APSi > GDPR

GDPR

General Data Protection Regulation (GDPR) je nařízení Evropského parlamentu a Rady EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Bylo přijato v dubnu letošního roku, je závazné pro všechny členské státy a vejde v platnost 25. května 2018.

Cílem tohoto nařízení je hájit práva občanů proti neoprávněnému zacházení s jejich citlivými daty a osobními údaji. Tato pravidla respektují právo na ochranu osobních údajů občanů bez ohledu na jejich státní příslušnost nebo bydliště.

Základní pojmy dle GDPR

Co jsou osobní údaje?

Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“).

Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat,

zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje,

síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Koho se GDPR týká

Ochrana se týká zpracování osobních údajů fyzických osob. Vztahuje se jak na automatizované, tak manuální zpracování osobních údajů, pokud jsou údaje uloženy v evidenci nebo do ní mají být uloženy.

Zásady ochrany údajů se vztahují na všechny informace týkající se identifikované nebo identifikovatelné fyzické osoby.

Nařízení platí pro firmy, instituce i jednotlivce ze všech odvětví, které zacházejí s osobními údaji zaměstnanců, zákazníků, klientů či dodavatelů.

GDPR se rovněž věnuje ochraně digitálních práv občanů a zahrnuje i subjekty, které sledují či analyzují chování uživatelů na webu.

V případě závažného porušení mohou firmám hrozit vysoké pokuty.

Jaké zásadní změny GDPR přinese

Občané získají právo na výmaz údajů a jeho rozšíření na právo být zapomenut, tzn. správce musí v takovém případě všechny osobní údaje vymazat, pokud neexistuje právní důvod pro jejich další zpracování.

Občanům musí být umožněn přístup k údajům, které jsou o nich shromažďovány.

Občané budou mít právo vznést námitku proti zpracování osobních údajů, na jejímž základě nebude moci správce údaje dále zpracovávat, nebude-li k tomu mít prokazatelné důvody.

Osobními údaji se rozumí všechny (i technické údaje) jako e-mail, IP adresa nebo soubory cookies v zařízení uživatele. Dále také genetické a biometrické údaje.

Povinnosti ukládaní institucím a firmám

Nařízení rozšiřuje a upřesňuje stávající právní normy o ochraně a zabezpečení osobních údajů. Základní principy se tedy nemění, nově však podnikatelům vznikají tyto povinnosti:

- zpracovávat osobní data pouze k oprávněným účelům a jen po nezbytně nutnou dobu
- zabezpečit osobní data před neoprávněnými osobami
- zajistit ohlašovací povinnost v případě zjištění úniku dat
- poskytnout subjektům údajů právo na výpis, výmaz (zapomenutí) a přenositelnost.
- vést záznamy o zpracování osobních údajů, spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit
- vypracovat posouzení vlivu na ochranu osobních údajů (DPIA)
- ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a subjektům údajů
- ustavit v některých případech pověřence pro ochranu osobních údajů (DPO)

GDPR a APSi.

Nařízení GDPR nestanovuje žádné podmínky pro nakládání s daty na technické úrovni jako šifrování nebo jiná specifická opatření.
Naopak, při stanovení povinnosti správce a zpracovatele zabezpečit osobní údaje, se obecné nařízení výslovně dovolává ohledu na stav techniky, náklady na přijetí a provedení jednotlivých technických a organizačních opatření k zabezpečení osobních údajů, povaze, rozsahu, kontextu a účelům samotného zpracování a také k pravděpodobným rizikům pro práva a svobody, jež s sebou zpracování nese. Vlastní povinnost pak zahrnuje zavedení vhodných technických a organizačních opatření a začlenění do zpracování nezbytných záruk, a to jak v době určení prostředků pro

zpracování, tak v době vlastního zpracování. Šifrování je uvedeno jako jedno z vhodných opatření („případně včetně /…/ šifrování osobních údajů“). Při posuzování úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům.

APSi tedy nelze chápat jako garanta ochrany údajů ale jako pomocníka při jejich evidenci a zpracování.

Úkoly GDPR řešené v APSi

Do programu byla nově přidána evidence důvodů (účelů) zpracování osobních údajů subjektů evidovaných v adresáři APSi. Tedy zákazníků, potenciálních zákazníků a dodavatelů.

Nová agenda umožňuje definovat jednotlivé důvody (účely) za jakými osobní údaje v systému zpracováváte a stanovit do kdy tyto důvody trvají. APSi definuje 5 základních důvodů a umožní definovat mnoho dalších podle povahy činnosti Vaší firmy.

Automatizované zpracování.

V APSi automaticky existuje důvod zpracování s názvem „Obchodní smlouva“. Ten plyne ze splnění právní povinnosti při uzavírání obchodu se zákazníky i dodavateli.

Program sám sleduje, jaké doklady vystavujete jednotlivým subjektům, a automaticky generuje v evidenci tento účel či stanovuje dobu konce jeho platnosti podle nastavení příslušných parametrů.

Evidence požadavků a incidentů

Pro každý evidovaný účel zpracování u každého subjektu Vám program nabídne i související evidenci různých změn. Tento nástroj vám efektivně umožní evidovat požadavky ze strany vašich klientů, např. na výmaz, přenositelnost a jiné, které GDPR přináší.

Díky této evidenci budete mít přehled jednotlivých úkonů a jejich stavu k dispozici na jednom místě.

Vše pod kontrolou

APSi Vám nabídne přehledné sestavy o tom, zda máte právo daná osobní data držet nebo už nemáte platný účel zpracování.

Kdykoli tak budete vědět, zda daný subjekt máte požádat a prodloužení souhlasu nebo zda musíte data anonymizovat nebo vymazat.

Omezení přístupu

Program již od svého počátku podporuje nastavení přístupových práv k různým agendám a jejich údajům. Jste schopni definovat kdo má do jaké agendy přístup a tím omezit přístup k osobním údajům.

Nově bylo zavedeno omezení na obecné i speciální exporty dat z databáze a přístup k přehledům.

Právo subjektu na přístup k osobním údajům a na jejich přenositelnost

Pro splnění této povinnosti přináší APSi novou možnost exportovat všechny údaje které o osobě evidujete ve strojově čitelném formátu.

GDPR přesně nedefinuje podobu souborů, nicméně APSi umožňuje data exportovat v nejrozšířenějším multiplatformním formátu XML.

Právo na opravu

Je již dnes standardní funkcí systému. Změnou dat v adresáři se změna projeví při dalším použití napříč systémem.

Pokud potřebujete provést změny i zpětně je umožněno opravit již existující doklady.

Uvádění vazby na adresář není na dokladech (fakturách, objednávkách, nabídkách atd.) povinné, údaje o subjektu lze zadat přímo na dokladu, přesto jej doporučujeme uvádět.

Velmi se tak zjednoduší dohledávání dat právě za účelem opravy nebo sdělení evidovaných údajů.

Právo na výmaz

Výmaz údajů je také standardní funkcí APSi. Nicméně do budoucna připravíme novou funkci, která vám umožní provést výmaz nebo anonymizaci údajů automaticky a napříč celým systémem.

Tato funkce zohlední i ostatní účely zpracování a vždy odstraní jen ty osobní údaje, kde již není platný účel zpracování.

Bezpečnost

K ochraně databáze doporučujeme použít jakýkoli z běžně dostupných nástrojů pro zabazpečení přístupu ke složkám a souborům v lokálních sítích.

O řešení požádejte dodavatele nebo správce vašich serverů a sítě.

Zálohy vytvářené programem APSi jsou již nyní automaticky chráněny heslem aby si je nikdo nepovolaný nemohl obnovit . Používáte-li k zálohování jiné nástroje, doporučujeme nastavit u nich podobnou ochranu.

Další informace o GDPR

Vymezení pojmů jako DPO nebo DPIA, kdo je subjekt údajů, správce osobních údajů, zpracovatel osobních údajů a další pokyny naleznete v přehledné formě na stránkách „Úřadu pro ochranu osobních údajů“ na adrese www.uoou.cz

Váš tým APSi