SEDLAKOVA
LEGAL

Co pro mě znamená GDPR?

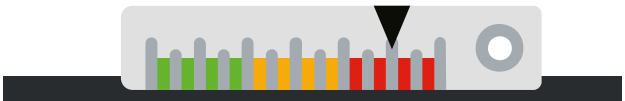
ZÁKLADNÍ INFORMACE

GDPR je zkratkou pro Obecné nařízení o ochraně osobních údajů. Toto nařízení, vydané Evropskou unií, začne platit od 25. 5. 2018 ve všech členských státech EU, včetně České republiky. Na rozdíl od evropských směrnic nařízení nevyžaduje ze strany České republiky přijetí jakýchkoliv prováděcích předpisů a jeho účinnost je tak nevyhnutelná. GDPR je jedním z nejrobustnějších předpisů, které EU v posledních letech přijala, a reguluje, jak mají správci osobních údajů s těmito údaji nakládat. GDPR téměř zcela nahradí současný český zákon o ochraně osobních údajů, přičemž zavádí celou řadu nových konceptů.

Vztahuje se na moji společnost GDPR?

- ☐ Máme zaměstnance
- ☐ Našimi zákazníky jsou mimo jiné fyzické osoby, například spotřebitelé či OSVČ
- ☐ Za účelem marketingu si vytváříme nebo využíváme databáze osobních údajů
- ☐ Máme automatizované nástroje, které vytváří profily anebo modely chování subjektů údajů

Pokud jste zaškrtli alespoň jedno pole, bude na Vaši společnost dopadat GDPR.



GDPR – Měřítko nutných změn

Nové povinnosti správců osobních údajů podle GDPR

Krom stávajících povinností správců zavádí GDPR několik nových konceptů, které musí do 25. 5. 2018 všichni správci adoptovat. V tomto přehledu stručně popisujeme z našeho pohledu nejzásadnější novinky a změny. Následující text, jakož i GDPR pracují s řadou pojmů. Pro usnadnění najdete na konci dokumentu glosář s jejich výkladem.

Přičitatelnost a privacy by design

GDPR pracuje s principem privacy by design, který znamená, že ochrana osobních údajů by měla být zakomponována do všech fází jakéhokoliv řešení, tzn. i do návrhu řešení, a měla by k tomu vždy existovat dokumentace. V praxi se to projeví tak, že pokud půjde správce na trh s novým řešením, už při jeho vývoji jej bude navrhovat s ohledem na ochranu osobních údajů a povede dokumentaci o přijatých opatřeních na ochranu osobních údajů. Správce musí být schopen přijatá opatření doložit.

Zpracovatelské smlouvy

Většina správců, aniž by si to uvědomovala, již dnes využívá pro zpracování osobních údajů řadu zpracovatelů, od poskytovatelů uložišť přes společnosti, které v rámci servisu obsluhují systémy obsahující osobní údaje. I podle dosavadní právní úpravy je nezbytné mít s těmito zpracovateli uzavřenou zpracovatelskou smlouvu. Dosavadní právní úprava však stanovila jen minimum náležitostí, jaké taková smlouva musí obsahovat. GDPR jde v tomto ohledu dál a obsahuje řadu dalších náležitostí.

V praxi to pro správce znamená znovu otevřít jednání se zpracovateli, většinou dodavateli ICT řešení, a vzájemné smlouvy doplnit. Podle velikosti organizace může být vhodné začít s tímto krokem již nyní.

Organizační a technické prostředky zabezpečení osobních údajů

Ačkoliv i podle dosavadní právní úpravy museli správci zabezpečit všechny osobní údaje vhodnými organizačními a technickými prostředky, tyto prostředky nebyly nikde výslovně stanoveny. GDPR naopak obsahuje seznam doporučených prostředků, které by správci měli přijmout. Ačkoliv je seznam zřejmě jen demonstrativní, správcům se doporučuje přijmout co nejvíc z doporučených prostředků. GDPR zejména klade důraz na častější využití pseudonymizace osobních údajů, kde to je možné.

Posuzování úrovně ochrany osobních údajů

Oproti dosavadní právní úpravě, kdy se správci obecně registrovali u Úřadu pro ochranu osobních údajů (oznamovali zpracování), GDPR od registrace zcela upouští. Namísto toho mají nyní správci povinnost posuzovat vliv konkrétních zpracování osobních údajů na práva subjektů údajů a v případě rizikových zpracování vypracovat analýzu, kterou následně konzultují s pověřencem ochrany osobních údajů (pokud jej mají) a v určitých případech i s dozorovým úřadem před zahájením zpracování.

Aby správci dostáli této povinnosti, budou muset přijmout několik nových opatření, zejména:
A) pokud jsou veřejnoprávním subjektem nebo zpracovávají citlivé (zvláštní) kategorie osobních údajů či systematicky a rozsáhlým způsobem zpracovávají osobní údaje, musí správci jmenovat ve své společnosti pověřence ochrany osobních údajů

B) vypracovat systém posuzování vlivů – jelikož u správců často dochází k několika různým zpracováním osobních údajů a tyto se můžou s časem měnit, je vhodné implementovat jednotný systém, jakým bude správce posuzovat vlivy.

Oznámení porušení zabezpečení osobních údajů

Správce osobních údajů je podle GDPR povinen oznamovat dozorovému úřadu všechny závažné případy porušení zabezpečení osobních údajů, tj. případy náhodného nebo protiprávního zničení, ztráty, změny nebo neoprávněného poskytnutí nebo zpřístupnění zpracovávaných osobních údajů. Toto oznámení by měl učinit bez zbytečného odkladu nejpozději do 72 hodin od chvíle, kdy došlo k porušení, jinak musí prodlení zdůvodnit.

Pokud porušení přináší vysoké riziko pro práva a povinnosti subjektů údajů, má správce povinnost porušení oznámit i všem dotčeným subjektům údajů.

Aby správci dostáli této povinnosti, opět bude vhodné implementovat systémy, které dokáží monitorovat a včas reagovat na případy porušení zabezpečení osobních údajů. Má-li správce pověřence ochrany osobních údajů, je důležité tuto povinnost koordinovat s pověřencem.

SROZUMITELNÝ JAZYK PRO KOMUNIKACI SE SUBJEKTY ÚDAJŮ

Stávající povinnosti správců informovat subjekty osobních údajů o zpracování osobních údajů se co do rozsahu zásadně nemění. GDPR však klade velký důraz, aby jazyk dokumentů využívaných pro komunikaci se subjekty údajů byl jasný a srozumitelný. Stávající dokumentaci, jako jsou souhlasy a poučení o zpracování osobních údajů je tedy vhodné přezkoumat a upravit tak, aby odpovídala nově vyžadovaným standardům.

Právo na přenositelnost osobních údajů

Toto právo subjektů údajů se týká správců, kteří provádějí zpracování osobních údajů (i) na základě souhlasu subjektů údajů (ii) automatizovanými prostředky. Tito správci mají povinnost na žádost subjektu údajů vydat jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu tak, aby mohli mimo jiné údaje předat jinému správci. Za tímto účelem bude u některých správců nezbytné implementovat nové systémy, které dokáží souhrnnou informaci v požadované formě vydat. Tato povinnost může být významná zejména u poskytovatelů telekomunikačních služeb nebo v oblasti energetiky.

Správci osobních údajů, kteří se nepřizpůsobí GDPR do 25. 5. 2018 se vystavují riziku sankce ze strany dozorového úřadu, která může činit až 20 milionů EUR nebo 4 % z celosvětového obratu, podle toho, která částka je vyšší.

Před uložením pokuty mají dozorové úřady celou řadu prostředků, jak upozornit správce, že nezpracovává osobní údaje v souladu s GDPR. Jedná se o například o písemné upozornění, napomenutí, nařízení uvést zpracování do souladu s GDPR či uložit dočasné nebo trvalé omezení zpracování. Možností dozorových úřadů je více. S ohledem na rozsah, účel a povahu zpracování osobních údajů očekáváme, že ze začátku GDPR budou dozorové úřady využívat převážně tyto prostředky před pokutami a budou mírnější.

Jak se máme na GDPR připravit?

1 Připravte se na případy porušení zabezpečení osobních údajů. Je nezbytné přijmout postupy a vnitropodnikové předpisy, abyste byli schopni rychle a efektivně reagovat na případy porušení zabezpečení osobních údajů v souladu s nejlepší praxí.

2 Zdokumentujte probíhající a nastávající zpracování osobních údajů včetně přijatých opatření pro jejich zabezpečení. Dostojíte tím principu přičitatelnosti. O každém opatření je vhodné vést paper trail neboli písemnou dokumentaci.

3 V rámci vývoje nových řešení přijměte princip privacy by design a inkorporujte do svých plánů ochranu osobních údajů. Nezapomeňte na paper trail.

4 Přezkoumejte báze, na základě kterých zpracováváte osobní údaje. Ať již provádíte zpracování na základě souhlasů nebo uložené zákonem, prověřte, zda máte stále zákonné podklady pro zpracování. Nezapomeňte, že zákonnost zpracování musíte být vždy schopni doložit.

5 Prověřte, zda Vaše organizačně-technická opatření zabezpečení osobních údajů naplňují nejnovější standardy a jsou přiměřená k rizikům souvisejícím se zpracováním. Je vhodné zkoumat, zda není na místě přijmout některá z doporučených organizačně-technických prostředků ochrany osobních údajů, například pseudonymizaci.

6 Přezkoumejte dokumentaci, kterou používáte pro komunikaci se subjekty údajů. Jakékoliv kodexy chování, obchodní podmínky, poučení o zpracování osobních údajů a další dokumenty týkající se zpracování osobních údajů určené pro subjekty údajů by měly používat jasnou, transparentní a srozumitelnou řeč.

7 Pokud využíváte služby zpracovatelů, například uložiště dat, správu informačních systémů s osobními údaji apod., přezkoumejte a patřičně upravte Vaše zpracovatelské smlouvy.

Glosář pojmů

GDPR pracuje s řadou právních pojmů. V tomto glosáři najdete vysvětlivky k těm, které považujeme za nejdůležitější:

Osobní údaj	Jakákoliv informace o subjektu údajů, která sama o sobě nebo v kombinaci s jinými informacemi může vést k identifikaci subjektu údajů. Osobními údaji jsou například jméno, příjmení a adresa bydliště subjektu údajů, ale mohou jimi být také informace o jeho vnějším vzezření, kamerový záznam či fotografie, informace o pracovní pozici, náboženském vyznání, mzdě nebo další informace, které ve své kombinaci mohou vést k identifikaci subjektu údajů.
Posouzení vlivů	Analýza, kterou provede správce před zpracováním osobních údajů, vyhodnocující možná rizika zpracování osobních údajů a obsahující seznam přijatých bezpečnostních opatření, která mají rizika minimalizovat.
Pověřenec ochrany osobních údajů (tzv. DPO)	Osoba, která ve společnosti plní řadu důležitých úkolů ve vztahu k GDPR. Pověřenec například posuzuje vliv zpracování osobních údajů na práva subjektů údajů, monitoruje všechna zpracování osobních údajů ve společnosti, komunikuje s dozorovým úřadem a poskytuje společnosti poradenství. Některé společnosti podle GDPR pověřence ochrany osobních údajů jmenovat musí.
Právo být zapomenut	Právo subjektů údajů na to, aby správci vymazali veškeré osobní údaje těchto subjektů údajů a přestali je dále zpracovávat.
Přenositelnost osobních údajů	Právo subjektů údajů na vydání jejich osobních údajů od správce ve strukturovaném, běžně používaném a strojově čitelném formátu tak, aby mohli tyto údaje například předat ke zpracování jinému správci.
Pseudonymizace	Zpracování osobních údajů tak, že nemohou být přiřazeny ke konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně opatření, aby bylo zajištěno, že nebudou přiřazeny k subjektu údajů.
Souhlas se zpracováním osobních údajů	Jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Souhlasem tak může být písemné prohlášení, ale například také ústní projev vůle.
Správce	Každá osoba, která sama, nebo společně s jinými osobami určuje účely a prostředky zpracování osobních údajů. Správcem osobních údajů jsou tedy mimo jiné společnosti, které si vedou databáze svých zaměstnanců.
Subjekt údajů	Každá fyzická osoba v Evropském hospodářském prostoru i mimo něj. Subjektem údajů jsou tedy např. zahraniční fyzické osoby či podnikatelé, podnikající jako takzvané OSVČ.
Zpracovatel	Každá osoba, která zpracovává osobní údaje pro správce. Zpracovatel je tedy osobou, která na pokyn správce provádí s osobními údaji nějaké operace. Zpracovatelem může být například poskytovatel datového uložiště, na které správce ukládá osobní údaje.
Zpracování osobních údajů	Jakákoliv operace či soubor operací s osobními údaji. Zpracování zahrnuje například shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení, zkombinování, omezení, výmaz nebo zničení osobních údajů. Každá z uvedených operací je i sama o sobě zpracováním osobních údajů.
Dozorový úřad	Nezávislý státní orgán, dohlížející nad dodržováním GDPR. V České republice jím je Úřad pro ochranu osobních údajů.

Kontakty

Najdete nás na adrese Purkyňova 648/125, 621 00 Brno

Zavolejte nám
739 390 182

Nebo pište
office@sedlakovalegal.com

Jana Sedláková
jana@sedlakovalegal.com | +420 739 314 413

Jiří Císek
jiri.c@sedlakovalegal.com | +420 739 643 235

Klára Bortlíková
klara.b@sedlakovalegal.com | +420 774 020 843

Břetislav Chod
bretislav.ch@sedlakovalegal.com | +420 777 039 899