EVA SKORNICKOVÁ

Nabídka služeb v rámci implementace GDPR pravidel

Co je obecné nařízení GDPR?

V roce 2016 Evropský parlament schválil nové nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR), které bude účinné v květnu roku 2018. Došlo tak k nahrazení současné směrnice z 90. let (č. 95/46/ES), která již požadavkům dnešní doby zcela nevyhovuje.

GDPR je jedním z nejkomplexnějších souborů pravidel na ochranu dat na světě a týká se každého subjektu, který shromažďuje nebo zpracovává osobní údaje občanů EU, bez ohledu na jeho geografickou lokalitu. Nařízení se dotkne prakticky každého, fyzické či právnické osoby, naprosto všech, kteří zpracovávají osobní údaje svých zaměstnanců, zákazníků, klientů či dodavatelů, a to napříč segmenty a odvětvími.

V případě porušení, nezavedení či nepřipravenosti na nové nařízení, mohou povinným subjektům hrozit vysoké pokuty, v mnoha případech až likvidační! Z toho důvodu je nezbytné, aby všechny subjekty, které zpracovávají osobní údaje fyzických osob, provedly komplexní datovou analýzu a následně implementovaly technická, procesní a organizační opatření, která zajistí plnou kompatibilitu a soulad s novými pravidly plynoucími z GDPR.

www.skornickova.eu | eva@skornickova.eu | +420 602 655 008 | Nobelova 812/4, 160 00 Praha 6

Hlavní změny vyvolané GDPR

Níže je uveden výčet hlavních změn, které GDPR oproti stávající legislativní úpravě přináší, a které budou muset organizace implementovat do svých systémů řízení ať už v podobě úpravy produktů, procesů nebo interní legislativy či ICT podpory.

- **Posílení práv subjektů údajů**

  GDPR klade hlavní důraz na práva fyzických osob subjektů údajů) a jejich dodržování ze strany správců/zpracovatelů osobních údajů.

- **Širší informační povinnosti**

  Správce je povinen subjekty údajů dostatečně informovat mj. o účelu a právním základu zpracování, řetězci zpracovatelů údajů, o jejich právech, atd.

- **Nové požadavky na smlouvu o zpracování**

  Smlouva mezi správcem a zpracovatelem musí být písemná (včetně elektronické formy) a obsahovat některé specifické povinnosti, vč. povinnosti auditů, bezpečnostních opatření, aj.

- **Požadavky na bezpečnostní opatření**

  GDPR zdůrazňuje pro zachování ochrany osobních údajů implementaci bezpečnostních opatření. Nařízení je založeno na principu technologické neutrality. Zmiňuje však konkrétní bezpečnostní opatření například ve formě pseudonymizace.

- **Vlastní vyhodnocení dopadů zpracování**

  Správci jsou povinni provést hodnocení vlastních aktivit a jejich dopadů na ochranu osobních údajů a zájmy fyzických osob, pokud jejich zpracování může představovat vysoké riziko pro takové zájmy.

- **Specifická pravidla pro zpracovatele**

  Některé povinnosti a jejich vynutitelnost (vč. ukládání pokut) se nově nevztahují jen na správce, ale i na zpracovatele osobních údajů.

- **Vznik Evropského sboru pro ochranu osobních údajů**

  GDPR nově vznikne nový celoevropský orgán (nahrazující dosavadní poradní skupinu WP 29), který bude mít pravomoci především v oblasti konzultací a sjednocování výkladu sporných otázek v oblasti ochrany osobních údajů.

- **Pověřenec pro ochranu osobních údajů**

  Správce i zpracovatel osobních údajů jsou povinni jmenovat nezávislého pověřence, pokud nakládání s osobními údaji tvoří důležitý pilíř jejich podnikání.

- **Jednoznačný souhlas k jakémukoli zpracování údajů**

  Kromě několika zákonných výjimek jako je plnění smlouvy, veřejný či oprávněný zájem, musí být zpracování osobních údajů vždy založeno na jednoznačném, konkrétním a informovaném souhlasu subjektu údajů.

- **Odvolání souhlasu a právo být zapomenut**

  Subjekt údajů má kdykoliv během zpracování svých údajů právo odvolat dříve udělený souhlas se zpracováním. Správce pak musí ukončit zpracování takových údajů.

- **Privacy by design and default**

  Pro zaručení souladu s GDPR jsou zdůrazňovány zásady „privacy by design“ (za každé situace brát v úvahu ochranu osobních údajů) a „privacy by default“ (automatická aplikace nejpřísnějšího režimu ochrany osobních údajů).

- **Přenositelnost údajů**

  Správci osobních údajů jsou povinni zajistit na žádost subjektu údajů možnost přenosu jeho údajů k jinému správci (v kompatibilním formátu).

- **Notifikace neoprávněného přístupu k osobním údajům**

  V případě neoprávněného přístupu k osobním údajům jsou správci i zpracovatelé povinni notifikovat dozorové orgány a ve vybraných případech i samotné subjekty údajů.

- **Zrušena povinnost registrace u dozorových úřadů**

  Subjekty zpracovávající osobní údaje nebudou mít od nabytí účinnosti GDPR povinnost registrovat se u ÚOOÚ. Namísto toho zavádějí jiné mechanismy například v podobě sebehodnotících procesů.

- **Hlavní dozorový orgán jako jedno správní místo**

  Subjekty zpracovávající osobní údaje v různých členských státech EU nemusí komunikovat se všemi národními dozorovými orgány. Díky pravidlu „one-stop-shop“ je možné komunikovat pouze s dozorovým orgánem v jedné členské zemi. Výběr dozorového orgánu je ponechán na subjektu zpracovávajícím osobní údaje.

- **Výrazně vyšší pokuty za neplnění povinností**

  Správci i zpracovatelé mohou za porušení svých povinností čelit pokutám ve výši až 4 % celosvětového obratu své skupiny či 20 mil EUR.

www.skornickova.eu | eva@skornickova.eu | +420 602 655 008 | Nobelova 812/4, 160 00 Praha 6

Dopady GDPR na organizaci

Implementace změn plynoucích z GDPR dopadne na celý systém řízení organizace a na všechny organizační úrovně. Náklady na implementaci GDPR budou vyplývat primárně z nutnosti adaptace na novou právní úpravu zejména v podobě úpravy parametrů produktů, přizpůsobení procesů (včetně vazeb na partnery), interní legislativy a informačních systémů.
Tyto náklady budou převážně jednorázové.

Hlavní podnikatelská činnost

- Úprava obchodních procesů
- Úprava nebo změna produktů
- Úprava smluvní dokumentace
- Úprava uživatelských textů a funkcionalit v aplikačních rozhraních
- Školení zaměstnanců

Procesy a interní legislativa

- Změny v procesu controllingu a reportingu
- Změny v procesu řízení rizik
- Změny v procesu řízení lidských zdrojů
- Úpravy zaměstnaneckých smluv
- Úpravy dodavatelských smluv
- Aktualizace interní legislativy

Informační a komunikační technologie

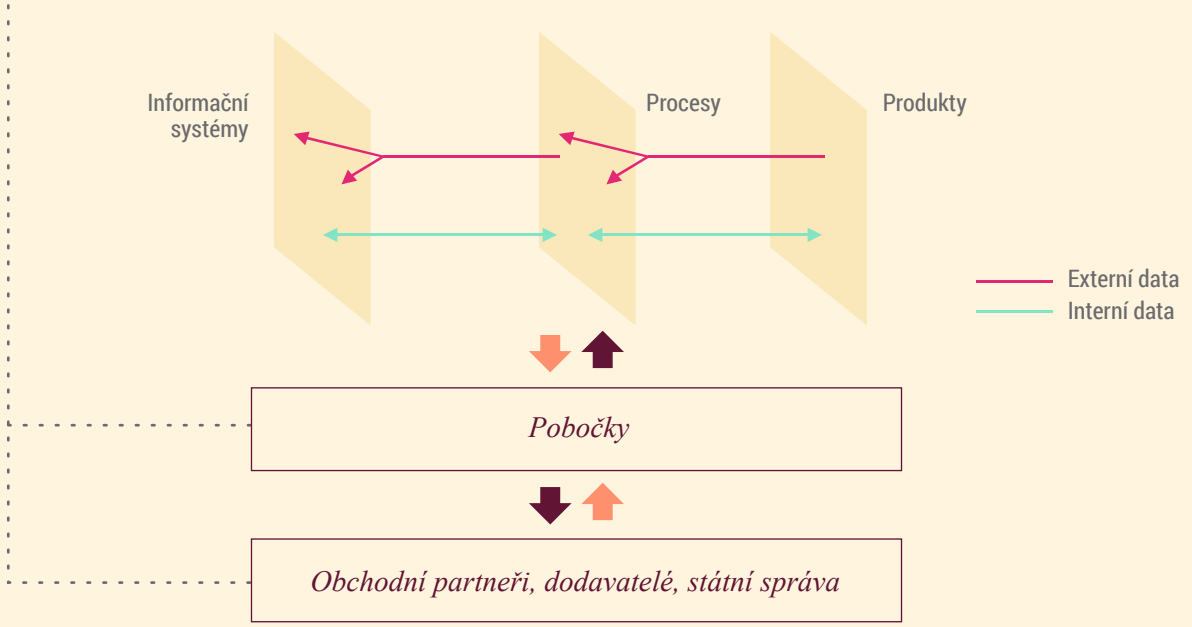
- Revize datové a bezpečnostní architektury
- Revize komunikačních rozhraní
- Aktualizace tiskových šablon
- Aktualizace a upgrade systémů
- Aplikace bezpečnostních opatření na všech vrstvách ICT infrastruktury

www.skornickova.eu | eva@skornickova.eu | +420 602 655 008 | Nobelova 812/4, 160 00 Praha 6

Náš přístup k zajištění shody s GDPR

Dopady GDPR se prolínají celou organizací a všemi úrovněmi její činnosti. Změny je vždy nutné vnímat v kontextu produktů, procesů a informačních systémů. GDPR ovlivňuje jak toky informací v podobě afilací (informací sdílených s pobočkami či dceřinými společnostmi), tak i externí toky (např. dodavatelé ICT).

Zdroje osobních dat



Zajištění shody s GDPR proto vyžaduje komplexní přístup. Nabídka služeb v rámci implementace GDPR pravidel se skládá z jednotlivých na sebe navazujících fází. S ohledem na skutečnost, že se aplikace GDPR pravidel dotkne celé organizace jako celku s výrazným dopadem na řadu interních činností a procesů, tak i tato nabídka vychází z nutnosti zapojení týmu expertů, kteří budou aplikaci pravidel nařízení řídit ve spolupráci s vrcholným managementem dané společnosti.

1. Definice rozsahu posuzování
2. Analýza stávajícího stavu zpracování osobních údajů
3. Příprava projektových záměrů a harmonogramu implementace
4. Realizace projektových záměrů

www.skornickova.eu | eva@skornickova.eu | +420 602 655 008 | Nobelova 812/4, 160 00 Praha 6

1. Definice rozsahu posuzování

Před samotným vyhodnocováním potenciálních změn, které GDPR pro organizaci představuje, je nejprve nezbytné předběžně vyhodnotit stávající stav organizace v oblasti shromažďování, zpracovávání a užití osobních údajů a identifikovat činnosti a informační systémy organizace, na které může GDPR dopadat.

Cíl:

- Zúžit povinnosti GDPR na ty, které jsou pro organizaci relevantní
- Definovat rozsah projektu, jeho harmonogram a rozpočet

Náš přístup

A Úvodní školení

Před samotnou analýzou stávajícího stavu zpracování osobních údajů bude v prvním kroku provedeno seznámení klíčových zaměstnanců organizace s problematikou GDPR.
Obsahem školení bude seznámení se základními změnami plynoucími z GDPR, představení základních povinností a představení postupu dalších prací.

B Definice rozsahu posuzování

Druhým krokem bude definice rozsahu posuzování. Tento krok je důležitý proto, že na každou organizaci se budou vztahovat jiné povinnosti plynoucí z GDPR. Bez tohoto kroku by nebylo možné seriózně definovat rozsah projektu a tedy ani připravit harmonogram a rozpočet. Definice rozsahu posuzování bude provedena formou pracovních schůzek s cílem:

- identifikovat typy dat a vymezit pouze ta data, která mají charakter osobních údajů – vymezení rozsahu;
- identifikovat základní kategorie osobních údajů, způsoby a účel jejich zpracování;
- identifikovat přibližný objem osobních údajů;
- identifikovat nástroje informační podpory (IS, databáze, atd.), které jsou pro zpracovávání osobních údajů organizací používané;
- identifikovat základní povinnosti a roli organizace dle GDPR.

Výstup

Projektový záměr definující rozsah, harmonogram a rozpočet, který bude sloužit i jako nabídka našeho expertního týmu.

2.

Analýza stávajícího stavu zpracování osobních údajů

Cíl:

- Analyzovat povinnosti organizace plynoucí z GDPR a získat důkazy o jejich (ne)plnění
- Popsat rozdíly mezi současným stavem a stavem, kdy organizace plnění povinnosti plynoucí z GDPR

Tato fáze si klade za cíl provést základní rozbor společnosti prostřednictvím poskytnutých softwarových modulů a seznamu otázek, jehož výsledkem bude souhrnná zpráva expertního týmu s výčtem kritických bodů, identifikací a analýzou rizik a doporučených následných opatření k nápravě. Výsledná zpráva bude zpracována na základě klientem poskytnutých informací a materiálů a bude sloužit managementu společnosti jako podklad pro rozhodnutí o dalších krocích v realizační fázi.

Náš přístup

A Analýza povinností a shromáždění důkazů o jejich (ne)plnění

Předmětem činností v rámci této analýzy bude:

- analýza zdrojů osobních údajů, právních titulů k jejich zpracování a způsobu jejich dokumentace;
- kategorizace typů osobních údajů;
- kategorizace způsobů zpracování a typů zpracovatelských operací;
- analýza životního cyklu dat;
- analýza interních a externích datových toků a způsobu jejich dokumentace;
- analýza interní legislativy popisující zpracování osobních údajů;
- analýza organizačních a technických opatření sloužících k zabezpečení informačních systémů;
- analýza dalších procesů relevantních pro GDPR (identifikace rizik, apod.).

Výstup

Souhrnná zpráva popisující rozdíly stávajícího stavu zpracování osobních údajů a stavu odpovídajícího legislativě GDPR.
Zpráva bude obsahovat manažerské shrnutí a přehledné tabulky s jednotlivými zjištěními.

Součástí výsledné zprávy bude právní, datový, bezpečnostní a procesní audit.

Právní audit

- S využitím speciálního softwarového modulu, který slouží k detailnímu zmapování interního nakládání s osobními údaji získáme ucelený přehled o současném účelu zpracování osobních údajů klientem, množství a charakteru osobních údajů, které má k dispozici a přehledu aktuálně používaných právních dokumentů a interních směrnic.
- Výsledkem právního auditu bude identifikace rizikových oblastí a činností, které budou muset být uvedeny do souladu s pravidly GDPR, doporučení sestavy dokumentů a směrnic odpovídajících požadavkům nařízení a vyhodnocení povinnosti jmenovat pověřence pro ochranu osobních údajů.
- Nedílnou součástí právního auditu jsou i firemní školení nebo workshopy coby úvod do problematiky nových požadavků na zpracování osobních údajů pro členy vrcholového managementu nebo jím pověřených osob, které budou následně rozhodovat o rozsahu implementace GDPR.

B Rozdílová analýza

Rozdílová analýza vychází z porovnání stávajícího stavu zpracování osobních údajů a stavu odpovídajícího legislativě GDPR.

Jednotlivé v analýze identifikované povinnosti budou popsány a ke každé povinnosti bude uveden závěr, zda je povinnost plněna, zda je plněna jen částečně, nebo zda plněna není. Vždy bude uveden odkaz na relevantní podkladový materiál, na základě kterého byl závěr učiněn a odkaz na článek nařízení GDPR, který povinnost ukládá.

Datový a bezpečnostní audit

- Tato analýza je zaměřena na zmapování výskytu osobních údajů fyzických osob napříč datovou infrastrukturou, tj. síťovými, cloudovými úložišti a různorodými databázemi klienta. Dojde ke zmapování technických HW a SW prostředků pro zpracování a přenosy dat včetně stavu jejich kybernetického zabezpečení, tzn. provozního a bezpečnostního monitoringu, dohledu, aktivních restriktivních a ochranných nástrojů, incident managementu a smluvního zajištění.V rámci analýzy proběhnou konzultace s vlastníky aktiv (osobních údajů) u klienta, v jejichž rámci dojde k identifikaci klíčových systémů, lokalit, oblastí a procesů práce s osobními údaji. Následnou implementací technického řešení na audit nakládání s osobními údaji proběhne u klienta monitoring toku dat po dobu cca 2 týdnů až 1 měsíce, jehož výsledkem bude analýza nasbíraných dat, jejich vyhodnocení a porovnání s procesy zákazníka.
- Výsledná datová analýza zachycených incidentů, potenciálních rizik a doporučení pro další kroky k řešení nalezených problémů bude součástí souhrnné auditní zprávy expertního týmu. Zpráva bude rovněž obsahovat k jednotlivým zjištěním a rizikům formulaci jak v oblasti práce s osobními daty, tak v oblasti jejich pokrytí bezpečnostními prvky ICT infrastruktury, doporučení technických a organizačních opatření k zajištění maxima možného při ošetření těchto rizik ve vazbě na požadavky GDPR.

3.

Příprava projektových záměrů a harmonogramu implementace

Cíl:

- Připravit projektové záměry, které budou obsahovat návrhy na eliminaci všech identifikovaných rozdílů mezi současným stavem a stavem odpovídajícím GDPR
- Připravit harmonogram implementace reflektující priority jednotlivých zjištění

Náš přístup

A Stanovení priorit

Zajištění souladu s GDPR je dlouhodobý proces. Prioritizace nejdůležitějších projektových záměrů proto napomůže zajistit maximální možnou shodu v co nejkratším čase. Priority realizace budou hodnoceny dle několika kritérií, mezi které patří například náročnost implementace, rizika implementace, nebo výše případné sankce za nesplnění povinnosti.

B Příprava projektových záměrů

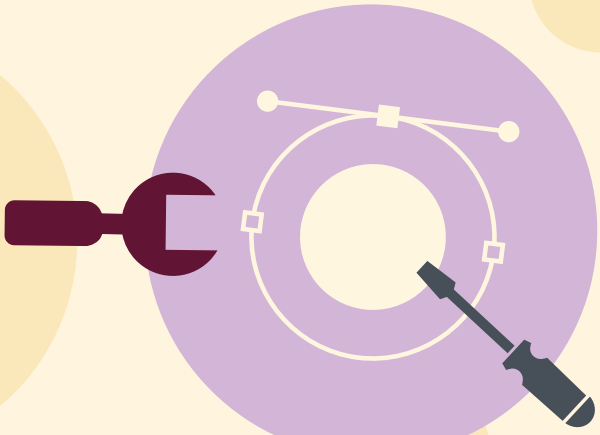
Rozdíly identifikované v rámci analýzy stávajícího stavu zpracování osobních údajů budou sloučeny do homogenních skupin, které budou představovat zadání projektu jehož cílem bude eliminace rozdílů. Na základě tohoto zadání budou zpracovány kroky, které je pro eliminaci rozdílů nutné provést a budou rovněž odhadnuty délky trvání jejich eliminace. Takto zpracované projektové záměry bude možné využít i jako zadávací dokumentaci. Ne všechny rozdíly však bude možné eliminovat (např. z důvodu časové nebo finanční náročnosti). Tyto rozdíly budou identifikovány jako tzv. reziduální rizika, které se organizace rozhodla akceptovat.

C Implementační harmonogram

Jednotlivé projektové záměry budou obsahově tvořit ucelený projektový program. Časové závislosti mezi jednotlivými projektovými záměry budou zachyceny formou implementačního harmonogramu.

Výstup

Jednotlivé projektové záměry budou obsahově tvořit ucelený projektový program. Časové závislosti mezi jednotlivými projektovými záměry budou zachyceny formou implementačního harmonogramu.



4. Realizace projektových záměrů

Cíl:

- Zabezpečit realizaci jednotlivých projektových záměrů a tím zajistit shodu s GDPR

Náš přístup

Realizace projektových záměrů je souhrn specifických řídících a odborných činností, které budou pro každou organizaci jiné, a které vyplývají z typů realizovaných projektových záměrů. Bez naplnění výše popsaných kroků nelze odhadnout ani jejich délku trvání, ani náklady na tyto činnosti.

Mezi tyto specifické řídící a odborné činnosti typicky patří:

- Zpracování dokumentu posouzení vlivu zpracování na ochranu osobních údajů dle § 35 odst. 1 GDPR, v souladu s požadavky stanovenými v § 31 odst. 7 a 8 GDPR;
- zabezpečení projektového řízení a podpory při realizaci projektových záměrů včetně řízení externích dodavatelů;
- zabezpečení technického dohledu nad implementací bezpečnostních opatření;
- zabezpečení technického dohledu nad revizemi ICT a bezpečnostní architektury;
- zajištění kapacit pověřence osobních údajů.

Všechny výše uvedené činnosti spolu s realizací vybraných projektových záměrů (typicky revize smluv, revize produktů, procesní změny) je možné zajisti rovněž externími kapacitami, které tímto náš expertní tým nabízí.

Výstup

Projektový záměr definující rozsah, harmonogram a rozpočet, který bude sloužit i jako nabídka našeho expertního týmu.