GDPR pod drobnohledem

Termín GDPR je zkratka názvu Obecní nařízení o ochraně osobních údajů fyzických osob (Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES). Jedná se o unijní předpis (nařízení EU) upravující ochranu osobních údajů fyzických osob.

TEXT: KATEŘINA LUKÁŠOVÁ

Podle Ing. Jitky Steinerové, pověřenkyně pro ochranu osobních údajů, náš dosavadní zákon 101/2000 Sb., o ochraně osobních údajů a nařízení nejsou nijak výrazně rozdílné. „Kdo dodržoval zákon 101/2000 Sb., nebude mít s nařízením problém," říká k tomu. Asi největší rozdíl je pak podle ní v sankcích, které nařízení za porušení ukládá. „Hlavním důvodem pro schválení GDPR byla potřeba sjednotit národní legislativy členských států EU tak, aby byly osobní údaje chráněny, případně předávány ve všech členských státech stejným způsobem," vysvětluje dále.

Jaroslav Benda, IT specialista na GDPR, definuje GDPR jako ochranu osobních údajů, která má za úkol ochraňovat osobní data fyzických osob uvnitř firem. „To znamená, že je potřeba získaná data řádně ochránit před jejich zneužitím nebo únikem z firmy. Je třeba zajistit, aby s těmito daty manipulovali a pracovali pouze ti zaměstnanci, kteří jsou oprávněni s těmito daty pracovat, a ostatním byla tato data znepřístupněna," vysvětluje. Dále je třeba informovanost osob, od kterých data nějakým způsobem získáváme, o takzvané transparentnosti, která má za úkol informovat subjekt o tom, jak je s daty dále nakládáno a hospodařeno.

„ÚOOÚ je dozorovým orgánem pro kontrolu dodržování zákona 101/2000 Sb., bude dozorovým orgánem pro kontrolu dodržování Nařízení a národní legislativy v oblasti ochrany osobních údajů (až Parlament ČR nějakou legislativu schválí...). Podrobné informace o činnosti ÚOOÚ lze nalézt na jejich webových stránkách," říká Jitka Steinerová.

Platnost a účinnost není z hlediska časové působnosti totéž

„U každého právního předpisu je z hlediska jeho časové působnosti třeba odlišovat termíny platnost a účinnost," vysvětluje Mgr. Tereza Lukášová, advokátní koncipientka advokátní kanceláře JUDr. Jiřího Lukáše z Ústí nad Orlicí. Toto nařízení Evropského parlamentu a Rady pochází ze dne 27. 4. 2016, od tohoto dne je tedy platnou součástí právního řádu EU. Jeho účinnost nastala dne 25. 5. 2018, což znamená, že od tohoto dne je nařízení přímo účinné pro občany členských států EU, zakládá tedy přímo práva a povinnosti.

Osobní informace vede k identifikaci fyzické osoby

Podle GDPR jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). „Zjednodušeně řečeno je tedy osobním údajem jakákoli informace, která může samostatně nebo ve spojení s další informací vést k identifikaci fyzické osoby," shrnuje Tereza Lukášová. „Mezi tyto údaje nejčastěji patří například jméno, příjmení, adresa, rodné číslo, datum narození, e-mail, telefon, SPZ automobilu, číslo bankovního účtu, zdravotní stav, rasa či etnický původ, členství v odborech, kamerový záznam a jiné...," doplňuje Jaroslav Benda a Jitka Steinerová dodává, že se sem řadí i citlivé osobní údaje o zdravotním stavu, politické či sexuální orientaci, biometrii apod.

GDPR poskytuje osobním údajům fyzických osob širokou ochranu

GDPR poskytuje značně širokou ochranu osobním údajům fyzických osob, nevztahuje se tedy na osoby právnické. „Zde je ovšem potřeba zdůraznit, že právnická osoba vždy jedná prostřednictvím osoby fyzické (jednatel, zaměstnanec apod.), jejíž osobní údaje již chráněny jsou," zdůrazňuje Tereza Lukášová. Např. personifikovaný e-mail zaměstnance, který jedná za zaměstnavatele – právnickou osobu, již osobním údajem je a je tudíž chráněn.

GDPR vyžaduje nějakým vhodným a dostatečným způsobem osobní data zabezpečit, aby nemohlo dojít k jejich zneužití či odcizení. „Je tedy vhodné, aby byla například IT zařízení vždy pod nějakým heslem, aby byly prováděny zálohy těchto zařízení, případně šifrování těchto dat. Co se týká papírové formy dokumentů, tak by zase měly být uložené na místech, ke kterým má přístup pouze oprávněná osoba. Například nějaká uzamykatelná místnost, skříň, která má zámek, trezor a jiné," dává konkrétní příklady Jaroslav Benda.

GDPR se vztahuje na veškeré osobní údaje fyzických osob

Rozsah ochrany, kterou GDPR poskytuje osobním údajům, je poměrně široký. Obecně lze říci, že se vztahuje na veškeré osobní údaje fyzických osob. „Ovšem nutno doplnit, že různým kategoriím osobních údajů je poskytována také různá míra ochrany," říká Tereza Lukášová a dává příklad: „Kupříkladu na ochranu zvláštní kategorie osobních údajů (údaje vypovídající o rasovém či etnickém původu ad.) jsou kladeny nároky vyšší než na ochranu běžných osobních údajů."

Jak jsou osobní údaje podle GDPR zpracovávány?

Zpracováním osobních údajů je jakákoliv operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizova-

»
„GDPR má vlastně dva důležité body. Tím prvním je ochrana získaných osobních údajů jako taková a tím druhým je informovanost fyzických osob o jejich právech a také o tom, jak je vlastně nakládáno s jejich osobními údaji. Za jakým účelem tato data potřebuji, z jakého právního titulu, na jak dlouho je uchovávám, kdo s nimi pracuje, jestli data předávám a komu atd.," vysvětluje Jaroslav Benda.

Jaroslav Benda

FOTO: SAMPHOTO

ných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

V Česku ochranu osobních údajů kontroluje pouze jeden úřad

Úřad pro ochranu osobních údajů je v ČR pouze jeden, jedná se o dozorový úřad podle terminologie GDPR. Tato instituce zastřešuje na území našeho státu ochrany osobních údajů, vykonává pravomoci vyšetřovací, nápravné, povolovací a poradní. Jde tedy o jakýsi generální orgán pro zajištění a kontrolu řádné ochrany osobních orgánů na území příslušného členského státu EU. „Nutno poznamenat, že tuto funkci plnil již před účinností GDPR na základě zákona č. 101/2000 Sb., o ochraně osobních údajů," informuje magistra Lukášová.

GDPR je založeno na zásadách ochrany osobních údajů

GDPR mimo jiné stanovuje zásady ochrany osobních údajů. Jedná se o základní stavební kameny, na kterých je GDPR založeno. „Většina z těchto zásad byla součástí již předchozí unijní úpravy ochrany osobních údajů (Směrnice 95/46/ES) a také zákona o ochraně osobních údajů," informuje magistra Lukášová. Novinkou v GDPR je pak dle jejích slov jejich přímé vyjmenování a stanovení odpovědnosti správce za jejich dodržování. Správce je zde povinen být schopen doložit soulad předmětného zpracování s těmito zásadami (tzv. princip odpovědnosti správce). Podle slov Terezy Lukášové pak mezi tyto zásady patří následující: zásada zákonnosti, zásada korektnosti a transparentnosti, zásada omezení účelu, zásada minimalizace údajů, zásada přesnosti, zásada omezení uložení, zásada integrity a důvěrnosti.

Správcům a zpracovatelům GDPR stanovuje nové povinnosti

GDPR se vztahuje také na nově stanovené povinnosti, které nařizuje správcům a zpracovatelům. „Jedná se o povinnost doložit soulad s GDPR – identifikace hrozeb, nastavení procesů pro jejich snižování a odstraňování, záznamy o činnostech zpracování, smlouvy se zpracovateli, sledování bezpečnostních incidentů, kodexy, osvědčení apod.," vyjmenovává inženýrka Steinerová. Primární povinností správců je pak podle jejích slov určit rizika a snižovat je na základě kontinuálního procesu – nastavit taková technická a organizační opatření, která budou rizika snižovat. V případě bezpečnostních incidentů tyto hlásit ÚOOÚ. „Těch povinností je celkem dost," dodává věcně odbornice.

Při porušení povinností dle GDPR může dozorový úřad ukládat sankce

„Nařízení jako jeden z pramenů evropského (unijního) práva se např. od směrnice, která musí být implementována a transponována do právních řádů jednotlivých členských států, odlišuje tím, že má tzv. přímý účinek, což znamená, že zakládá práva a ukládá povinnosti přímo jednotlivcům (občanům členských států EU), je tedy platné a účinné bez nutnosti prováděcí úpravy členského státu," vysvětluje Tereza Lukášová.
Povinnosti, které GDPR ukládá, tedy platí pro adresáty této normy přímo od 25. 5. 2018. Ke kontrole jejich dodržování je potom oprávněn dozorový úřad (u nás Úřad pro ochranu osobních údajů), který při porušení těchto povinností může např. uložit nápravná opatření či sankce.

Transparentnost je nezbytná

„Zásadami ochrany osobních údajů je myšlen právě ten dokument, který popisuje, jak má firma zpracované GDPR, jaká jsou jejich práva, jak je dále pracováno s osobními údaji, kam se mohou obrátit v případě dotazů či stížností atd.," vysvětluje Jaroslav Benda. Tento dokument by měl být jednoduše přístupný buď na webových stránkách, nebo v místě, kde k předání osobních údajů dochází, aby si je mohl každý, kdo bude tato data poskytovat, přečíst ještě před tím, než tato svoje data někomu sdělí. Podnikatel tak musí zajistit ochranu dat uvnitř společnosti a zároveň zpřístupnit informace o transparentnosti dat a o právech daného subjektu, takzvanou informovanost.

» **Primární povinností správců je pak podle jejích slov určit rizika a snižovat je na základě kontinuálního procesu – nastavit taková technická a organizační opatření, která budou rizika snižovat.**