PRÁVNÍ PROSTOR

CODEXIS publishing

Elektronický časopis vydává CODEXIS publishing spol. s r.o.
ve spolupráci s právním portálem Právní prostor.cz

II. ROČNÍK 13 21. ČERVNA 2017

HLAVNÍ TÉMA

ÚVODNÍ SLOVO: GDPR

Když Evropský parlament schválil v říjnu roku 1995 směrnici o ochraně osobních údajů (95/46/ES), jednalo se o vůbec první evropský dokument, který se komplexně ochranou osobních údajů zabýval. Za posledních 22 let se mnoho změnilo. Internet byl v té době ještě v kolébce, neexistoval Google ani sociální sítě a umělá inteligence byla doménou sci-fi nežli realitou, která by vyžadovala právní regulaci.

Ačkoliv se soudy i dozorové orgány (u nás Úřad pro ochranu osobních údajů) napříč celou Evropou snažily zastaralost směrnice zhojit, ne vždy se jim to dařilo a i hranice, kam ještě lze směrnici ohýbat, nejsou nekonečné. Do dynamicky se proměňujícího prostředí zpracování (velkých) dat – a zejména těch osobních – navíc v roce 2010 vstoupil evropský ústavodárce, který v rámci Lisabonské úmluvy zařadil Listinu základních práv Evropské unie mezi základní (tzv. primární) právní předpisy EU, čímž se právo na ochranu osobních údajů stalo základním lidským právem každého občana EU, kterého se tak nikdo z nás nemůže vzdát a vůči kterému je potřeba poměřovat každé jiné právo. Evropská úprava se tak posunula od obecné ochrany soukromí k výslovné ochraně osobních údajů jakožto základního lidského práva každého jedince.

V ten moment bylo zřejmé, že stávající právní rámec je nadále neudržitelný a že je potřeba přinést novou, moderní úpravu, která zajistí dostatečnou úroveň ochrany osobních údajů, ale která bude rovněž reagovat na dramaticky se vyvíjející technologický sektor a různorodé potřeby nakládání s osobními údaji, včetně jejich uchovávání.

Tímto novým předpisem se stalo obecné nařízení o ochraně osobních údajů (2016/679/EU), pro který se za poslední rok vžilo, a to i v českém prostředí, zkrácené označení GPDR pocházející z anglického názvu *General Data Protection Regulation*.

Co vše nám GDPR přináší a jaké jsou vlastně povinnosti správců a zpracovatelů při zpracování osobních údajů? A co vůbec lze považovat za osobní údaje? Jaké sankce hrozí podnikům, pokud se nebudou novými pravidly řídit? V tomto předprázdninovém speciálu bychom vám rádi nabídli alespoň stručný vhled do problematiky zpracování osobních údajů a změn, které nás čekají v květnu 2018, kdy se GDPR stane závazné.

Lenka Suchánková |
partnerka advokátní kanceláře Pierstone

Připraveno ve spolupráci s
PIERSTONE

Na právním portálu Právní prostor.cz naleznete v nejbližších 14 dnech i tato témata:

Otcovská dovolená

Vybrané aktuality z oblasti civilněprávní a profesní legislativy

Práce z domova – výhody a nevýhody, plánované změny

Naléhavost změn právní úpravy postavení církevních škol

WWW.PRAVNIPROSTOR.CZ

STRUČNĚ

CO JE GDPR A CO ZNAMENÁ?

- Představuje nový standard kybernetické bezpečnosti občanů Evropské unie a tomu odpovídající povinnosti veškerých osob, které s jejich osobními údaji nakládají.
- **GDPR** = *General Data Protection Regulation* = Obecné nařízení na ochranu osobních údajů
- **Evropské nařízení** – tedy evropský předpis, který je přímo aplikovatelný na každého – veškeré fyzické i právnické osoby – bez toho, aniž by vyžadoval jakoukoliv implementaci do národních právních řádů
- **Celosvětový dopad** – jakmile osoba nakládá s osobními údaji občanů EU a/nebo pokud sídlí v EU, bude vždy podléhat GDPR
- **25. května 2018** – datum, odkdy se GDPR stává pro všechny závazné
- **20 milionů EUR nebo až 4 % z celosvětového obratu skupiny** – sankce, které je možné udělit za porušení povinností vyplývajících z GDPR
- **Vztahuje se i na zpracovatele** – GDPR ukládá povinnosti každé osobě, která se na zpracování osobních údajů podílí – tedy správcům i zpracovatelům – a umožňuje každou takovou osobu v případě porušení těchto povinností sankcionovat

ZÁKLADNÍ POJMY

GDPR pracuje se základními pojmy, které naleznete definované v čl. 4 GDPR. Tyto pojmy je nezbytné vnímat v kontextu dosavadní judikatury i výkladové praxe dozorových orgánů a neomezovat se tedy jen na zákonný text. Základní přehled těchto pojmů vám nabízíme níže:

- **Osobní údaj** – každá informace, která může sloužit k identifikaci fyzické osoby = subjektu údajů
  - **Zřejmé:** jméno, číslo dokladu totožnosti, kreditní karta, kontaktní údaje, údaje o zdraví, lokalizační údaje, IP adresy (dynamické i statické), fotografie aj.
  - **Ale také:** jakákoliv informace o nákupech, užívaných službách či vlastněných a užívaných zařízeních, (meta)data týkající se předchozího užívání služby aj.
  - **Co tedy není osobním údajem?** Anonymní nebo anonymizované informace, tedy informace, které neidentifikují nebo na základě kterých nelze identifikovat – ani při vynaložení přiměřeného úsilí – žádnou fyzickou osobu. Rovněž informace o právnických osobách nejsou osobními údaji.
- **Subjekt údajů** – jakákoliv fyzická osoba, jejíž osobní údaje se zpracovávají.
  - *Např. zákazníci, zaměstnanci, návštěvníci internetové stránky, uživatelé služby aj.*
- **Zpracování osobních údajů** – jakákoliv činnost související s nakládáním s osobními údaji, včetně jejich získávání, ukládání, strukturování, použití, vyhledávání, šíření, zpřístupnění, výmazu nebo zničení… A to vše bez ohledu na to, zda se jedná o elektronickou nebo papírovou formu.
- **Účel zpracování** – obchodní nebo jiný důvod, proč ke zpracování osobních údajů dochází.
- **Správce** – jakýkoliv subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.
  - *Např. zaměstnavatel je správcem údajů při zpracování zaměstnaneckých údajů, eshop je správcem zákaznických údajů, uživatel cloudu je správcem svých údajů.*
- **Zpracovatel** – subjekt, který zpracovává osobní údaje z pověření a na základě pokynů správce (tj. sám neurčuje ani účel ani prostředky zpracování).
  - *Např. se může jednat o mzdové agentury, které pro zaměstnavatele zpracovávají zaměstnanecké údaje, poskytovatele cloudových služeb, marketingové agentury, které zpracovávají údaje pro své zákazníky aj.*

10 HLAVNÍCH NOVINEK GDPR

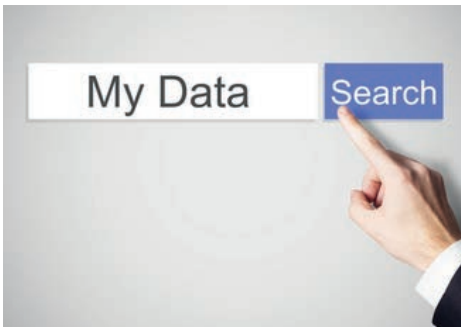
GDPR je spíše evolučním než revolučním předpisem. Přesto přináší anebo nově klade mnohem větší důraz na několik oblastí. Těmi jsou zejména:

1. **Jednoznačný souhlas k jakémukoli zpracování údajů** – Kromě několika dalších důvodů, které GDPR nabízí (plnění smlouvy, plnění zákonné povinnosti, oprávněný zájem správce, veřejný zájem aj.), musí být zpracování osobních údajů vždy založeno na jednoznačném, konkrétním a informovaném souhlasu subjektu.
2. **Odvolání souhlasu a právo být zapomenut** – Subjekt údajů má kdykoli během zpracování svých údajů právo odvolat dříve udělený souhlas se zpracováním; správce pak musí ukončit zpracování takových údajů.
3. **Nové požadavky na smlouvu o zpracování (včetně řetězení)** – Smlouva mezi správcem a zpracovatelem musí být písemná (včetně elektronické formy) a obsahovat některé specifické povinnosti, vč. povinnosti auditů, bezpečnostních opatření aj.
4. **Požadavky na bezpečnostní opatření** – GDPR zdůrazňuje pro zachování ochrany implementaci bezpečnostních opatření. GDPR vychází z principu technologické neutrality, avšak zmiňuje např. pseudonymizaci jako jeden z prvků pro zajištění bezpečnosti údajů.

5. **Přenositelnost údajů** – Správci osobních údajů jsou povinni zajistit na žádost subjektu údajů možnost přenosu jeho údajů k jinému správci (v kompatibilním formátu).
6. **Dokumentace zpracovatelských činností** – Zatímco se podle stávající právní úpravy museli správci registrovat u Úřadu, tato povinnost jim spolu s GDPR odpadá. Ohlašovací povinnost však nahrazuje povinnost dokumentovat – správci tak budou muset mít veškeré své činnosti řádně zdokumentovány a popsány. V určitých případech rovněž vzniká povinnost vyhotovit tzv. posouzení vlivu na ochranu osobních údajů, tj. posouzení zpracovatelských činností a existujících rizik pro subjekty údajů.
7. **Notifikace neoprávněného přístupu k osobním údajům** – V případě neoprávněného přístupu k osobním údajům jsou správci i zpracovatelé povinni notifikovat zodpovědné orgány (především Úřad na ochranu osobních údajů) a v některých případech i samotné subjekty údajů.
8. **Pověřenec pro ochranu osobních údajů** – Správce i zpracovatel osobních údajů jsou nyní v určitých případech povinni jmenovat nezávislého pověřence, pokud zpracování osobních údajů tvoří důležitý pilíř jejich podnikání.
9. **Hlavní dozorový orgán jako jedno správní místo** – Subjekty zpracovávající osobní údaje v různých členských státech nemusí komunikovat se všemi národními dozorovými orgány (one-stop-shop).
10. **Vyšší pokuty** – až 4 % celosvětového obratu – Správci i zpracovatelé mohou za porušení svých povinností čelit pokutám ve výši až 4 % celosvětového obratu své skupiny či 20 mil. EUR.

PRÁVA SUBJEKTŮ ÚDAJŮ

GDPR jako celek slouží k ochraně fyzických osob a rozvíjí tak jejich základní lidské právo na ochranu osobních údajů a ochranu soukromí. GDPR pro účinnou ochranu osobních údajů poskytuje subjektům údajů několik práv, které jim umožňují pečlivě sledovat, kdo a jak s jejich osobními údaji nakládá.



- **Právo být informován o zpracování osobních údajů**

  Každá osoba má právo být řádně informována nejen o tom, kdo a jak s jejími osobními údaji nakládá, ale i proč tak činí nebo komu všemu tyto údaje zpřístupňuje.
- **Právo na přístup k osobním údajům**

  Každý subjekt údajů si může vyžádat potvrzení o tom, zda dochází ke zpracování jeho osobních údajů a má rovněž právo si tyto údaje vyžádat. Správce je povinen toto potvrzení vydat a případně rovněž poskytnout kopii veškerých zpracovávaných údajů.
- **Právo na opravu**

  Zpracování nepřesných informací může být problematické a může fyzickým osobám způsobit značnou újmu – např. pokud by docházelo ke zpracování lživých informací, které by pak byly s takovou osobou spojovány. Proto má každá osoba právo požadovat opravu nepřesných nebo doplnění neúplných údajů, které se jí týkají.
- **Právo být zapomenut (právo na výmaz)**

  Právo být zapomenut umožňuje každému, aby se domáhal výmazu svých osobních údajů. Pokud neexistují důvody, které by správci umožňovaly ve zpracování těchto údajů pokračovat, je povinen veškeré osobní údaje o takové osobě vymazat. Největší význam má toto právo zejména v případě, kdy ke zpracování osobních údajů dochází na základě uděleného souhlasu a subjekt údajů tento souhlas odvolá.
- **Právo na omezení zpracování**

  V určitých případech mají subjekty právo požadovat, aby zpracování jejich osobních údajů bylo omezeno na nezbytné minimum, např. aby osobní údaje žádající osoby byly u správce pouze uloženy. Dokud neodpadnou legitimní důvody, nesmí správce s těmito údaji jakkoli nakládat.
- **Právo na přenositelnost údajů**

  Právo na přenositelnost údajů je jednou z novinek GDPR, která umožňuje, aby si subjekt údajů mohl, v určitých případech, vyžádat veškeré své osobní údaje, které správci poskytl – ať již přímo nebo svou činností (např. surfováním po internetu). Správce údajů je v takovém případě povinen žádající osobě tyto údaje předat, případně je rovnou předat jinému správci, a to ve strukturovaném, běžně používaném a strojově čitelném formátu.
- **Právo vznést námitku**

  Pro zajištění kontroly nad vlastními osobními údaji, má každá osoba rovněž právo namítat určitý způsob zpracování jejích osobních údajů. Vzhledem k tomu, že toto právo lze využít pouze v případech, kdy ke zpracování dochází na základě zákonných povinností správce či na základě jeho tzv. oprávněného zájmu, účinně doplňuje právo být zapomenut. Námitku lze rovněž podat proti jakémukoliv přímému marketingu (tedy např. proti telefonátům, emailům, či SMS zprávám s marketingovými nabídkami).

CO JE POTŘEBA PODNIKNOUT?

- **Analýza stávajícího stavu**
  - Identifikace osobních údajů, se kterými společnost nakládá
  - Zmapování datových toků a procesů nakládání s osobními údaji
  - Identifikace postavení společnosti (správce × zpracovatel) ve vztahu k zpracovávaným osobním údajům
  - Zmapování životního cyklu údajů
- **Rozdílová analýza**
  - Porovnání stávajícího stavu s požadavky GDPR
  - Analýza nedostatků a dopadů z pohledu GDPR
  - Rozpad do celé společnosti – právní, obchodní i technický pohled, včetně celkové IT infrastruktury
- **Implementace**
  - Implementace zjištěných nedostatků a dosažení souladu s GDPR

CODEXIS® GOLF TOUR 2017
7. – 8. 8. 2017 NOVAVOICE CUP, Panorama Golf Resort – Kácov www.codexisgolf.cz
CODEXIS®

IMPLEMENTACE GDPR (PŘEHLED/ČASOVÁ OSA)

Aktivita/časový rozsah v měsících	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Definice rozsahu posuzování	→													
Analýza stávajícího stavu zpracování osobních údajů		→	→	→										
Příprava projektových záměrů a harmonogramu implementace					→	→								
Realizace projektových záměrů						→	→	→	→	→	→	→		
Posouzení vlivu na ochranu osobních údajů												→	→	
minimální časový rozsah implementace		→	→											

HLAVNÍ TÉMA

ZÁVĚREČNÉ SLOVO

Jana Pattynová |
partnerka advokátní kanceláře Pierstone

GDPR je dosud nejkomplexnějším souborem pravidel na ochranu osobních údajů na světě. Evropská unie se tak díky své dlouhodobé snaze na tomto poli stává atraktivním datovým trezorem, který nabízí nejen stabilní politické prostředí, fyzickou bezpečnost, ale i robustní právní rámec. To vše může být důležitým argumentem pro využívání Evropy jako bezpečného datového úložiště.

GDPR, spolu se směrnicí o kybernetické bezpečnosti NIS zároveň významně přispěje ke kybernetické bezpečnosti celého online (a tím spíš i offline) prostředí. Dnes na trhu vidíme, jak velké množství organizací díky GDPR staví nakládání s daty a jejich zabezpečení na důležité místo ve své strategii. Takový přístup pak příznivě působí na zvýšení kybernetické bezpečnosti i ochrany práv spotřebitelů.

Stávající vývoj ukazuje, že veškerý technologický vývoj, vytváření *smart cities* i fenomén umělé inteligence se neobejdou bez masivních datových toků a jejich zpracování. Ačkoliv je GDPR v některých oblastech poměrně rigidním předpisem, věřím, že pomůže ke zvýšení kybernetické bezpečnosti i k posílení práv každého jedince i povědomí o nich.

ČLÁNEK

PRVNÍ VÝKLADOVÁ PRAVIDLA K GDPR

Pracovní skupina Evropské komise – Working Party 29 („WP29“) vydala v pátek 16. prosince 2016 první z řady slíbených dokumentů, které mají poskytnout výklad k obecnému nařízení o ochraně osobních údajů („GDPR“).

číst více na www.pravniprostor.cz

MEZINÁRODNÍ PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ Z POHLEDU NOVÉ REGULACE

Předávání osobních údajů v rámci celé problematiky ochrany osobních údajů představuje jedno z nejzásadnějších a v současnosti i nejdiskutovanějších témat. Dnešní globalizovaná společnost by bez mezinárodních přenosů údajů nemohla vůbec existovat, a proto si tento institut zaslouží zvláštní pozornost.

číst více na www.pravniprostor.cz

Tento elektronický časopis byl připraven ve spolupráci s advokátní kanceláří Pierstone. Díky zastoupení v Londýně, Bruselu a Moskvě Pierstone nabízí jeden z největších specializovaných právních týmů zaměřených na právo technologií, médií a komunikací. Pierstone se dlouhodobě zabývá ochranou osobních údajů, IT sektorem, IoT, právem nových technologií či podporou start-upového sektoru.

Na přípravě elektronického časopisu se podíleli

- Lenka Suchánková, advokátka a partnerka advokátní kanceláře Pierstone
- Jana Pattynová, advokátka a partnerka advokátní kanceláře Pierstone
- Iva Zothová, advokátka a partnerka advokátní kanceláře Pierstone
- Dominik Vítek, advokátní koncipient v advokátní kanceláři Pierstone

Pro více informací kontaktuje Pierstone. Aktuální informace o GDPR můžete rovněž sledovat na Pierstone LinkedIn profilu.

PRÁVNÍ PROSTOR – elektronický časopis nakladatelství CODEXIS publishing spol. s r.o., a redakce právního portálu Právní prostor.cz, jehož provozovatelem je společnost ATLAS consulting spol. s r.o.; www.atlasconsulting.cz, klientske.centrum@atlasconsulting.cz, Výstavní 292/13, Ostrava-Moravská Ostrava, 702 00, tel.: 596 613 333. Vychází jednou za 14 dní. Kontakt na redakci: Ing. Václav Chládek, šéfredaktor, tel.: 603 826 782, chladek@pravniprostor.cz, Ing. Lubomír Brož, obchodní manažer, tel.: 731 422 841, broz@pravniprostor.cz.
© Všechna práva vyhrazena. Bez předchozího písemného souhlasu nakladatelství CODEXIS publishing spol. s r.o. je zakázána jakákoli další publikace, přetištění nebo distribuce (tištěnou i elektronickou formou) jakéhokoli materiálu nebo části materiálu zveřejněného v tomto elektronickém časopisu. Přihlášení nebo odhlášení elektronického časopisu na klientske.centrum@atlasconsulting.cz.