GDPR

25. květen 2018

GENERAL DATA PROTECTION REGULATION

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Účinnost normy je od 25. května 2018!

VZTAHUJE SE NA VŠECHNY PRÁVNICKÉ OSOBY, KTERÉ ZPRACOVÁVAJÍ NEBO SPRAVUJÍ CITLIVÁ DATA FYZICKÝCH OSOB, FYZICKÝCH OSOB PODNIKAJÍCÍCH (IČO), NEZLETILÝCH

České firmy a instituce stále tápou, v jakém rozsahu se jich *Obecné nařízení o ochraně osobních údajů* dotkne. Často nevědí, zda vůbec a co případně začít dělat, aby svou organizaci dovedly do stavu souladu s GDPR principy. Je obtížné zorientovat se v dost nepřehledné situaci, kdy ani sami zpracovatelé osobních údajů nevědí, kde je mají uloženy, proč je vlastně mají a k čemu je potřebují. Názor řady organizací, že se jich GDPR vůbec netýká, protože nezpracovávají žádné osobní údaje, není žádnou výjimkou. Bohužel však zapomínají na své **zaměstnance**, **zákazníky**, **obchodní partnery, externí spolupracovníky, dodavatele, odběratele** atd., kteří jsou zdrojem celé řady údajů, jež je zapotřebí adekvátně chránit a zpracovávat podle zákona.

Je úplně jedno, jestli jste malou organizací o několika zaměstnancích, nebo velkým nadnárodním korporátem. Čas, kdy GDPR vstoupí v platnost, **25. května 2018**, se totiž nezadržitelně blíží. Nařízení bude mít za následek změny v procesech řízení rizik, lidských zdrojů. Projeví se v úpravě pracovněprávních a dodavatelských smluv, v aktualizaci interních směrnic a veškeré dokumentace navázané na zpracování osobních údajů. Zásadním způsobem se dotkne i informačních technologií, u kterých budou *společnosti* a státní instituce povinny projít revizí datové architektury, aktualizací a případným upgradem systémů a bezpečnostních opatření ve všech vrstvách ICT infrastruktury.

Co s tím?

1. Zmapování současného stavu

Prvním krokem příprav by mělo být zmapování toho, jaké osobní údaje zpracováváte, kudy k vám přicházejí a jestli se po zpracování, když už nejsou potřeba, také smažou.

Nejde přitom jen o údaje zákazníků nebo zaměstnanců nebo třeba uživatelů webových stránek. V internetovém světě bude osobním údajem třeba také **IP adresa**, a za určitých podmínek jím mohou být i **cookies** soubory, které webové stránky používají k rozlišování uživatelů. Různé osobní údaje budou vyžadovat rozdílnou úroveň ochrany. Je důležité upřednostnit řešení a ochranu hlavně citlivých osobních údajů, kterými jsou například údaje o **finanční situaci, o zdravotním stavu.**

2. Analýza zpracování osobních údajů

Tato fáze si klade za cíl shromáždit veškeré důkazy k zákonnému zpracování osobních údajů a poté provést jejich podrobný rozbor. GDPR je v této fázi příležitostí k revizi právních důvodů zpracování dat. Pokud analýzou dojdete k závěru, že pracovat s osobními údaji bez **souhlasu** nepůjde, budete muset posoudit, zda stávající žádosti o souhlas splňují všechny náležitosti podle nařízení. Zdali jsou srozumitelné a jednoznačné, protože GDPR již nebude tolerovat souhlasy „schované“ v hloubi všeobecných podmínek, jejichž podpisem předává osoba téměř neomezené právo s nakládáním jejích osobních údajů. Tato část analýzy je jakýmsi právním auditem, v jehož **rámci** provedete inventuru stávajících právních dokumentů, kterými jsou interní **směrnice**, smlouvy s dodavateli či zákazníky, v nichž se vyskytují osobní údaje.

Jak už bylo několikrát řečeno, osobní údaje se mohou vyskytovat nejenom v dokumentech, a to jak v písemných, tak i v elektronické podobě, ale jsou součástí informačních systémů a různých procesních nástrojů. V rámci organizace může jít o data z externích zdrojů, která bývají často velmi opomíjena. Z tohoto důvodu se řada organizací nevyhne tzv. datovému a bezpečnostnímu auditu, který by měl zmapovat výskyt osobních údajů napříč datovou infrastrukturou, různorodými úložišti a databázemi společnosti. Revize informačních technologií a úrovně jejich zabezpečení je naprostou samozřejmostí, na kterou nesmíte v této části analýzy zapomenout.

Výsledkem této fáze by mělo být shrnutí v podobě zprávy, která zhodnotí zjištěné výstupy a vyhodnotí rizika spojená se zpracováním osobních údajů. V **praxi** to může znamenat následnou úpravu firemní dokumentace, vnitřních směrnic, smluv s dodavateli a mnohdy budou nutné úpravy IT systémů.

GDPR

25. květen 2018

GENERAL DATA PROTECTION REGULATION

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Účinnost normy je od 25. května 2018!

A co bude potom?

3. Projektová část

Vyústěním předchozí analytické fáze je důkladná příprava projektu včetně časového harmonogramu, podle kterého byste měli postupovat, abyste stihli uvést svou organizaci do souladu s pravidly GDPR včas. Prošli jste si náročnou, ale velmi důležitou fází analýzy, která vás jednoznačně navedla k tomu, co musíte změnit nebo nově zavést. Bude toho s ohledem na GDPR hodně, z dosaženého výsledku však budete profitovat. Nejenže mnohem lépe zabezpečíte data všech osob, ale zároveň tím implicitně lépe ochráníte také svou organizaci před vnitřními i vnějšími útoky. Smyslem této fáze není zničit nebo nahradit vše, do čeho jste léta **investovali** a co jste složitě zaváděli, ale projdete si vnitřní inventurou, která jen odhalí, zdali je to z pohledu GDPR dostatečné. Sami můžete být překvapeni, kolik zbytečných a po dlouhé roky nevyužitých dat a informačních systémů máte k dispozici.

Sankce za porušení GDPR?

Pracovní skupina WP29 (Working Party 29) představila dlouho očekávané vodítko ke stanovování pokut. Když se proviníte, budou orgány kontrolující dodržování GDPR (v České republice je to Úřad pro ochranu osobních údajů) posuzovat především „povahu, závažnost a dobu trvání protiprávního jednání“. Z toho vyplývá, že v některých případech by nemusely hned padat pokuty, ale úřad by vás mohl jen „pokárat“ nebo „napomenout“. Formu upozornění zvolí úřady v situacích, kdy zpracovatelé neohrozí práva dotčených občanů. K pokárání se úřady uchýlí také v případech, kdy by pokuta „nepřiměřeně zatěžovala“ fyzickou osobu.

Teď jsou známá tato kritéria, kterými se budou úřady řídit.

- Počet osob, kterých se porušení GDPR dotklo. Platí, že čím více lidí zpracovatel ohrozí svým jednáním, tím vyšší bude pokuta. Více zaplatí také organizace, které budou nařízení porušovat opakovaně.
- Účel zpracování osobních údajů. Úřady budou zkoumat, jak se organizace ke zpracování osobních údajů postavila z hlediska specifikace účelu i kompatibilního použití.
- Škody, které subjekty utrpěly. Ačkoliv úřady nemají pravomoci přiznávat **odškodnění** občanům, jejichž údaje byly zpracovávány, měly by zohlednit škodu, kterou lidé utrpěli.
- Doba trvání protiprávního jednání. Nejde ani tak o samotný čas, ale také o prokázání úmyslu, podcenění vhodných preventivních opatření nebo o neschopnost provést technická zabezpečení.

O finální částce rozhodnou i další ukazatele. Přitěžující okolností bude nedbalost nebo úmyslné porušení nařízení. Příkladem je situace, kdy společnost bude navenek působit tak, že přijala opatření vedoucí k ochraně osobních údajů, ale skutečnost bude opačná. Jako nedbalost bude chápána situace, kdy společnost nezvládne držet krok s nejnovějšími bezpečnostními postupy nebo nedokáže dodržovat zásady, jež sama zavedla. Za porušení GDPR pravidel bude vždy zodpovědná samotná organizace, resp. její statutární orgán.

Vodítko neprozrazuje konkrétní výši pokut pro jednotlivá provinění, přesto alespoň trochu napovídá:

- Maximální výše pokuty může být 20 milionů eur, respektive 4 % z celkového ročního obratu firmy.

O velikosti firmy pokutování rozhodně nebude. Platí princip přiměřenosti. Přesto se pokutám nevyhnou ani menší společnosti jen s několika málo zaměstnanci, ale určitě v jiných číselných řádech.

Zaplacením pokuty však celá nepříjemnost nemusí skončit. Správci a zpracovatelé osobních údajů totiž mohou čelit žalobám podaným samotnými fyzickými osobami, které mohou žádat o náhradu škody.

Diestra®

Diestra consulting CZ, s.r.o.
email: gdpr@diestra.cz
telefon: +420 724 21 4377

Diestra je vaším spolehlivým **partnerem** pro dosažení souladu s nařízením **GDPR**