Wolters Kluwer

Když si musíte být jistí

GDPR a vaše právnická firma

Poznejte své právní povinnosti vyplývající z nového obecného nařízení o ochraně osobních údajů v oblasti práv klientů na soukromí a ochrany jejich údajů.

Úvod

Dne 25. května 2018 vstoupí v platnost evropské obecné nařízení o ochraně údajů, které nahradí směrnici o ochraně údajů z roku 1995 (směrnici 95/46/ES).

Podle nového GDPR budou správci údajů muset vynaložit výrazně více úsilí, aby splnili nově upravené požadavky na ochranu údajů. Teď už nejde jen o dodržování osvědčených postupů pro zpracování soukromých údajů a prevenci porušení zabezpečení údajů. Právní předpisy upravující práva jednotlivců, požadavek na vedení evidence o postupech používaných při zpracování údajů a potřeba **zavedení náležitých technických a organizačních opatření** pro zajištění úrovně bezpečnosti odpovídající danému riziku představují pro právnické firmy zcela nové výzvy.

Správcům nesplňujícím příslušné požadavky mohou být uloženy pokuty až do výše **20 milionů eur nebo 4 % jejich celosvětových příjmů,** to ale není všechno. V závislosti na místních předpisech o ochraně údajů byste také mohli být ve Vaší jurisdikci **vystaveni postihu za porušení zabezpečení údajů a/nebo mohli nést osobní odpovědnost.** Německý spolkový zákon o ochraně údajů stanovuje pokuty za přestupky nebo dokonce tresty odnětí svobody za trestné činy. Francouzský trestní zákoník uvádí celou řadu trestných činů souvisejících s neplněním nebo porušováním právních předpisů o ochraně údajů, za které může být **fyzickým osobám uložen pětiletý trest odnětí svobody a pokuta ve výši 300 000 eur** (v případě právnických osob je tato pokuta pětkrát vyšší)[2].

Právnické firmy disponují obrovským množstvím citlivých údajů týkajících se fyzických osob a společností, což z nich dělá potenciálně lukrativní terč pro hackery, kteří chtějí tyto údaje zneužít nebo za ně požadovat výkupné. Skutečnost, že právnické firmy jsou ideálním terčem pro kybernetické útoky, o to víc zvyšuje důležitost plnění GDPR. Právnické firmy musí nejenže zajistit, aby i ony samy splňovaly toto nařízení, **aby se tak vyhnuly riziku pokut,** ale také, jak se dozvíme níže v tomto materiálu, musí vynakládat mimořádné úsilí, aby **zabránily jeho porušení,** protože podle GDPR jej musí zveřejnit – a takové odhalení může být **pro pověst firmy katastrofální.**

Abychom vaší právnické firmě pomohli připravit se na plnění požadavků GDPR, sepsali jsme 5 klíčových bodů týkajících se vašich nových povinností, jejich praktických důsledků a způsobu, jak chránit údaje vašich klientů.

1. Znát právní základ pro používání osobních údajů

Kdy a jak může moje firma zpracovávat osobní údaje klientů?

Článek 6 GDPR stanovuje, že zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- subjekt údajů udělil souhlas;
- je to nezbytné pro splnění smlouvy se subjektem údajů nebo pro uzavření smlouvy;
- je to nezbytné pro splnění právní povinnosti;
- je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné osoby;
- je to nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- je to nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy, práva nebo svobody subjektu údajů.

Pokud spoléháte na **souhlas**, musíte zajistit, aby byl **vyžádaný, získaný, zaznamenaný, sledovaný a upravený** podle požadavků GDPR. Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle daného jedince. Fyzické osoby mají **právo být informovány** o tom, jak a kým budou jejich osobní údaje použity, pro jaké účely, na jak dlouho atd. U zvláštních kategorií osobních údajů (tj. údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení) musí souhlas výslovně odkazovat na tyto údaje. Nutností je určitá forma **jednoznačného potvrzení** – jinými slovy, výslovného souhlasu (tzv. opt-in). Souhlas nelze vyvozovat z nečinnosti nebo předem zaškrtnutých políček.

Souhlas může být implicitní pouze v rozsahu, v jakém může být mlčky předpokládán na základě vztahu subjektu údajů se společností. Kupříkladu pokud firma poskytovala služby, předpokládá se, že dané údaje mohou být použity pro účely poskytování těchto služeb. Nicméně pro zasílání e-mailových marketingových sdělení firma potřebuje výslovný souhlas.

V případech, kdy je zpracování založeno na souhlasu, musí být tento souhlas **ověřitelný,** což znamená, že správce musí být schopen souhlas doložit. Právnické firmy proto budou muset zkontrolovat, zda dokumenty a formuláře souhlasů odpovídají aktuálním požadavkům. Žádosti o souhlas musí být jednoznačné a jasné, oddělené od ostatních podmínek. Fyzické osoby navíc mají právo svůj souhlas kdykoli stáhnout, takže Váš systém evidence souhlasů musí být dostatečně flexibilní, aby bylo možné údaje na základě žádosti odstranit.

A konečně spoléhání se na souhlas klienta nutně neznamená, že můžete dané údaje používat pro jiné účely, aniž byste získali nový souhlas. Budete zřejmě potřebovat nalézt alternativní právní základ, nebo budete muset ukončit nebo nezačínat jejich zpracování.

Důsledky:

- Údaje zpracovávejte pouze korektním a zákonným způsobem a zastavte veškeré zpracovávání, které je neslučitelné, včetně poskytování údajů třetím stranám.
- Shromažďujte pouze údaje, které konkrétně potřebujete. Pokud je rozsah případu neznámý, může být dodržení tohoto pravidla náročné. V takovém případě může být pro firmy vhodné zintenzivnit kontroly toho, co zaměstnanci shromažďují, a posoudit, zda jsou tyto údaje relevantní a nezbytné.

2. Znát práva svých klientů

Jaká práva mají moji klienti ohledně svých údajů?

Vedle práva kdykoli stáhnout svůj souhlas mají subjekty údajů celou řadu práv, které jsou vysvětleny v kapitole 3 GDPR (články 12-23). GDPR stanovuje následující práva fyzických osob:

1. **Právo na informace:** informace o tom, kdo, co, kdy, jak a kde bude údaje zpracovávat.
2. **Právo na přístup:** právo získat potvrzení o tom, že jejich údaje jsou zpracovávány; přístup ke svým osobním údajům; další doplňující informace.
3. **Právo na opravu:** fyzické osoby mají právo požadovat, aby byly jejich osobní údaje opraveny, jsou-li nepřesné nebo neúplné. Pokud jste takové osobní údaje poskytli třetím stranám, musíte je informovat o jejich opravě, je-li to možné. Stejně tak musíte v příslušných případech informovat danou osobu o třetích stranách, kterým byly tyto údaje poskytnuty.
4. **Právo na výmaz:** neboli „právo být zapomenut“ – fyzické osoby mají právo požadovat, aby jejich osobní údaje byly vymazány, a také právo zabránit jejich zpracování.
5. **Právo na omezení zpracování:** fyzické osoby mají právo požadovat, abyste přestali používat jejich údaje.
6. **Právo na přenositelnost údajů:** to znamená, že fyzické osoby mohou získat a opakovaně používat své osobní údaje pro své vlastní účely napříč různými službami (tj. možnost snadného přenosu osobních údajů z jednoho IT prostředí do jiného bezpečným a zabezpečeným způsobem bez narušení jejich použitelnosti).
7. **Právo vznést námitku:** znamená, že fyzické osoby mohou vznést námitku proti zpracování na základě oprávněných zájmů, námitku proti přímému marketingu či profilovacím činnostem nebo námitku proti zpracování pro výzkumné a statistické účely.
8. **Práva související s automatizovaným rozhodováním a profilováním:** fyzické osoby mají právo rozhodnout se nebýt součástí automatizovaného rozhodování, které má pro ně právní účinky nebo se jich obdobným způsobem významně dotýká.

Důsledky:

- Zajistěte, aby pravidla ochrany soukromí byla aktuální a obsahovala náležité informace o právech klientů, včetně jejich práva omezit zpracování nebo vznést námitku proti zpracování.
- Zajistěte přesnost a aktuálnost údajů, které máte k dispozici. To může pro firmy znamenat kontaktování klienta za účelem ověření přesnosti údajů nebo poskytnutí klientovi přístup do chráněného systému, kde může opravovat údaje nebo žádat o jejich odstranění.
- Zajistěte zavedení náležitých technických a administrativních mechanismů pro splnění požadavků na přístup, výmaz, omezení zpracování a přenositelnost.
- Zaveďte opatření pro likvidaci údajů, jakmile dané osobní údaje přestanou být potřeba v souvislosti s účelem, pro který byly původně získány/zpracovány.
- V případě námitek zajistěte, abyste byli schopni prokázat závažné legitimní důvody pro zpracování údajů, které převažují nad zájmy, právy a svobodami daného jednotlivce, nebo že zpracování probíhá z důvodu určení, výkonu nebo obhajoby právních nároků.

3. Znát odpovědnost své firmy

Co musí moje firma dokumentovat a evidovat?

Má-li vaše organizace více než 250 zaměstnanců, musíte vést doplňkovou interní evidenci o Vámi prováděném zpracování. Má-li vaše organizace méně než 250 zaměstnanců, jste povinni vést evidenci o činnostech spojených s vyšším rizikem zpracování, jako je:

- zpracování osobních údajů, které může vést k ohrožení práv a svobod jednotlivce nebo
- zpracování zvláštních kategorií údajů nebo údajů o trestných činech a odsouzení za trestné činy.

Dále musíte vést interní evidenci o zpracování údajů včetně následujících informací, které jsou detailně upraveny v článku 13 GDPR:

- název a údaje o vaší organizaci (případně jiných správců, vašeho zástupce a pověřence pro ochranu osobních údajů);
- účely zpracování a právní základ;
- v příslušných případech oprávněné zájmy správce nebo třetí strany, na jejichž základě probíhá zpracování údajů (v případech podle čl. 6 odst. 1 písm. b) GDPR);
- popis kategorií fyzických osob a kategorií osobních údajů;
- kategorie příjemců osobních údajů;
- informace o předávání do třetích zemí včetně dokumentace o zavedených bezpečnostních opatřeních mechanismu předávání;
- harmonogramy uchovávání (není-li možné je přesně určit, je třeba uvést kritéria pro stanovení doby uchovávání);
- popis technických a organizačních bezpečnostních opatření.

Obavy z toho, že vás spletitosti GDPR hodně zdrží, mohou být reálné – je tedy důležité pamatovat na to, že GDPR spojuje informace s majetkovými právy, a organizace se proto musí rozhodnout, kde budou uloženy a zpracovávány jednotlivé typy údajů včetně různých kategorií osobně identifikovatelných informací (PII). Vedení evidence či „mapy“, která uvádí místo uložení každého typu údajů a parametry pro nakládání s nimi, je jednak vaší povinností a jednak vám pomůže snižovat riziko porušení zabezpečení údajů. Obecně by mělo platit, že údaje by měly být pouze tam, kde to předepisují firemní pravidla.

Máte-li jasná a efektivní pravidla a postupy, máte také část toho, co potřebujete pro zajištění souladu s předpisy a prokázání regulačním orgánům, že splňujete požadované normy. Školení napříč vaší právnickou firmou pomůže zajistit plnění předpisů i do budoucna. Nicméně je třeba, aby používané postupy byly podpořeny neustálým monitorováním, přičemž toto přezkoumání Vašich procesů zpracování údajů musí být prováděno pravidelně ve formě auditů dopadů.

Důsledky:

- Vzhledem k tomu, že si od vás tuto evidenci může pro účely šetření vyžádat příslušný orgán dozoru, je nezbytné, abyste měli po ruce následující informace:
  - směrnici o bezpečnosti IT, zajišťování souladu s předpisy a ochraně údajů;
  - příručku a odpovědnosti v oblasti ochrany údajů;
  - prohlášení všech zaměstnanců pověřených zpracováním osobních údajů o ochraně údajů;
  - přehledy zpracování pro všechny příslušné automatizované procesy (elektronické zpracování dat – EDP);
  - trvale doložená prohlášení o souhlasu se shromažďováním osobních údajů.
- Informujte o požadavcích GDPR všechny zaměstnance a obzvláště oddělení odpovědná za zpracování elektronických údajů.
- Posilujte roli pověřence pro ochranu osobních údajů uvnitř společnosti.

4. Znát své povinnosti v případě porušení zabezpečení údajů

Co musí moje firma udělat v případě úniku klientových údajů nebo neoprávněného přístupu k nim?

Porušení zabezpečení údajů je podle GDPR definováno jako zničení, ztráta nebo změna osobních údajů nebo neoprávněné poskytnutí (nebo zpřístupnění) osobních údajů v důsledku porušení zabezpečení. Povinnosti týkající se ohlášení a oznámení případů porušení zabezpečení údajů, ke kterým již došlo, jsou upraveny v článcích 33 a 34 GDPR.

Došlo-li k porušení zabezpečení osobních údajů, správce je povinen jej ohlásit příslušnému orgánu dozoru „bez zbytečného odkladu" (tj. nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděl). Povinnost ohlásit takový případ však nevzniká, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Analýza a posouzení, zda v daném konkrétním případě vznikla povinnost ohlásit porušení, nebudou vždy tak snadné.

Ohlášení příslušnému orgánu dozoru by mělo obsahovat přinejmenším následující:

- popis povahy daného případu porušení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
- popis opatření, která správce přijal nebo navrhl s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

V případě nutnosti může správce poskytnout právoplatně požadované informace postupně, není-li možné všechny tyto informace poskytnout do 72 hodin.

Správce je také povinen vést kompletní dokumentaci podle čl. 30 odst. 5 GDPR.

Porušení zabezpečení osobních údajů musí správce oznámit subjektu údajů stejným způsobem, bez zbytečného odkladu a za použití "jasných a jednoduchých jazykových prostředků", jak je uvedeno v článku 34 GDPR.

Důsledky:

- Hlavní příčinou porušení zabezpečení údajů často bývá interní lidská chyba. Zajistěte, aby všichni zaměstnanci používali bezpečné postupy sdílení souborů (věnujte pozornost případům vynášení souborů z kanceláře, ztráty údajů na laptopech, soukromých mobilních zařízeních (BYOD) a jiných mobilních zařízeních) a dokázali rozpoznat podezřelé e-maily za účelem snížení rizika porušení zabezpečení údajů, kterému je možné předejít.
- Přezkoumávejte zabezpečení vaší firmy před kybernetickými útoky a její schopnost obstát při technologických poruchách (zálohování a obnova).
- Zajistěte, abyste měli jasný protokol, který vám umožní rychle reagovat na jakékoli porušení, ohlásit jej orgánům a oznámit příslušným subjektům údajů do požadovaných 72 hodin.
- Zaveďte evidenční systém pro dohledání předchozích případů porušení zabezpečení údajů pro případ, že by orgán dozoru chtěl provést nezávislé posouzení.
- Je-li to možné, zaveďte technická a organizační bezpečnostní opatření, která učiní osobní údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (například šifrování). Šifrování údajů je vaší poslední obranou v případě, že údaje padnou do rukou hackerů.

5. Vědět, jak mohou pomoci právnické technologie

Jak může můj systém pro řízení praxe pomoci mé firmě plnit naše povinnosti?

Ochrana strategických údajů a Legal Tech jdou ruku v ruce. Volba softwaru pro řízení praxe nebyla nikdy jednoduchá, obzvláště pokud je jedním z faktorů zajištění shody s předpisy. V souvislosti s GDPR musí právnické firmy ověřit:

- *Kde se údaje fyzicky nacházejí. Pokud jsou uloženy na lokálním serveru, je váš dodavatel schopen zabránit rozsáhlému porušení zabezpečení údajů? Jsou-li uloženy v cloudu, dokáže zpracovatel zaručit zabezpečení na úrovni bankovního standardu a obnovu v případě havárie?*
- *Jaká bezpečnostní opatření jsou zavedena za účelem ochrany údajů před neoprávněným přístupem nebo ztrátou.*
- *Jak dlouho vaše firma uchovává soubory a údaje.*
- *Jaké třetí strany mají přístup k údajům a nakolik bezpečně je sdílejí (tj. prostřednictvím zabezpečeného portálu nebo elektronické pošty).*
- *Zda zaměstnanci používají svá vlastní zařízení a pokud ano, zda mají bezpečný přístup k souborům mimo kancelář.*
- *Jak často jsou údaje zálohovány a jak dlouho trvá obnova údajů v případě kybernetického útoku.*

Níže naleznete některé z výhod a potenciálních možností využití těchto specializovaných technologií:

- Centrální uložení údajů a jednodušší, rychlejší a spolehlivější analýza údajů v reálném čase.
- Přístup ke všem údajům o případech a klientech, a to kdykoli, stejně jako komunikace.
- Archivace důležitých právních dokumentů, jako jsou dohody o mlčenlivosti (NDA), dohody s třetími stranami o zpracování údajů a/nebo prohlášení o souhlasu.
- Grafický přehled úkolů a automatická e-mailová upozornění sloužící pro kontrolu nad plněním povinností, pravidla pro uchovávání/likvidaci údajů.
- Bezproblémová a spolehlivá dokumentace procesů a odpovědností v oblasti elektronického zpracování dat.
- Chráněné prostory pro sdílení údajů (tzv. data room), určené pro citlivé údaje a projekty.
- Flexibilní správa přístupu za účelem minimalizace počtu osob, které mají oprávnění k přístupu k citlivým údajům.
- Ukládání smluvních dokumentů, které byly zkontrolovány podle zákonů na ochranu údajů.
- Automatizovaná tvorba smluv včetně příslušných příloh pro účely zákonů na ochranu údajů (např. pro získání souhlasu se zpracováním údajů).

V případě, že nepoužíváte vhodnou technologii pro splnění zvýšených požadavků na ochranu údajů a bezpečnost, které přináší GDPR, pak je pravý čas se nad ní nejen zamyslet, ale také **ji co nejrychleji zavést.** Nejenže můžete pracovat na tom, abyste **předešli riziku vysokých pokut a odpovědností,** ale se správnou technologií navíc **můžete pracovat efektivněji** a **bezpečněji.** Ba co víc, budete moci **přenést přinejmenším některá rizika** spojená s odpovědností v oblasti zabezpečení a ochrany údajů **na externí poskytovatele služeb.**

Wolters Kluwer

Kleos

Wolters Kluwer ČR, a.s., U nákladového nádraží 10, 130 00 Praha 3
tel: 246 040 400, kleos@wolterskluwer.cz, **www.kleos.cz**

3/2018