GDPR (General Data Protection Regulation) alebo všeobecné nariadenie na ochranu osobných údajov. Ide o nariadenie Európskej únie, ktoré upravuje a nahrádza doterajší zákon o ochrane osobných údajov.

Ochrana fyzických osôb v súvislosti so spracovávaním osobných údajov patrí medzi základné ľudské práva. Najdôležitejší je rešpekt súkromného a rodinného života či uchovávanie citlivých informácií o ostatných.

Naša spoločnosť Vám ponúka poradenské služby v oblasti ochrany osobných údajov a ochrany informačných systémov. Súčasťou týchto služieb je aj vypracovanie nevyhnutnej, zákonom požadovanej dokumentácie.

Jedno z podstatných rozhodnutí pri riadení Vašej spoločnosti je aj rozhodnutie ako zabezpečiť ochranu spracovávaných osobných údajov vo Vašich informačných systémoch.

Tvorba bezpečnostného projektu je náročný proces, v ktorom je potrebné zmapovať interné prostredie Vašej organizácie, identifikovať spracúvané osobné údaje a zhodnotiť a navrhnúť spôsoby ich ochrany. Organizácie si často neuvedomujú, že Zákon o ochrane osobných údajov sa nevzťahuje len na osobné údaje spracúvané v počítačových systémoch, ale aj na osobné údaje uložené v kartotékach, alebo spracúvané iba v papierovej podobe. Častým dôsledkom tvorby dobrého bezpečnostného projektu sú úpravy v IT prostredí organizácie. Z tohto pohľadu je výhodou vypracovať bezpečnostný projekt v rámci tvorby systému manažmentu informačnej bezpečnosti.

Skupiny užívateľov

GDPR sa nejakým spôsobom týka skoro všetkých. Každého sa ale týka v inom rozsahu, primerane tomu, akým spôsobom osobné dáta spracováva. Pre ľahšiu orientáciu sme vytvorili 6 základných skupín užívateľov a k nim aj zodpovedajúce odporúčania, na čo sa pre splnenie GDPR povinností zamerať**.**

Skupina	**Osobné údaje nemám**	Cena
1	Všetci, ktorí osobné údaje neukladajú. (S výnimkou údajov pre rýdzo osobnú potrebu.) Spadá sem väčšina ľudí-nepodnikateľov, výnimočne aj niektorí podnikatelia.	Cena dohodou
Skupina	**Osobné údaje ukladám, ale ďalej ich nespracúvam**	
2	Mnoho malých živnostníkov, typicky vykonávajúcich svoju činnosť osobne, buď u zákazníka alebo "v teréne". Aj tak by ale mali dodržiavať základné pravidlá zabezpečenie svojich dát, a to nielen kvôli GDPR. Remeselníci, kaderníčka, podnikatelia v službách ...	120- 200,- Eur v závislosti na rozsahu spracovanej dokumentácie
Skupina	**Osobné údaje mám, zpracovávám, ale nikomu sa nezasielajú**	
3	Živnostníci, firmy, ale aj rôzne záujmové spolky. Či už ide o dáta zamestnancov, členov, klientov alebo obchodných partnerov, jedná sa o spracovanie osobných údajov. V takom prípade už treba dbať na zabezpečenie systémov a tiež zabezpečiť, aby mali prístup len oprávnené osoby. Podľa rozsahu je potom potrebné vhodne zvoliť spôsob, akým budú o spracúvaní dát ľudia informovaní a akým spôsobom budú zabezpečené ich práva. Výnimku pre odovzdávanie tvoria externé účtovné a daňové firmy, štátne inštitúcie a podobne, pretože takéto odovzdávanie slúži na splnenie zákonných povinností. Drobné firmy so zamestnancami, malé e-shopy, všetci, ktorí majú web s registráciou ...	200-550,- Eur v závislosti na rozsahu spracovanej dokumentácie

Skupina	**Osobné údaje mám, zpracovávám a odovzdávam ďalším**	
4	Jedna z najväčších skupín - sem spadajú predovšetkým firmy, ktoré využívajú online marketing, či už cielenej reklamy, alebo pomocou Google Analytics. Najmä u webových služieb je potrebné dbať na správne informovanie návštevníka o spracovaní a postúpení jeho údajov ďalším subjektom. Pre väčší rozsah spracovaných údajov je vhodné zvoliť online riešenia, takže v tejto kategórii bude často potrebná úprava webov a systémov. Väčšia e-shopy s cielenou reklamou, rôzne výrobné firmy s externými dodávateľmi, firmy využívajúce cloudové služby	500-900,- Eur v závislosti na rozsahu spracovanej dokumentácie
Skupina	**Osobné údaje zpracovávám pre niekoho iného**	
5	Analytické a marketingové spoločnosti, pre ktorých je spracovávanie osobných údajov súčasťou ponuky ďalším firmám. Je potrebné dbať na vyššiu opatrnosť. V tomto prípade sa veľmi odporúča dôkladná analýza IT riešení. Je tiež dôležité s obchodnými partnermi správne zmluvne zabezpečiť rozdelenie zodpovednosti za spracovávané dáta. Je v záujme takejto firmy, aby mala veľmi dobre ošetrený celý proces prenosu a spracovania dát. Nielen kvôli GDPR, ale aj preto, aby bola dôveryhodným obchodným partnerom. Online služby ponúkajúce rozosielanie newsletterov, analytici na voľnej nohe, marketéri na voľnej nohe aj agentúry	Cena bude stanovená individuálne v závislosti na rozsahu spracovanej dokumentácie
Skupina	**Predstavujem vysoké riziko úniku či zneužitiu osobných údajov**	
6	Patrí sem celá štátna správa, ale aj korporáty zo sféry biznisu. V tomto prípade už treba individuálny prístup. Pre splnenie GDPR povinnosťou je potrebné spracovať DPIA (posúdenie vplyvu na spracovanie osobných údajov) a nechať preveriť povinnosť zriadenia DPO (určiť zodpovednú osobu). Štátna správa, obce, nemocnice, banky, poisťovne, bezpečnostné agentúry, call centrá ...	Cena bude stanovená individuálne v závislosti na rozsahu spracovanej dokumentácie

Pozn.:
Toto rozdelenie bolo navrhnuté našou spoločnosťou len pre lepšiu orientáciu v GDPR. V žiadnom prípade nie je oficiálnym rozdelením podľa nariadenia GDPR. Uvedené odporúčania nie sú vyčerpávajúce a sú zamýšľaná pre typické všeobecné prípady, kedy v individuálnych prípadoch sa môžu povinnosti dotknutých subjektov odlišovať. Odporúčania nepredstavujú akékoľvek právne stanovisko a nemôžu nahradiť individuálne posúdenie zo strany právnych a iných špecializovaných poradcov, ktorí sa zameriavajú na GDPR

Rozsah a riziko

Ako veľmi to mám všetko brať vážne?
U každej skupín užívateľov stanovujeme navyše orientačný údaj o rozsahu spracúvaných údajov a riziku prípadných postihov. Podľa množstva spracúvaných údajov, veľkosti a obratu firmy stanovujeme 3 základné rozsahy:

- malý
- stredná
- veľký

1. U malého rozsahu je veľmi pravdepodobné, že bude stačiť splniť základné povinnosti vlastnými silami čiže sedliackym rozumom. Aj tak je ale vhodné sa zamyslieť nad odporúčaniami, ktoré pre danú skupín užívateľov odporúčame. Už len preto, že každá firma môže raz vyrásť.
2. Stredný rozsah spracovania sa bude týkať väčšiny malých a stredných firiem, najmä e-shopov. Väčšinu povinností je možné splniť vlastnými silami.
3. U veľkého rozsahu už odporúčame individuálne posúdenie a prípadné využitie právnych a IT služieb.

Čo ponúkame

- **Ponúkame Vám vypracovanie kompletného bezpečnostného projektu v zmysle zákona č.18/2018 Zz.**
- **Aktualizáciu (zosúladenie) projektov so zákonom o OOU č. 18/2018 Z.z.**
- **Aktualizáciu bezpečnostného projektu pri zmene v spracúvaní osobných údajov.**

Spracovanie Bezpečnostného projektu

Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Na tento účel je za podmienok ustanovených v zákone č. 18/2018 Z. z. o ochrane osobných údajov v znení neskorších predpisov povinný prijať bezpečnostné opatrenia. Bezpečnostný projekt musí byť vypracovaný s ohľadom na konkrétne podmienky spracúvania osobných údajov, ktoré i z hľadiska personálneho, technického, organizačného, finančného vybavenia sú u každého prevádzkovateľa špecifické, teda iné.
Teda každý bezpečnostný projekt je jedinečný dokument, závislý na konkrétnych podmienkach a spôsobu spracovania osobných údajov. Pri jeho spracovaní sa prihliada na konkrétne okolnosti daného informačného systému v oblasti fyzickej-objektovej, personálnej a informačnej bezpečnosti.

Cenu za spracovanie bezpečnostného projektu určuje jeho rozsah, pričom ten je daný počtom informačných systémov a náročnosťou informačných systémov ako aj súčasným stavom informačnej bezpečnosti vo Vašej spoločnosti.

Svojím klientom spracúvame bezpečnostné projekty v cenových reláciách od 200 €, kde v uvedenej cene pre Vás spracujeme:

- bezpečnostný projekt pre 2-3 informačné systémy,
- prijatie bezpečnostných opatrení,
- vypracovanie kompletných zmlúv pre prevádzkovateľa, sprostredkovateľa a pod,
- vypracovanie všetkých potrebných poučení pre oprávnené osoby dotknuté osoby a pod.
- v prípade kontrol a previerok vám bude z našej stany poskytnutá súčinnosť a pomoc

Uvedená cena a služby nie sú konečné a dajú sa upraviť na základe vzájomnej dohody.
Ak Vás naša ponuka zaujala radi sa s Vami stretneme pri osobnom kontakte.

GREP Plus spol. s r.o.
Roľnicka 10
831 07 Bratislava
Tel.: +421 902 930 120
info@grepplus.eu

Čo je GDPR ?...
čo by ste mali vedieť

Nové nariadenie Európskeho parlamentu a Rady EÚ so sebou prináša balíček zmien v oblasti ochrany osobných údajov. Nariadenie s názvom GDPR – General Data Protection Regulation vstúpi do platnosti 25. mája 2018.

Toto potrebujete vedieť!

1. **Koho sa zmena týka?** Nová legislatíva sa bude týkať všetkých podnikateľských subjektov, ktoré spracúvajú osobné údaje zamestnancov, zákazníkov alebo klientov. Takisto sa legislatívne zmeny dotknú aj sprostredkovateľov, akými sú účtovníci, právnici atd..
2. **Nová definícia osobných dát.** V rámci GDPR sa osobnými dátami stávajú údaje, ktoré vedú k identifikovaniu jednotlivca. Pre predstavu teda ide aj o údaje, ktoré sú prepojené s genetikou, duševným zdravím alebo sociálnou situáciou.
3. GDPR vyžaduje prísnejšie pravidlá pre získanie súhlasu so spracovaním osobných údajov. Nový zákon bude kontrolovať spôsob, akým organizácie komunikujú s klientom pri získavaní súhlasu o spracovaní a použití osobných údajov. GDPR tak bude vyžadovať použitie jednoduchého jazyka a takisto bude musieť byť zreteľne jasné, prečo daná firma osobné údaje potrebuje, ako ich bude spracovávať a taktiež ako s nimi bude nakladať.
4. Firmy a organizácie budú mať povinnosť určiť zodpovednú osobu. DPO – Data Protection Officer bude musieť byť pracovná pozícia, ktorá bude odborníkom na ochranu a spracovanie osobných údajov. Pozíciu okrem verejnej správy budú musieť obsadiť, respektíve dať do kompetencie osobe, zamestnancovi, ktorej pravidelnou činnosťou bude systematické monitorovanie a spracovanie osobných údajov.
5. Únik osobných údajov sa musí oznámiť. Nové nariadenie GDPR ukladá za povinnosť, aby firma či organizácia informovala úrad pre ochranu osobných údajov o úniku do 72 hodín po zistení. Firma musí zaistiť proces, ktorým umožní odhalenie úniku a jeho riešenie.
6. Právo byť vymazaný. Právo na výmaz je v znení i terajších platných zákonov. Tentoraz však ak používateľ požiada o výmaz údajov, poskytovateľ posúdi oprávnenosť žiadosti a následne po splnení podmienok užívateľa musí údaje vymazať. Následne však musí informovať i spracovávateľov, ktorí údaje spracovali, o ich odstránení.
7. GDPR žiada ochranu súkromia už v samotnom systéme. Ide teda o ochranu osobných údajov už v návrhu systému. Teda počiatočné fázy IT systémov pre spracovanie osobných dát musia vyhovovať samotným princípom ochrany.
8. Povinné PIA – Privacy Impact Assessment. Tento nástroj je definovaný ako spôsob, ktorým možno odhaliť dopad ochrany osobných údajov na súkromie klientov. Ide teda o preverenie rizík spojených s možným únikom osobných dát. Takto sa ešte v procese vývoja dá zistiť, ako účinný projekt je.
9. Jednotný prístup. Toto nariadenie sa dotýka každej spoločnosti a organizácie, ktorá podlieha úradu na ochranu osobných údajov, bez ohľadu na to, kde má sídlo.
10. Sprostredkovatelia budú mať prísnejšie pravidlá. Účtovné či právnické firmy, ktoré spracúvajú osobné údaje klientov, budú musieť splniť určité nové podmienky. Ako napríklad viesť zoznam spracovateľských operácií každého klienta alebo využívať šifrovanie a chránenú komunikáciu.
11. Spracúvanie údajov detských užívateľov. V tomto bode sa GDPR dotkne osôb mladších ako 16 rokov, kde sa pre spracovanie osobných údajov bude vyžadovať súhlas zákonného zástupcu (rozhranie API).
12. Pokuty budú vyššie! Za porušenie nariadení týkajúcich sa spracúvania osobných údajov hrozí pokuta až do výšky 20 000 000 eur, prípadne pokuty do výšky 4 % svetového ročného obratu za predchádzajúci účtovný rok.

Nadobudnutie účinnosti ?

Súbor ucelených pravidiel na ochranu dát nadobudne účinnosť 25.5.2018. Dotkne sa aj vás? V roku 2016 bolo GDPR schválené. Do 25. 5. 2018 musia všetci zrevidovať a zjednotiť informačné systémy a postupy pri práci s údajmi. Ich tok je v rámci Únie podporovaný a nariadenie zaručuje vysokú ochranu pred zneužitím citlivých informácií.

Aké budú sankcie?

Záleží hlavne na charaktere a závažnosti incidentu. Pokuty však môže dosiahnuť až 4 % z celkového obratu spoločnosti či 20 miliónov eur. Podľa toho, ktorá suma je vyššia.

Koho sa GDPR dotýka?

Každého, kto zhromažďuje a spracováva osobné údaje Európanov, vrátane spoločností a inštitúcií mimo EÚ, ktoré pôsobia na našom trhu. Nariadenie je platné pre firmy, inštitúcie, jednotlivcov – zamestnancov, zákazníkov, klientov aj dodávateľov naprieč všetkými odvetviami. Rovnako sa týka aj tých, ktorí analyzujú chovanie užívateľov webov a aplikácií.

V čom GDPR spočíva?

GDPR nahradí zákon o ochrane osobných údajov na SR. Cieľom je ochrana digitálneho práva všetkých občanov. Hlavým bodom je upravený spôsob spracovávania osobných údajov. Pri porušeniach hrozia vysoké pokuty.

Najvýznamnejšie povinnosti a zmeny:

• ustanovenie zodpovednej osoby,
• upravenie príslušnej dokumentácie podľa novej právnej úpravy,
• zmena súhlasu so spracovaním osobných údajov,
• likvidačné pokuty za porušenie povinností,

Kedy je potrebné stanoviť zodpovednú osobu?

Stanoviť zodpovednú osobu je potrebné pre:
• orgán verejnej moci a verejnoprávny subjekt,
• subjekty, ktorých hlavnou činnosťou sú spracovateľské operácie, ktoré si vyžadujú pravidelné monitorovanie osôb,
• subjekty, ktoré spracovávajú informácie, ktoré sa týkajú viny za trestné činy,

Hlavné zmeny a povinnosti, ktoré na vás čakajú a je potrebné ich zabezpečiť:

- pre stanovené subjekty ustanoviť zodpovednú osobu,
- upraviť, prispôsobiť príslušnú dokumentáciu podľa novej právnej úpravy,
- čakajú vás zmeny v oblasti súhlasu so spracúvaním osobných údajov,
- zavedenie likvidačných pokút za porušenie povinností (pokuty až do 20 miliónov eur),
- nové práva dotknutých osôb (napr. právo byť zabudnutý) ,
- viaceré nové povinnosti pre osoby spracúvajúce osobné údaje.