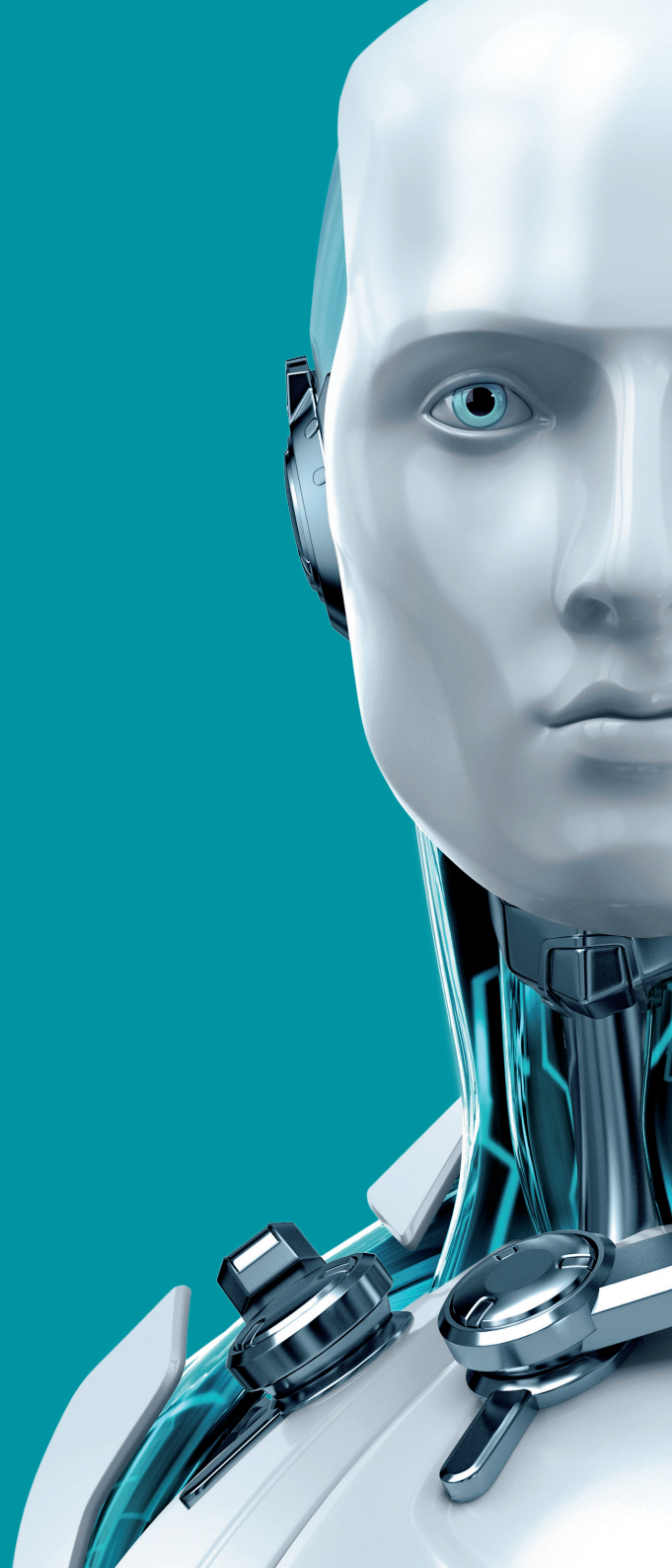
ENJOY SAFER TECHNOLOGY™

Význam šifrování v nařízení GDPR

BUSINESS



ENJOY SAFER TECHNOLOGY™

Krátký úvod do problematiky

25. května příštího roku vstoupí v platnost Obecné nařízení pro ochranu osobních údajů (z anglického General Data Protection Regulation, zkráceně GDPR). Jde o nařízení, které reaguje na překotný vývoj informačních technologií, který má za následek ne vždy právě zodpovědné či přímo neoprávněné zacházení s osobními daty a údaji občanů jednotlivých států Evropské unie. Nařízení navazuje na dosud platnou Směrnici Evropského parlamentu a Rady 95/45/ES, jejíž hlavním cílem bylo zajištění fungování jednotného trhu, a účinnou ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů. Jednotlivé státy postupně zapracovávaly směrnici do svých právních řádů a výsledkem byla jistá nejednotnost, která dělala problémy hlavně nadnárodním podnikatelským subjektům. Evropská unie představila prostřednictvím obecného nařízení o ochraně osobních údajů č. 2016/679 - "GDPR", výčet nových požadavků, pomocí nichž má být posílena práva subjektů údajů a sjednocena právní úprava v členských státech EU.

Osobní údaje

Citlivá osobní data jsou definována jako jakákoliv informace vedoucí k identifikaci konkrétní fyzické osoby, přímo či nepřímo, která má povahu identifikačního čísla nebo jednoho nebo více faktorů specifických pro určení fyzické, fyziologické, genetické, psychologické, mentální, ekonomické, kulturní nebo sociální identity. Za osobní údaje jsou považovány i **síťové identifikátory**, jež zanechávají stopy. Jde tedy například o e-mailové a IP adresy nebo soubory **cookie**. Zjednodušeně řečeno se nařízení GDPR dotkne značné části podnikatelských subjektů.

Zpracování osobních údajů

Je jakákoli operace nebo soubor operací s osobními údaji, které je prováděna s pomocí či bez pomoci automatizovaných procesů. Jde například o shromáždění, zaznamenání, uspořádání, strukturování, **uložení**, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, výmaz nebo zničení.

V praxi tak půjde o všechny firmy a podnikatele, kteří automaticky zpracovávají osobní údaje k profilování osobních aspektů zákazníka (pracovní výkon, ekonomická situace, zdravotní stav, osobní preference, zájmy, kde se nachází, jeho pohyb atd.).

Co nového právní úprava přináší?

První změnou je povinnost **ohlášení případů úniku dat** - Společnosti a organizace musí takové bezpečnostní incidenty nahlásit lokální autoritě ihned po objevení úniku. Nejpozději však do 72 hodin od chvíle objevení incidentu. Výjimkou je případ, kdy je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Ohlášení musí obsahovat poměrně detailní informace o daném úniku dat jako je popis incidentu, počet postižených subjektů, důsledky úniku a popis opatření, která byla přijata nebo navržena.

Pokud představuje konkrétní únik dat pro zákazníka velké nebezpečí, musí ho firma o úniku dat jednoduše a srozumitelně informovat. Pokud ale jsou uniklá data zabezpečena pomocí šifrování, tudíž se k nim útočník nemůže dostat, pak tato povinnost odpadá.

Zákazník může podat stížnost, pokud má za to, že byla jeho práva porušena v důsledku zpracování jeho osobních údajů v rozporu s GDPR. Kdokoli, kdo v důsledku porušení GDPR utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy. Správce nebo zpracovat se své povinnosti zprostí, prokáží-li, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Bezpečnost dat - Tato část GDPR nařízení je podobná současné právní úpravě. Firma musí zajistit, aby se s osobními daty zacházelo způsobem, který zajišťuje jejich bezpečnost, včetně ochrany před neautorizovaným nebo nezákonným procesem, pro případ ztráty, zničení a poškození. Nařízení doporučuje bezpečnostní opatření, které mohou firmy implementovat. Jde o **pseudonymizaci** a **šifrování** osobních dat. Pseudonymizací se rozumí zpracování osobních údajů tak, že již **nemohou být přiřazeny konkrétnímu subjektu** údajů **bez použití dodatečných informací**.

Značné **navýšení finančních postihů** – Společnosti, které nebudou v souladu s nařízením GDPR, mohou dostat pokutu až ve výši 4 procent jejích ročního globálního obratu nebo 20 milionů euro. Záleží na tom, která částka bude vyšší. Nejde však o pevně daný postih, protože každý případ se má posuzovat samostatně. Nicméně pokuta má být účinná, přiměřená a odrazující.

Právní nařízení platné **ve všech zemích Evropské unie** – V současnosti existuje 28 různých právních předpisů, pro každou zemi v podstatě unikátní. Podnikatelé a firmy tak po zavedení nařízení nebudou muset analyzovat zákony jednotlivých zemí. Sjednocením legislativy by se mělo ušetřit okolo 2.3 miliard euro ročně.

GDPR nařízení musí dodržet i společnosti, které **sídlí mimo EU**, pokud v rámci Evropské unie podnikají (včetně zboží a služeb zdarma) nebo monitorují chování zákazníků.

Záměrná a standardní ochrana dat (by design a by default) – Nové nařízení přináší řadu povinností pro zpracovatele dat, který musí být schopen doložit fakt, že nařízení GDPR dodržuje. Může jít například o vhodné technické opatření (šifrování dat) nebo organizační opatření (interní bezpečnostní politiky). Ve větších společnost to bude znamenat, že si buď najmou, nebo z interního zaměstnance musí udělat takzvaného **pověřence pro ochranu osobních údajů**, který bude za dodržování nařízení ve firmě zodpovědný. Zároveň bude hlavní kontaktní osobou pro dozorový úřad.

Nařízení definuje i postavení pověřence, který má být náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Má dostat zdroje nezbytné k plnění jeho úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí. Zároveň nedostává od správce či zpracovatele žádné pokyny týkající se výkonu svých úkolů, je na nich nezávislý. Pověřenec může plnit i jiné úkoly a povinnosti, ale jeho činnost nesmí **vést ke střetu zájmů** (např. to nesmí být IT administrátor).

Jaké jsou další změny?

Obecné nařízení o ochraně osobních údajů také obsahuje souhlas se zpracováním dat. V současnosti je to velmi podobné, souhlas musí být jednoznačný, svobodný, transparentní, snadno přístupný, jasně oddělen od ostatních smluvních ujednání a vyjádřen jednoduchým a jasným jazykem. U osob mladších 16 let mohou udělit souhlas pouze jejich zákonní zástupci. Zde je ale ponechána určitá volnost, jelikož jednotlivé státy si mohou věkovou hranici snížit.

Firmy musí být schopny doložit, že pro zpracování dat mají souhlas zákazníka. Nesmí souhlas podmiňovat podepsáním smlouvy, kde to není pro plnění dané smlouvy nutné. Zákazník má právo kdykoli svůj souhlas odvolat. Proces odvolání souhlasu musí být stejně snadný, jako jeho poskytnutí.

Právo na přenositelnost údajů – Zákazník má právo získat své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a následně je předat dalšímu správci dat v případě, že je zpracování založeno na souhlasu, provádí se automatizovaně, a kdy nedojde k dotčení práv a svobod jiných osob.

Právo na **zapomenutí nebo být zapomenut** je další věcí, které nové nařízení obsahuje. V reálu jde o situaci, kdy subjekty mohou požadovat bezodkladné vymazání osobních údajů za zákonem daných podmínek. Ten pamatuje i na výjimky. Firmy nemusí osobní údaje vymazat, pokud je potřebují např. pro obhajobu právních nároků nebo z důvodu veřejného zájmu v oblasti zdraví. A to nejen z interních systémů dané firmy. Pokud taková firma předává citlivé osobní údaje třetím stranám, tak musí zajistit výmaz dat i tam.

Kontaktní informace: