeným přístupem, chráněný zabezpečením dveří.
- V objektu jsou speciálně upravené místnosti pro uložení dat (trezorová místnost, atd.).
- Jiná:

Krok 6: Souhlasíme...

Zajistíte souhlasy se zpracováním OÚ tam, kde nemáte jiný zákonný důvod

Souhlas se zpracováním osobních údajů potřebujete u činností, u kterých nelze uplatnit nějaký jiný zákonný důvod zpracování (viz strana 5). Připravte si různé druhy souhlasů, přesně podle toho, jak je budete využívat, podle formy (např. elektronický formulář na webu se zaškrťovacím políčkem, nebo písemný formulář s místem pro podpis) a podle účelu, ke kterému dává subjekt údajů souhlas. Platí, že OÚ nesmíte zpracovávat za jiným účelem, než ke kterému máte souhlas. Pokud budete potřebovat OÚ zpracovávat z jiného důvodu, musíte subjekt o souhlas požádat znovu.

Pozor: Souhlasy u dětí do věku 16ti let (15ti po schválení prováděcího zákona ČR) - zpracování OÚ je možné pouze s rodičovským souhlasem zákonného zástupce dítěte!

Každý souhlas se zpracováním OÚ by měl obsahovat:

- Jméno a kontaktní údaje správce (vás)
- Seznam poskytovaných OÚ (*příklad: jméno, příjmení, e-mail, telefonní číslo, ...*)
- Účely zpracování (*příklad: zasílání newsletteru na e-mail, zveřejnění fotek na webu, soutěže, ...*)
- Dobu, po kterou budou OÚ zpracovávány
- Informace o případných zpracovatelích, které správce pro zpracování OÚ využije
- Informace o existenci práva vzít souhlas kdykoliv zpět a jak to provést
- Informace o existenci práva požadovat přístup k OÚ, vysvětlit způsob zpracování, jejich opravu, vymazání, omezení zpracování, možnost vznést námitku proti zpracování, podání stížnosti k dozorovému úřadu
- Vlastní udělení výslovného souhlasu a datum
(*příklad: elektronicky na webu **nezaškrtnutý** checkbox + tlačítko, písemně místo pro podpis*)

Připravte dle potřeby různé **Formuláře E – souhlas se zpracováním OÚ**

(použijte vzor souhlasu stažený z webu www.GDPRstart.cz/dokumenty/, nebo vytvořte vlastní)

Myslete na to, že každý udělený souhlas musíte umět doložit, proto je pečlivě archivujte – ať už papírové podepsané formuláře, nebo elektronické souhlasy s IP adresou a časovým razítkem.

Pokud již při nějaké stávající činnosti zpracováváte OÚ dle zákonného důvodu „Souhlas...“, a potvrzené souhlasy od subjektů údajů nemáte, máte ho k jiné činnosti nebo neodpovídají uvedeným požadavkům GDPR, musíte subjekty o souhlas požádat znovu, nebo je nezpracovávat.

Souhlas může být buďto samostatný dokument, nebo může být zakomponován do jiného dokumentu, který s klientem podepisujete. Musí být však jasně odlišitelný od dalšího obsahu, srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.

Shrnutí: subjekt údajů musí jasně a úplně pochopit, kdo souhlas chce, k jakým údajům, pro jaký účel, na jak dlouho, jestli bude mít k údajům přístup někdo další a jaká má práva.

A na závěr ještě jedna praktická informace: pokud jste se subjektem údajů ve smluvním vztahu (je to například stávající zákazník), nemusíte mít pro zpracování OÚ při souvisejících činnostech udělený výslovný souhlas – zde je důvodem plnění smlouvy nebo váš oprávněný zájem. Příklady: objednání termínu na masáž nebo ke kadeřnici, zasílání newsletteru (při zajištění všech platných požadavků: možnost odhlášení, uvést pravé jméno a platný e-mail, označit jako obchodní sdělení).

Krok 7: Směrnícujeme...

Vytvoříte si interní směrnici, která stanoví pravidla a postupy práce s OÚ

Vytvořením interního dokumentu – směrnice - jednoznačně deklarujete vaše principy zacházení s OÚ a jejich zpracovávání v souladu s GDPR. Může se na ni odvolat pracovní smlouva (v případě, že máte zaměstnance), k jejímu dodržování zavažte spolupracovníky nebo členy.

Ve směrnici uveďte zásady a postupy při zpracování OÚ jak elektronicky s využitím IT, manuálně v papírové podobě a také obecná technická a organizační zabezpečení. Z povahy věci vyplývá, že směrnice bude u každého správce více či méně rozdílná, v závislosti na nastavených pracovních postupech.

Určitě ale chybu neuděláte, když si z webu stáhnete vzor směrnice, projdete si ji a potřebné části upravíte – zde jsou klíčovým vodítkem vaše již vyplněné formuláře záznamů o činnosti zpracování a opatření u používaných technických prostředků (viz strana 6 a 7). Jednoduše do vzoru směrnice doplníte vámi nastavená opatření a postupy.

Do směrnice také uveďte postup v případě, že dojde k porušení zabezpečení zpracovávaných OÚ.

Zjednodušeně řečeno: uveďte kdo, kdy a jak může u vás zpracovávat osobní údaje a jak jsou zabezpečeny proti zničení, ztrátě nebo zneužití, co dělat a co nedělat.

Použijte **Formulář F – Směrnice pro práci s OÚ** a rychle a jednoduše vytvořte vlastní směrnici. (použijte formulář stažený z webu www.GDPRstart.cz/dokumenty/, nebo vytvořte vlastní)

Příklady znění textů uvedených ve směrnici:

- *Všichni zaměstnanci, kteří přicházejí do styku s výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí možnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou ICT, požárem, živelní pohromou atp.*

Nebo třeba:

- *V uzamykatelném prostoru budou dokumenty obsahující osobní údaje umístěny do samostatných a uzamykatelných skříní, trezorů, boxů, nebo jiného obdobného vybavení.*
- *Klíče a přístupy od vybavení uzamykatelného prostoru i jeho vybavení bude mít k dispozici pouze pověřená osoba. Klíče musí mít pověřená osoba neustále při sobě.*
- *Pověřené osoby jsou povinny zamykat uzamykatelné prostory v době své nepřítomnosti, a to i v případě krátkodobé nepřítomnosti.*
- *Oprávněné osoby jsou povinny zabezpečit uzamykatelné prostory před vnějším vniknutím třetích osob dveřmi, okny, či jinými obdobnými přístupovými možnostmi.*

Krok 8: Zaměstnáváme...

Informujete a proškolíte zaměstnance tak, aby s OÚ pracovali bezpečně

V úvodu je třeba zdůraznit, že veškerá zodpovědnost – z hlediska dozorového orgánu - za zpracovávání OÚ v souladu s GDPR je na správci údajů, nikoliv na jeho zaměstnancích. Proto je třeba věnovat pozornost vysvětlení alespoň základních principů ochrany OÚ, případně zaškolení zaměstnanců a také založit informaci o provedeném poučení zaměstnance do jeho pracovní složky.

Nejen to, že vaši zaměstnanci zpracovávají OÚ například vašich zákazníků nebo členů, samozřejmě i oni sami jsou pro vás subjekty údajů, proto musíte s jejich OÚ zacházet s náležitou péčí a dle všech zásad GDPR. Z pohledu personální a mzdové agendy po zaměstnancích požadujte pouze ty informace, které jsou ze zákona nutné a nezbytné, velkou pozornost (zvýšené zabezpečení atd.) věnujte zpracování zvláštní kategorie OÚ, jako je jejich zdravotní stav (viz strana 5).

Pokud chcete nebo potřebujete zpracovávat OÚ zaměstnanců z jiného důvodu než splnění právní povinnosti, **vyžádejte si jejich souhlas**. Týká se to například marketingových účelů, různých akcí, zájezdů a podobně.

I u zaměstnanců nebo potenciálních zaměstnanců důsledně mažte všechny OÚ, které již nejsou platné, nebo je nepotřebujete.

Příkladem může být nábor nových zaměstnanců: při zařazení do výběrového řízení uchazečů o zaměstnání si s předáním životopisu a dalších dokladů vyžádejte souhlas s jejich zpracováním. Když je uchazeč vybrán, potřebné informace založte do jeho personální složky. Když ne, bez odkladu je smažte.

Pracovní smlouvy se GDPR dotkne buď minimálně, nebo vůbec ne. V podstatě jde pouze o ověření, že do smlouvy neuvádíte OÚ, které nejsou nezbytně nutné. A druhou možnou úpravou je doplnění smlouvy o ujednání, že zaměstnanec byl náležitě poučen a proškolen ohledně zpracovávání osobních údajů fyzických osob, se kterými přijde při své práci do kontaktu a bude se řídit platnou směrnicí zaměstnavatele. V praxi lze toto také vyřešit podepsáním dodatku ke smlouvě a účasti na školení (podobně, jako se řeší BOZP a PO).

Podle svých potřeb a uvážení zpracujte následující kroky:

Použijte a upravte **Formulář G – Pracovní smlouva – dodatek ochrana osobních údajů**
a

připravte si **Formulář H – Školení zaměstnanců o ochraně OÚ + potvrzení účasti**

(použijte formuláře stažené z webu www.GDPRstart.cz/dokumenty/ , nebo vytvořte vlastní)

Nezapomínejte průběžně proškolovat nové zaměstnance (ideálně při nástupu do zaměstnání) a kontrolovat dodržování směrnice a všech přijatých opatření.

Krok 9: Smlouváme...

Upravíte smlouvy s dodavateli, odběrateli a zpracovateli OÚ

Co je zpracovatelská smlouva a s kým je třeba ji uzavřít?

Pokud využíváte služeb nějakého dalšího subjektu a předáváte mu ke zpracování vámi spravované OÚ, máte za povinnost uzavřít s ním smlouvu o zpracování osobních údajů – zpracovatelskou smlouvu. Tato situace v praxi nastává docela často – například když využíváte služeb účetní kanceláře, daňového poradce, právní kanceláře, necháváte si externě zpracovávat mzdovou agendu, náборы zaměstnanců, nebo v oblasti marketingu – správa webu, rozesílání e-mailů, akce „na klíč“, ale i třeba pokladní systém s ukládáním dat na serveru dodavatele. Ve všech těchto případech – zpracovává-li pro vás spolupracující subjekt OÚ – **s daným subjektem musíte zpracovatelskou smlouvu uzavřít.**

Účelem smlouvy je zajistit náležitou bezpečnost vámi spravovaných OÚ, i když se dostanou z vašeho dosahu. Ve smlouvě je uvedeno, kdo, kdy, jak, jaké OÚ a za jakých podmínek bude vaše OÚ zpracovávat.

Ta pozitivní věc je, že naprostá většina firem poskytující tyto služby bude mít smlouvu připravenou. Buďto vám její uzavření nabídne sama, nebo ji k tomu vyzvěte. Také si můžete vzor smlouvy obsahující všechny náležitosti stáhnout z webu, doplnit potřebné údaje a se zpracovateli ji uzavřít.

Použijte **Formulář I – Zpracovatelská smlouva**, doplňte ji a uzavřete se všemi zpracovateli (použijte vzor stažený z webu www.GDPRstart.cz/dokumenty/, nebo vytvořte vlastní)

Jak upravit smlouvy s dodavateli, obchodními partnery, zákazníky, klienty?

Pokud si vybavíte zákonné důvody pro zpracování OÚ (strana 5), tak zjistíte, že podstatná část údajů uvedených ve smlouvách (znovu upozorňuji, že GDPR se týká fyzických osob, **NE** právnických) se schová pod splnění právní povinnosti, splnění smlouvy nebo oprávněné zájmy správce.

Pokud však ve smlouvách máte nějaké další OÚ, nebo je plánujete zpracovávat ještě při jiných činnostech, nebo k jiným účelům, než které jsou předmětem smlouvy, **vždy do smlouvy přidejte vyjádření souhlasu se zpracováním OÚ** (jak již víte, souhlas musí být dobrovolný, jednoznačný a informovaný). Pokud je souhlas součástí smlouvy, musí být snadno jednoznačně oddělitelný od dalšího obsahu (nesmí se nikde pod ničem schovávat), srozumitelný a jeho udělení nesmí být podmínkou vlastního plnění smlouvy. Ideálním řešením je například vlastní článek, nebo odstavec. Pokud by získání souhlasu komplikovalo smlouvu, bude vhodnější jeho udělení řešit na zvláštním dokumentu.

Co všechno je třeba zakomponovat do smlouvy obsahující souhlas / do zvláštního souhlasu? Vše podstatné najdete na již použitém dokumentu (strana 8) **Formulář E – souhlas se zpracováním OÚ** (z webu www.GDPRstart.cz/dokumenty/).

Gratuluji vám, to je všechno...

Pokud jste postupovali podle této příručky, máte nyní šanon nebo složku, která obsahuje:

- Úvodní list s identifikačními a kontaktními údaji vás – správce (dokument A)
- Vytisknuté základní pojmy, principy, povinnosti a zásady GDPR
- Vyjmenované skupiny subjektů a činností, při kterých zpracováváte OÚ (B)
- Záznamy o všech činnostech zpracování OÚ s vyznačenými opatřeními (C)
- Podrobný výčet technických opatření pro zabezpečení OÚ (D)
- Systém pro získávání a uchovávání všech souhlasů se zpracováním OÚ (E)
- Máte vytvořenou interní směrnici pro práci s OÚ v souladu s GDPR (F)
- Upravili jste pracovní smlouvy (G) v souladu s ochranou OÚ
- Připravili jste školení pro zaměstnance a systém pro evidování jeho účastníků (H)
- Máte uzavřenou zpracovatelskou smlouvu se všemi zpracovateli (I)
- A konečně upravili jste všechny dodavatelské a odběratelské smlouvy dle zásad GDPR

Jak jsem již zmiňoval dříve, dle vaší konkrétní situace nemusíte potřebovat realizaci všech uvedených kroků, nebo se můžete svobodně rozhodnout některé kroky vynechat. V této příručce uvedený postup je ale docela neprůstřelný plán, jak mít GDPR vyřešené.

SNADNO

RYCHLE

BEZPEČNĚ

LEVNĚ

Nyní máte zpracováno to nejdůležitější, co je třeba k prokázání souladu vaší práce a zpracování osobních údajů s **GDPR a 25. květen 2018 pro vás už není strašákem.**

Samozřejmě je třeba dodržovat všechna přijatá opatření a postupy, mít v pořádku a pro případ kontroly nebo problému připravenou dokumentaci, sledovat novinky a změny v oblasti zpracování osobních údajů a vše aktualizovat dle případných změn a potřeb.

S úctou, Tomáš Říha
www.GDPRstart.cz