GDPR teorie a praxe

O evropské směrnici se toho, alespoň v teoretické rovině, již napsalo dost. Není tedy třeba citovat jednotlivé pasáže či výklady. Pojďme se zaměřit na konkrétní provedení, která se od úmyslu trošku liší. Na úvod je třeba si říct, že záměrem směrnice rozhodně není tlak na to, abyste po léta posbíraná data vymazali. Je však nutné se zamyslet nad způsobem ukládání, uchovávání, zabezpečení přístupu k nim a v neposlední řadě informovanosti lidí, kteří s daty nakládají. Rovněž je třeba popsat procesy.

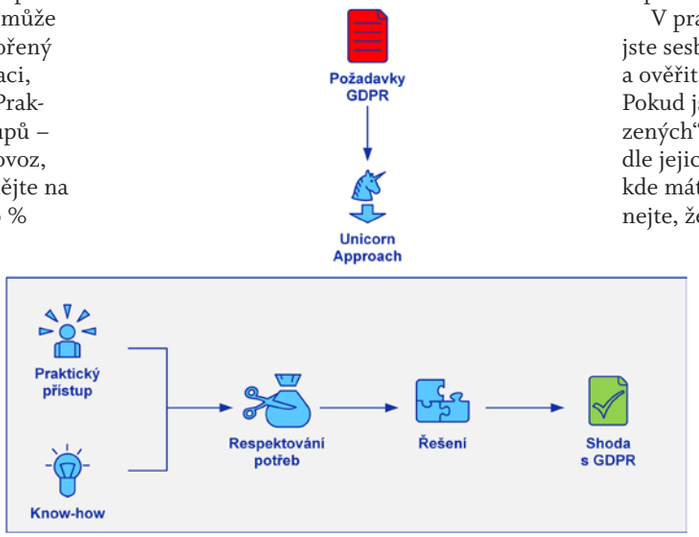
PAVEL KUDRMAN

Zastavme se teď u procesů. Budete se možná divit, ale většina firem má procesy popsány jen částečně, někde dokonce chybějí úplně. Na druhou stranu věřte, že popis procesu může být stručný, třeba jen jeden odstavec vytvořený odborníkem. Ve své praxi jsem zažil i situaci, kde popis procesu byl svěřen právníkovi. Praktické je zvolit podle mne kombinaci přístupů – tvorbu můžete svěřit lidem, kteří znají provoz, a právníky pověřit až finální kontrolou. Mějte na paměti, že kontrola procesu zabere cca 20 % času tvorby. Společnosti, které mají certifikát ISO 27001, jsou v tomto trochu napřed, jelikož mají procesy již popsané. Fungují podle léty ověřených standardů a stačí mnohdy jen drobné úpravy. Dá se tedy říct, že záleží na míře počátečního „chaosu".

V samotném úvodu je potřeba si udělat pořádek v osobních údajích podle aktuálně platného zákona č. 101/2000 Sb. Pokud již máte data identifikovaná, je dobré k nim posbírat informace a definovat, jakou část z nich sbíráte podle kterého zákona včetně toho, o jaký zákon jde. Česká legislativa totiž disponuje zákony, které zatím nejsou v souladu s GDPR směrnicí. Mám na mysli např. zákon a opatření proti legalizaci výnosů z trestné činnosti a financování terorismu (AML zákon), účetní zákon (nebo alespoň o termín uchovávání po dobu deseti let) nebo třeba zákon o archivnictví a spisové službě (možná budete znát termín skartační řád) atd.

Další kolonkou mohou být data, která zpracováváte na základě oprávněného důvodu. Ten však musíte být schopni prokázat, například proč sbíráte fotografii zaměstnance. Oprávněným důvodem může být např.: „Je umístěná na vstupní kartě a slouží ke kontrole osoby, která se jí prokazuje. Chceme tím zabránit vstupu do areálu neoprávněným osobám," apod.

Pokud jsou data sbírána v rámci předmětu podnikání a spadají do GDPR, je nutné se rozhodnout, jestli jsou opravdu potřeba. Pokud ne, doporučuji je vymazat – obvykle to vyjde levněji. Pokud ano, je nutné data ukládat ideálně na jedno místo, kde je bude možné snadněji zabezpečit, monitorovat, vymazat nebo přenést podle instrukcí případných budoucích žadatelů.



Co v praxi znamená dodržení GDPR směrnice

Ve zkratce, budete muset věnovat čas hlavně personální a klientské agendě. Tam najdete spoustu osobních údajů.

Stejně tak budete zjišťovat způsob zpracování. Děje se tak automatizovaně, nebo jedete „postaru", ručním způsobem? Nezapomínejte, že budete údaje neustále aktualizovat.

S tím souvisí i to, kdo k jakým datům může přistupovat a nakládat s nimi. Pokud budete mít data posbíraná, je třeba zaměřit se na termíny uchovávání, jelikož je musíte uchovávat jen po dobu nezbytně nutnou. A tím se dostáváte k odpovědnosti, každý proces musí mít svoji odpovědnou osobu. Rovněž musíte určit kontakt pro komunikaci, jak směrem do firmy (personální oddělení), tak směrem ven (právní oddělení nebo tiskový mluvčí) a ideálně mít to někde popsáno.

A od procesů přicházíte k nástrojům. Musíte zjistit, zda máte k dispozici technické nástroje, které vám pomohou ochránit osobní údaje. Rovněž je nutné zamezit náhodnému či cílenému neautorizovanému přístupu k datům, jejich změně, zničení nebo ztrátě. V tomto případě statistiky nelžou a říkají, že nejslabším článkem je „lidský faktor", proto je potřeba své zaměstnance pravidelně vzdělávat.

Praktické příklady

Rád bych vám nabídl rozdílné pohledy účastníků vstupujících do těchto úprav podle evropské směrnice. To, co je na jedné straně chápáno jako pozitivní, jasné, transparentní a logické na straně právní, je z pohledu IT chápáno jako problém, se kterým se bude muset firma vypořádat velmi rychle.

Co nastane, když bývalý zaměstnanec bude požadovat podle zmiňované směrnice „být zapomenut"?

V praxi to znamená zkontrolovat data, která jste sesbírali po dobu trvání pracovního poměru, a ověřit, na základě jakých zákonů jste je sbírali. Pokud jsou tato data sbírána na základě „nadřazených" zákonů, musíte je ponechat přesně podle jejich znění. To samé můžete udělat s daty, kde máte „oprávněný zájem". Ovšem nezapomínejte, že pokud dojde ke střetu, budete muset oprávněný zájem doložit. Ostatní osobní údaje budete muset, pokud o to budete požádáni, umět systémově smazat. Termín systémově volím záměrně, neboť si nedovedu představit dělat tento proces manuálně.

Otázka je, jak rychle a kvalitně vyřešit v praxi právo „být zapomenut". V aktivních datech problém nebude, pozornost je však potřeba věnovat práci s archivem. A to především při obnově dat z archivu v situaci, kdy o aktivně používaná data přijdete a musíte je získat do systému zpět. Zaměstnanec požádal před půl rokem o vymazání, a to se také stalo. Je třeba ale myslet na to, že obnovujete data starší, a tudíž i s jeho všemi daty – těmi, které jste později z databáze vymazali. Doporučuji proto tento proces řešit automatizovaně. Proč? To je jednoduché, náklady na vyhledání a vymazání nelze přenést na žadatele, a tím pádem vám mohou neúměrně narůstat provozní náklady.

Práce s osobními daty

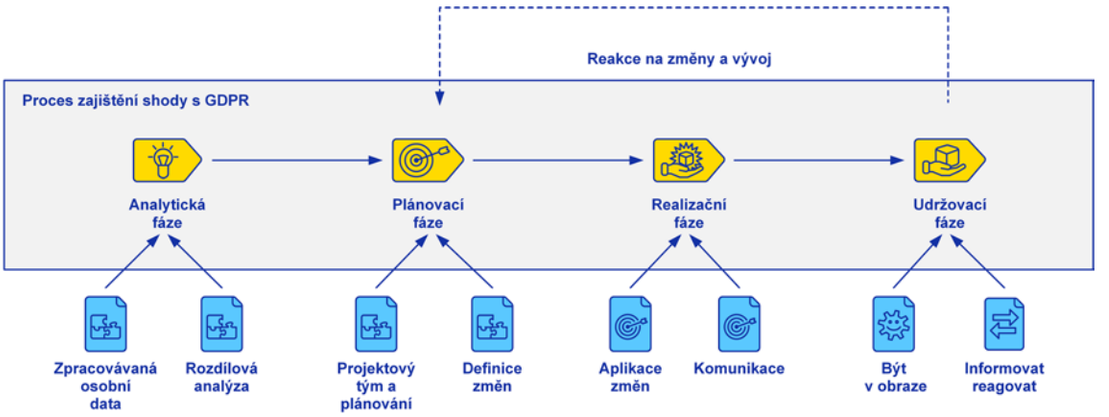
Věcí, se kterými se IT musí vyrovnat, je více. Například směrnice pojem, co to jsou osobní data, výrazně rozšiřuje. Záhy zjistíte, že to, co dříve nebylo považováno za osobní údaj, najednou osobním údajem je. Z pohledu vývoje je to logické a pochopitelné. Ovšem jak to sdělit systémům, které byly vytvořeny dříve než směrnice? A teď nemám na mysli např. rodné číslo s daným formátem xxxxxx/xxxx, které v nestrukturovaných datech snadno vyhledáte. Z praxe vím, že ve firmách a institucích se dlouhá léta sbíraly osobní údaje a ukládaly se do různých sy-

stémů a aplikací atd. S nástupem GDPR bude muset IT oddělení zajistit systémově konzistentní vymazání napříč celou firmou a všemi systémy, databázemi, aplikacemi apod.

Vymazání je ovšem jen jednou částí. Pokud bychom se zaměřili na přenositelnost údajů k jinému zpracovateli, bude potřeba řešit hodně exportů ze systémů napříč celou firmou. Dá se předpokládat, že přenos strukturovaných dat půjde do textových souborů, .xls souborů nebo jejich alternativ. Nestrukturovaná data bude těžší vyhledat než přenést, a to samé bude s papírovou dokumentací.

Co se vývoje týče, na vzestupu je psaní konektorů přes API a exporty do nějakého normalizovaného, přenositelného formátu. Samostatnou disciplínou v přenosu bude dostat data ze SW psaného na míru konkrétnímu zákazníkovi.

Viděl jsem nemalý počet metodik od desítek společností a v drtivé většině se zabývaly v analytické fázi jen procesy. Za své mnohaleté působení v IT i bezpečnosti jsem pochopil, že procesy a nástroje jsou spojené nádoby. A neustále zjišťuji, že analýza procesů a nástrojů musí jít ruku v ruce. Proto apeluji na to, abyste brali bezpečnost jako celek dělící se na procesní část (GDPR) a kybernetickou část (nástroje ochrany). Tyto dvě části musejí být kontinuálně rozvíjeny a musejí na sebe navazovat.



Analytická část je pouze první etapou přechodu firmy na „GDPR compliance“. Situace je jasně daná – termín je květen příští rok, a potřebujete myslet několik kroků dopředu. Například po analytické části přijde na řadu část rozhodovací a následně realizační. Realizací to však nekončí, neboť budete muset udržovat to, co jste si za své peníze pořídili, ve stavu shodném se směrnicí a případně měnili podle v budoucnu platných regulativ. To samé platí, pokud učiníte obměnu starého systému za nový, a tím výrazně změníte tok dat. Dohlížející osoba nad těmito procesy by měla být schopna zvládnout vypracování analýzy rizik.

Pozor, pokud budete analýzu rizik řešit na poslední chvíli nebo ji zadáte někomu bez zkušeností (analýza, právo – evropská regulativa, přesah do IT infrastruktury a bezpečnosti), může soulad se směrnicí dopadnout i jinak, než byste si přáli. Každopádně cílem by mělo být dodržení evropské legislativy pouze s minimálním navýšením provozních nákladů.

Na závěr se trochu zasním: představte si budoucnost – pracovnici v call centru nebo za přepážkou, která bude mít ve svém profilu na monitoru tři tlačítka: anonymizovat, vymazat, nebo přenést osobní údaje. A bude řešit požadavky zákazníků jedním klikem. Nebude to krásné?

Autor je Infrastucture, Security, GDPR consultant v Unicorn Systems