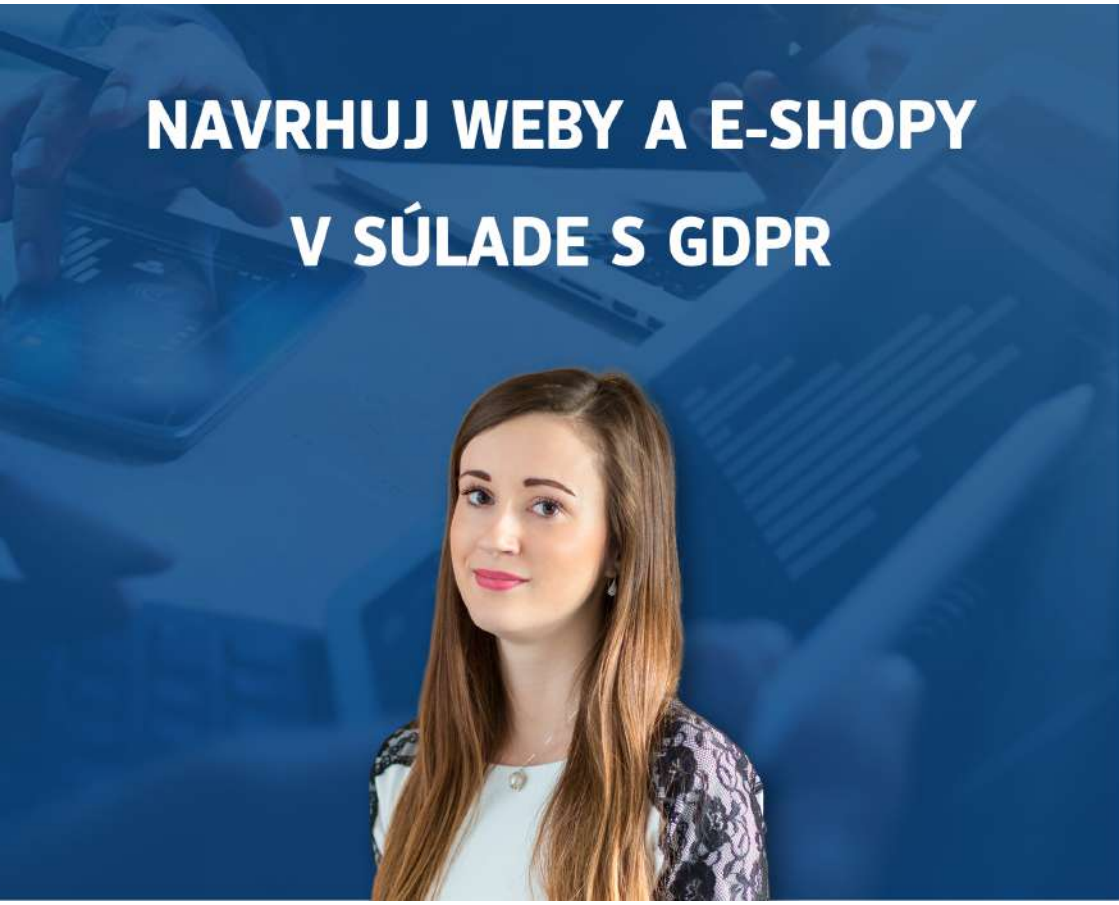
positive

Workshop o GDPR v online prostredí



Mgr. Natália Hučková, Positive Corporate Attorney

positive

Financial Report
www.finreport.sk

UP

študentský parlament elektrotechnikov a informatikov

ZÁKLADNÉ KROKY IMPLEMENTÁCIE GDPR

1. Účel spracúvania osobných údajov

V prvom rade urči, za akým účelom budeš osobné údaje spracúvať. V rámci webovej stránky či e-shopu je potrebné určiť každý účel samostatne. Preskúmaj teda, v ktorých častiach webu či e-shopu získavaš alebo inak spracúvaš osobné údaje. Napríklad pri kontaktnom formulári je účelom zaistenie komunikácie, poskytovanie informácií, vybavovanie podnetov a pododobne.

2. Právny základ

Po tom, ako si zistil, pri ktorých situáciách dochádza k spracúvaniu osobných údajov, urči pre každú z týchto činností samostatný právny základ.

Právnym základom môže byť:
a. súhlas
b. plnenie zmluvy
c. osobitný právny predpis
d. ochrana životne dôležitých záujmov
e. plnenie úlohy vo verejnom záujme
f. oprávnený záujem prevádzkovateľa

Napríklad pri kontaktnom formulári môže byť právnym základom oprávnený záujem prevádzkovateľa. Určenie právneho základu je veľmi dôležité, no v praxi často problematické. Odporúčame ti preto, aby si sa vopred poradil s odborníkom.

3. Rozsah osobných údajov

Pred spracúvaním osobných údajov urči, ktoré osobné údaje nevyhnutne potrebuješ pre dosiahnutie stanoveného účelu (bod 1). Zároveň zohľadni zásadu minimalizácie údajov. Ostatné údaje nezískavaj a prípadne, ak ich už máš vo svojej databáze, údaje anonymizuj (alebo vymaž). Napríklad pre kontaktný formulár by malo postačovať získavanie mena, priezviska, e-mailu či telefónneho čísla.

4. Doba spracúvania

Následne je potrebné určiť primeranú dobu uchovávania. Pokiaľ jej stanovenie nevyplýva z osobitného právneho predpisu, určuješ ju ty ako prevádzkovateľ. Primeranosť možno chápať tak, že dotknutá osoba v danom čase očakáva, že jej osobné údaje budú spracúvané. Zároveň neopomeň nastaviť mechanizmus, ktorý ti notifikuje blížiace sa uplynutie lehoty alebo automaticky uskutoční výmaz. Napríklad v prípade kontaktného formulára sa ako primeraná javí lehota do 1 roka.

5. Príjemcovia a sprostredkovateľ

Preskúmaj, či pri spracúvaní údajov na daný účel využívaš služby nejakého dodávateľa a či on sám vykonáva spracúvanie v tvojom mene. V takom prípade je nevyhnutné uzatvoriť

s ním zmluvu o spracúvaní osobných údajov podľa GDPR. Ak však má k týmto osobným údajom prístup len príležitostne, postačuje zaviazať ho mlčanlivosťou. Nezabudni, že už len samotné uchovávanie osobných údajov sa považuje za spracúvanie. Napríklad v prípade kontaktného formulára môže byť sprostredkovateľom poskytovateľ hostingu.

6. Prenos osobných údajov

Dôležité je aj posúdiť, či neuskutočňuješ prenos týchto osobných údajov do tretej krajiny. Treťou krajinou je každý nečlenský štát EÚ. Ak áno, následne na stránke Úradu na ochranu osobných údajov zisti, či takáto krajina poskytuje záruku primeranej ochrany, prípadne či spoločnosť, ktorej takéto osobné údaje prenášaš, je v režime Privacy Shield.

7. Práva dotknutej osoby

Už pred začatím spracúvania údajov na stanovený účel si premysli, akým spôsobom bude umožnený výkon práv dotknutých osôb. Napríklad, či ti štruktúra databázy osobných údajov umožňuje realizovať právo na zabudnutie, prípadne, akou formou budeš realizovať prenos údajov do databázy iného prevádzkovateľa. Čo patrí k právam dotknutej osoby?

- právo na informácie
- právo na prístup k údajom
- právo na opravu
- právo na vymazanie („zabudnutie“)
- právo na obmedzenie spracúvania
- právo na prenosnosť
- právo namietať

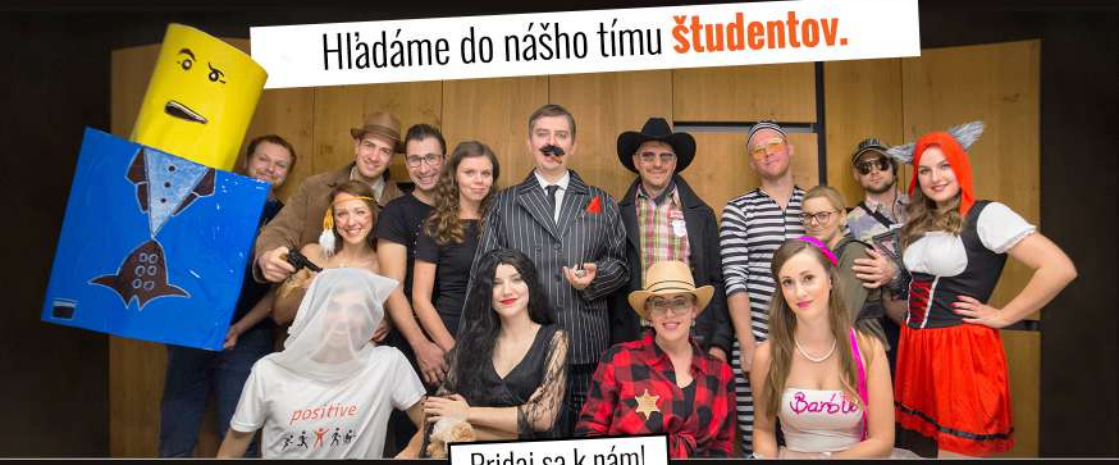
8. Odhalenie bezpečnostného incidentu

Prijmi také opatrenia, ktoré zaistia primeranú úroveň ochrany. V prípade, ak by i napriek ich prijatiu došlo k vzniku bezpečnostného incidentu, prijaté opatrenia by ti mali umožniť jeho okamžité zistenie. GDPR v niektorých prípadoch zároveň vyžaduje, aby porušenie ochrany osobných údajov bolo do 72 hodín oznámené Úradu na ochranu osobných údajov. Vo veľmi závažných prípadoch porušenia ochrany osobných údajov si povinný informovať aj dotknuté osoby.

9. Aktualizácia dokumentácie

Po tom, ako posúdiš všetky vyššie uvedené náležitosti, aktualizuj svoju bezpečnostnú dokumentáciu o túto novú spracovateľskú operáciu. Aktualizuj najmä záznamy o spracovateľských činnostiach. Ak si dosiaľ nebol povinný prijať DPIA, preskúmaj, či ti povinnosť jeho prijatia nevznikla pri tejto novej spracovateľskej operácii.

BUĎ SÁM SEBOU,
BUĎ POSITIVE.



UI / UX WEB DESIGNER

PHP PROGRAMÁTOR

UI / UX WEB DEVELOPER

positive software s.r.o.
www.positive.sk/joby

kariera@positive.sk
+421 903 012 102

SLOVNÍK

Anonymizácia

Proces, ktorý znemožňuje identifikáciu dotknutej osoby. Anonymizáciu je potrebné odlišovať od výmazu osobných údajov či pseudonymizácie. Anonymizácia je nenávratný proces. Prostredníctvom nej dochádza k situácii, kedy osobné údaje nie je možné priradiť k určitej konkrétnej osobe.

Bezpečnostný incident

Akékoľvek porušenie ochrany osobných údajov. Ide o také porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

Dotknutá osoba

Každá fyzická osoba, ktorej osobné údaje sa spracúvajú. Za určitých okolností sa ochrana poskytuje aj údajom charakterizujúcim fyzickú osobu podnikateľa. V takom prípade je dotknutou osobou aj fyzická osoba – podnikateľ.

DPIA

Posúdenie vplyvu na ochranu osobných údajov (Data protection impact assessment) predstavuje jeden z dokumentov tvoriacich bezpečnostnú dokumentáciu podľa GDPR. Jeho spracovanie sa nevzťahuje na každého prevádzkovateľa, je však potrebné napríklad v prípade, ak v rámci hlavnej činnosti prevádzkovateľa dochádza k spracúvaniu údajov o zdraví vo veľkom rozsahu.

Informačný systém

Akýkoľvek usporiadaný súbor osobných údajov. Takýto súbor údajov nemusí byť automatizovaný. Nejde teda len o softvérové riešenia alebo elektronické databázy. Môže ísť o listinnú zmluvnú dokumentáciu, evidenciu objednávok, knihu návštev.

Osobitný právny predpis

Zákon. Na účely spracúvania osobných údajov a stanovenia právnych základov ním môže byť napríklad Zákonník práce, Školský zákon, zákon o finančnom sprostredkovaní a finančnom poradenstve a pod.

Osobitná kategória osobných údajov

Osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia, alebo sexuálnej orientácie a sexuálneho života.

SLOVNÍK

Osobný údaj
Akýkoľvek údaj, ktorý vedie, alebo by mohol viesť, k identifikácii fyzickej (dotknutej) osoby. Napríklad meno, priezvisko, dátum narodenia, rodné číslo, a iné. Avšak aj údaje ako cookies a IP adresa môžu byť za určitých okolností osobným údajom.

Prevádzkovateľ
Každý, kto určil účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene. Môže ním byť napríklad obchodná spoločnosť, škola, nemocnica, prevádzkovateľ e-shopu, či orgán verejnej správy.

Príjemca
Každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou. Môže ním byť napríklad poskytovateľ hostingu, externý mzdový účtovník, ale za určitých okolností aj kuriér, ktorý doručuje tovar z e-shopu.

Pseudonymizácia
Proces, pri ktorom dochádza k takej úprave osobných údajov, v dôsledku ktorej nie je bez poskytnutia ďalších informácií (napr. určitého kľúča) možné identifikovať konkrétnu osobu. Pseudonymizáciu je potrebné odlišovať od anonymizácie osobných údajov.

Režim Privacy Shield
Ide o zoznam spoločností so sídlom v USA, vo vzťahu ku ktorým je možné realizovať prenos osobných údajov za rovnakých podmienok, ako v prípade prenosu osobných údajov do tretej krajiny zabezpečujúcej primeranú úroveň ochrany. Zoznam takýchto spoločností je prístupný na www.privacyshield.gov/list.

Spracúvanie osobných údajov
Operácia alebo súbor operácií s osobnými údajmi. Ide napríklad o získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmenu, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením, vymazanie alebo likvidácia a iné spracovateľské operácie.

Sprostredkovateľ
Každý, kto spracúva osobné údaje v mene prevádzkovateľa (napr. externý mzdový účtovník, poskytovateľ hostingu, dopravca zabezpečujúci dodanie tovaru z e-shopu). Jedná sa o subjekt, ktorý na účely riadneho poskytovania služieb prevádzkovateľovi potrebuje spracúvať osobné údaje, ktoré sú v pôsobnosti prevádzkovateľa.

Tretia krajina
Štát mimo rámca Európskej únie (nečlenský štát EÚ).

Záruka primeranej ochrany
Zatiaľ čo voľný pohyb osobných údajov v rámci EÚ GDPR zaručuje, prenos do tretích krajín musí spĺňať stanovené kritériá a vyžaduje prijatie dostatočných záruk. Komisia EÚ však určila, ktoré z nečlenských štátov EÚ poskytujú garanciu záruky primeranej ochrany osobných údajov na rovnakej úrovni ako členské štáty EÚ. Pri týchto krajinách sa realizuje prenos osobných údajov rovnako, ako by sa jednalo o členský štát. Ich zoznam nájdeš na webovej stránke Úradu na ochranu osobných údajov SR.

Zásada minimalizácie údajov
Vyžaduje, aby boli spracúvané len také osobné údaje, ktoré sú nevyhnutné pre dosiahnutie stanoveného účelu spracúvania.

Záznamy o spracovateľských činnostiach
Dokument, ktorého spracovanie vyžaduje GDPR. Vymedzuješ v ňom účel spracúvania, právny základ, kategórie dotknutých osôb, či osobných údajov, a ostatné v GDPR stanovené náležitosti. Na webovej stránke Úradu na ochranu osobných údajov nájdeš aj vzor, ktorého sa môžeš pridržiavať. Záznam nikam nezasielaš, ponechávaš si ho u seba, no si povinný ho viesť a v prípade kontroly povinný ho predložiť.

Zmluva o spracúvaní osobných údajov
Upravuje vzťah medzi prevádzkovateľom a sprostredkovateľom a vymedzuje ich vzájomné práva a povinnosti. Takáto zmluva musí obsahovať náležitosti vymedzené v čl. 28 GDPR.

Myslíte si, že vás sa GDPR netýka?

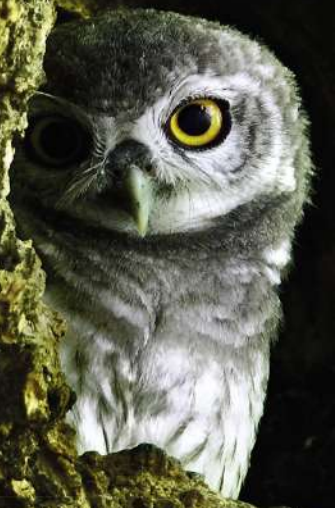
Likvidačnej pokute predchádzajú výroky:

„Nás sa GDPR netýka,
veď predsa zákazník si vypĺňa údaje sám,
pretože to potrebuje on."

„GDPR v podstate nič nemení!"

„Naša spoločnosť by predsa
vedome nezneužila osobné údaje."

„A to sa vážne týka aj zamestnancov,
PFA a tipérov?"



Múdro a spoľahlivo vám poradíme s problematikou GDPR, obráťte sa na nás.

positive

www.gdprnariadenie.eu
gdpr@positive.sk
+421 903 012 102
Positive Services s.r.o.