POVINNOSTI SPOLEČNOSTI ESO9 INTERNATIONAL A.S. VZHLEDEM K IMPLEMENTACI NAŘÍZENÍ GDPR

Před samotným popisem, jak bude nařízení GDPR implementováno v IS ESO9, je nutné uvést, že se jedná o problematiku zasahující do více oblastí. Základní rámec jí dává právo, pro vlastní realizaci je nutná dobrá orientace ve firemních procesech a technická řešení nabízí oblast IT. I když se následující text týká jen oblasti IT (konkrétně zpracování dat v IS ESO9), je třeba mít na paměti, že záběr GDPR je daleko širší.

Povinnosti naší společnosti pro splnění podmínek nařízení GDPR se odvíjejí od způsobu provozu IS ESO9. Z pohledu zabezpečení přístupu k datům lze IS ESO9 provozovat dvěma základními způsoby:

- *na vlastních HW prostředcích*
- *v cloudu*

1 Na vlastních HW prostředcích

Pokud zákazník provozuje informační systém ESO9 (dále jen IS) na vlastních prostředcích, figurujeme zde jen jako dodavatelé systému, zatímco provozovatelem IS a vlastníkem (a zpracovatelem!) dat v něm obsažených je zákazník. Od tohoto faktu se pak odvíjejí povinnosti obou stran.

Naše povinnosti

Vzhledem k tomu, že za osobní údaje zpracovávané v IS zodpovídá zákazník, leží implementace GDPR především na jeho bedrech.

Ze strany společnosti ESO9 international a.s. budou mít zákazníci k dispozici vzorovou směrnici popisující nakládání s osobními údaji v IS ESO9, která jim může posloužit jako základ jejich vlastních směrnic pro tuto oblast. Půjde zejména o:

- Popis způsobu zabezpečení přístupu k datům v IS ESO9 na systémové úrovni, tj. obecná doporučení zabezpečení serverové a klientské vrstvy IS ESO9 (např. tedy doporučení pro zabezpečení přístupů k MS SQL Serveru).
- Popis způsobu zabezpečení přístupu k datům v IS ESO9 na aplikační úrovni, tj. popis možností zabezpečení IS ESO9. Jedná se o stejné postupy, se kterými jsou seznamováni správci IS ESO9 na certifikačních školeních. Pokud má tedy daná společnost svého certifikovaného správce, tak již tyto postupy zná a využívá.
- Popis zabezpečení komunikační infrastruktury v rámci IS ESO9.
- Audit přístupů do aplikace, který vychází ze záznamů v logovací databázi.
- Vzorový souhlas se zpracováním osobních údajů. Zákazník by si měl od svých obchodních partnerů (tj. od subjektů osobních údajů) vyžádat stejný souhlas, o jaký jej bude žádat naše společnost (ve svém interním IS si potenciálně uchováváme i osobní údaje našich zákazníků).

Povinnosti zákazníka

Povinnosti zákazníka se budou odvíjet zejména od faktu, zda zpracovává osobní údaje a v jakém rozsahu. Každá společnost by tedy měla projít minimálně interním auditem, v němž si zmapuje, které osobní údaje zpracovává a v jakých agendách (kromě IS ESO9 se mohou taková data vyskytovat např. v papírové podobě či v groupware typu MS Exchange, vztahují se na ně však stejná pravidla).

Za osobní údaj se považuje každá informace, kterou lze specifikovat konkrétní osobu, např. tedy rodné číslo, e-mail či telefonní číslo. Kromě osobních údajů může zákazník evidovat i tzv. citlivé údaje, za které se považuje např. rasový původ, sexuální orientace, trestní delikty, zdravotní stav či biometrické údaje. Na zpracování takových údajů se vztahují přísnější normy bez ohledu na jejich objem či počet zaměstnanců společnosti (viz níže). V ESO9 se však takové údaje nezpracovávají, vzorové směrnice se tedy budou týkat jen osobních údajů. Pokud by si však zákazník v rámci vlastního rozšíření aplikace ESO9 Profi citlivé údaje zpracovával, je nutné počítat s jejich přísnější technickou ochranou např. anonymizací či šifrováním.

Za osobní údaje se naopak nepovažují kontaktní informace v rámci společnosti, tedy např. firemní e-mail či firemní telefon. Pokud tedy daná společnost ve svém portfoliu nemá fyzické osoby, není třeba uvažovat o ochraně osobních údajů v této agendě.

Dalším rozměrem GDPR agendy je množství zpracovávaných osobních údajů. Od toho se odvíjí nejen otázka, jak hluboce analyzovat vnitrofiremní procesy, ale i otázka pověřence pro ochranu osobních údajů (DPO – Data Protection Officer). Povinnost zavést tuto pozici se týká organizací s počtem zaměstnanců vyšším než 250 nebo organizací zpracovávajících velký objem rizikových dat. Jiná situace tedy bude např. ve výrobním podniku a zcela jiná např. v personální agentuře či cestovní kanceláři. Může se tedy ukázat, že s ohledem na množství (resp. neexistenci) osobních údajů nebude nutné žádné další interní směrnice vytvářet.

Po zmapování všech firemních agend, v nichž se osobní údaje vyskytují, je třeba určit účel, za jakým se osobní data shromažďují. Podle něj se mj. určuje, zda zákazník bude či nebude potřebovat souhlas se zpracováním. Obecně zde platí princip minimalizace dat a práva na zapomnění v okamžiku, kdy pomine účel, k němuž byla osobní data shromažďována (a ke kterému byl udělen souhlas). Tj. o subjektu shromažďujeme minimální nutné údaje po minimálně nutnou dobu.

Pokud je během těchto analýz nalezen nedostatek (tj. některé zpracování osobních údajů není v souladu s GDPR), je třeba změnit příslušné vnitrofiremní procesy.

Následuje tvorba interních směrnic pro zacházení s osobními údaji. V tomto místě bude možné vycházet ze vzorových šablon dodaných naší společností.

2 Provoz IS ESO9 v cloudu

Provozem IS ESO9 v cloudu se myslí především provoz na našem hostingu, za který zodpovídá společnost ESO9 international a.s. Principielně stejné podmínky by však měly platit u všech ostatních providerů. V takovém režimu provozu jsme dodavateli a provozovateli IS, vlastníkem a zpracovatelem dat je zákazník. Pro zpracování osobních údajů v cloudu platí totéž co v předchozím případě - žádná osobní data obsažená v databázích na cloudu nezpracováváme, jedná se vždy o data zákazníků. K datům v cloudu nemáme přístup, za jejich obsah a zpracování zodpovídá zákazník. Výjimkou budou servisní zásahy (viz níže).

Naše povinnosti

Hlavní výhodou cloudového provozu je, že zákazníkovi odpadá nutnost řešit zabezpečení přístupu k datům na systémové úrovni. Za systémovou bezpečnost zodpovídá naše společnost.

S každým z našich zákazníků provozujících svou aplikaci v našem cloudu uzavřeme rámcovou smlouvu o zpřístupnění dat (resp. databází a jejich obsahu, tedy potenciálně i osobních dat) pro účely implementace či servisního zásahu. Pro řešení zákaznických požadavků se zpravidla bez lokální kopie zákaznické databáze neobejdeme, dvojnásob to pak platí ve fázi implementace nové aplikace. Při tvorbě každé objednávky (telefonicky, e-mailem či přes systém Podpory) nám bude zákazník udělovat souhlas s přístupem k osobním údajům pro účel vyřešení jeho požadavku. Po dokončení práce příslušný zaměstnanec bezodkladně smaže všechny kopie zákaznických dat. Souhlas musí být dán samostatně a svobodně, tj. nesmí být součástí např. obchodní smlouvy, aby jej šlo samostatně odvolat.

Součástí smlouvy se zákazníky naopak bude právo na zapomnění. Interní směrnice cloudového provozu pak bude obsahovat mechanismus ukončení provozu zákaznické aplikace. V takovém případě zákazník dostane kompletní zálohu svých dat a všechny kopie zákaznických dat (ostrá a záložní) budou vymazány ze všech našich úložišť.

Data zákazníků (až na výjimky občanů EU) udržujeme na území Evropské unie a v žádném případě nedochází k jejich převodu na jiné zpracovatele bez ohledu na jejich umístění. Pro řadu cloudových providerů může být právě tento bod problematický.

Povinnosti zákazníka

Vzhledem k tomu, co bylo řečeno výše, budou povinnosti zákazníka vzhledem k implementaci požadavků GDPR stejné jako v případě provozu IS ESO9 na vlastních HW prostředcích, ovšem bez nutnosti řešit zabezpečení dat na systémové úrovni a na úrovni komunikační infrastruktury.

Koho se GDPR týká?

GDPR zavádí celou řadu nových práv a povinností a platí celosvětově pro všechny subjekty, které zpracovávají osobní údaje občanů EU. GDPR obecně reguluje zacházení s jakýmikoliv informacemi vztahujícími se k identifikované nebo identifikovatelné osobě. Stanovuje povinnosti pro správce i zpracovatele údajů (včetně povinnosti hlásit jakékoliv incidenty v oblasti práce s osobními daty a jejich ochrany), definuje podmínky, za kterých mohou být takové údaje zpracovávány, stanovuje pro jejich zpracování řadu pravidel a dává subjektům těchto informací řadu práv – včetně práva „být zapomenut“. Zavádí také roli pověřence pro ochranu osobních údajů (DPO - Data Protection Officer).

Osobní údaje

Osobní údaje jsou jakékoli informace, které vedou k identifikaci subjektu či osoby. Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

Citlivé údaje

Zvláštní pozornost je pak směřována na tzv. citlivé údaje, které zahrnují údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Jedná se v souhrnu o data, která by mohla zapříčinit dané osobě případnou diskriminaci. Do kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje.

Platnost nařízení

Toto nařízení by mělo vstoupit v platnost 25. května 2018 a nahradit zákon 101/2000 Sb. o ochraně osobních údajů a směrnici EU 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Základní informace

GDPR (Global Data Protection Regulation) - Nařízení EU 2016/679 představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji.

Jaké budou sankce?

Sankce za nedodržení tohoto nařízení mohou být dle charakteru a závažnosti incidentu až 20 milionů EUR nebo až 4 % z celkového obratu společnosti. Neberte tedy GDPR na lehkou váhu a začněte se připravovat co nejdříve.

Kde začít?

Vyhovět všem náročným podmínkám nařízení GDPR si vyžádá řadu opatření organizačního, procesního i technického charakteru. Žádný technologický prvek ani software shodu s požadavky GDPR nezajistí, ale bez něj je dosažení shody s těmito požadavky nemyslitelné. Správci a zpracovatelé jsou za určitých podmínek povinni jmenovat pověřence pro ochranu osobních údajů.

Každá z firem by tedy měla:

1. Zmapovat, kde všude jsou osobní údaje uloženy.
2. Zjistit, kdo má právo s nimi manipulovat.
3. Odhalit, kdo všechno k nim má přístup a proč.
4. Vyřešit nekoncepčnost v IT, kdy jsou data uložena mimo úložiště k tomu určená (neoficiální zálohy, data v telefonech zaměstnanců apod.).
5. Obeslat subjekty, se kterými obchoduje a jejichž osobní údaje eviduje, a zajistit si potřebný souhlas se zpracováním (pokud jej z minulosti již nemá).
6. Definovat pravidla pro zajištění dat před úniky – a to jak před útoky zvenčí, tak před internimi incidenty.
7. Zpracovat metodiky pro všechny možné incidenty a zajistit jejich plnění.