GDPR

nařízení č. 2016/679, obecné nařízení o ochraně osobních údajů

Tento dokument má za cíl shrnout rámcově základní informace k nařízení Evropského parlamentu a Rady č. 2016/679, obecné nařízení o ochraně osobních údajů, ze dne 27. dubna 2016 (dále jen „**GDPR**"), které vstoupilo v platnost všech členských státech Evropské unie dne 24. května 2016, a ve všech členských státech začne být přímo aplikovatelné od **25. května 2018.**

Co GDPR upravuje

GDPR se týká nakládání s osobními údaji a jejich zpracování všemi subjekty. Rozšiřuje a mění pravidla ochrany osobních údajů stanovená zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**ZOOÚ**"). GDPR se vztahuje jak na soukromé, tak veřejnoprávní subjekty, a to v celém svém rozsahu. Týká se tak jak HMP, MHMP a rovněž tak příslušných městských částí a ÚMČ.

Jednou ze zásadních změn GDPR, jsou podstatně vyšší sankce v případě jeho porušení, které bude možno uplatnit též vůči organizacím veřejné správy.

Povinnosti vyplývající z GDPR je nutné promítnout do všech procesů, dokumentů a informačních systémů zpracovávající či nakládajícími s osobními údaji.

MHMP, ÚMČ a MČ při zpracování osobních údajů v jejich působnosti vystupují jako správci osobních údajů na **všechna taková zpracování osobních údajů se nařízení GPDR bude vztahovat.**

Dopady GDPR

- **GDPR EXPLICITNĚ STANOVÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ**

zásada zákonnosti, korektnosti a transparentnosti

Všechna zpracování osobních údajů je tedy možno realizovat pouze na základě zákonných titulů, které musí být dostatečně specifické, korektní a transparentní.

zásada účelového omezení

Osobní údaje nutno zpracovávat pouze pro určité, výslovně vyjádřené a legitimní účely. Účel je stanoven určitě, jestliže je z jeho dikce jasné, jaká zpracování budou probíhat a lze tak posoudit jejich legitimitu, kterou se rozumí soulad účelu s právním řádem. Výslovně vyjádřený účel, který musí být stanoven a znám nejpozději při shromažďování osobních údajů, znamená povinnost tento účel sdělit subjektům údajů.

zásady minimalizace údajů

Zpracovávané údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

ZOOÚ již dříve zavedlo dostatečně přísný režim, na který bude kontinuálně navazováno, a který je zcela v souladu s nařízením GDPR. V této oblasti tedy není třeba se GDPR obávat. Nicméně bude zcela nezbytně nutné důsledně kontrolovat dodržování této zásady, která je jednou z nejdůležitějších zásad nařízení GDPR, a kterou je nezbytné vždy respektovat.

zásada přesnosti

Na základě této zásady je kterýkoli správce osobních údajů povinen sám opravovat údaje, o kterých zjistí, že nejsou přesné.

Rovněž tak musí řešit požadavky subjektů na opravu a případné další situace, při kterých se na základě vnějšího podnětu dozví o neaktuálnosti osobních údajů.

zásada omezení uložení

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektu po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány.

zásada integrity a důvěrnosti

Dle této zásady musí správci, zajistit, aby zpracovávané údaje byly chráněny před hrozbami vevnitř organizace (krádeže dat zaměstnanci, úniky způsobené špatným zacházením s daty apod.) i vně organizace (ochrana před kybernetickými útoky apod.). Tato zásada má své zhmotnění zejména v čl. 32 nařízení GDPR, ve kterém jsou uvedena konkrétní opatření pro splnění vhodné úrovně zabezpečení.

zásada odpovědnosti

Podle této zásady nese správce odpovědnost za dodržování všech výše uvedených principů. Nařízení GDPR pak přináší novinku, dle které musí být správce vždy schopen doložit, jak dodržování souladu s principy nařízení GDPR probíhá.

➢ GDPR STANOVÍ TITULY PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Jakékoliv zpracovávání osobních údajů bez existence alespoň jednoho z následujících titulů je protiprávním a postižitelným dle nařízení GDPR a ostatních právních předpisů. Tyto tituly jsou taxativně vymezeny v čl. 6 nařízení GDPR:

a) souhlas se zpracováním osobních údajů,
b) plnění smlouvy, plnění právní povinnosti,
c) životně důležitý zájem,
d) úkol ve veřejném zájmu nebo
e) výkon veřejné moci,
f) oprávněný zájem.

Pro potřeby MČ jsou zásadní tituly pro zpracování osobních údajů v rozsahu nezbytném pro **splnění právní povinnosti**, která se na správce vztahuje a pro **splnění úkolu prováděného ve veřejném zájmu** nebo **při výkonu veřejné moci**, kterým je správce pověřen.

Je třeba jednoznačně odlišovat rozdíl mezi povinností uloženou zákonem a oprávněným zpracováním na základě zákona. Např. dle ustanovení § 312 odst. 1 zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „ZP"), je zaměstnavatel oprávněn vést osobní spis zaměstnance, o právní povinnost se zde tedy nejedná.

Proti titulu plnění právní povinnosti stojí titul veřejného zájmu dle čl. 6 odst. 1 písm. e) nařízení GDPR. Analogicky jako v případě plnění právní povinnosti i veřejný zájem musí vycházet z práva členského státu či Evropské unie. Veřejný zájem však nemusí být právně konkrétně ustanoven (jako je tomu v případě zpracování na základě plnění právní povinnosti) a je typický pro správce, kteří jsou orgány veřejné moci.
V případě zpracování osobních údajů na základě veřejného zájmu bude ovšem třeba vždy důsledně posuzovat, kde má tento veřejný zájem hranice. Jelikož je třeba veřejný zájem vykládat vždy spíše restriktivně, je v každém případě vhodnější, aby bylo zpracování osobních údajů podloženo konkrétním zákonným ustanovením (v opačném případě by o konkrétních parametrech zpracování mohly vznikat pochybnosti).

Dalším relevantním titulem pro zpracování osobních údajů **je zpracování nezbytné pro splnění smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro **provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů**.

Osobní údaje lze taktéž zpracovávat **na základě souhlasu subjektu** se zpracováním jeho osobních údajů pro jeden či více konkrétních účelů. Souhlas se zpracováním osobních údajů je často nadužíván správci, kteří jsou oprávněni zpracovávat údaje na základě jiného titulu. Vyžadování souhlasu po subjektu, jehož údaje lze zpracovávat na základě jiných právních titulů, je dle názoru Úřadu pro ochranu osobních údajů (dále jen „**ÚOOÚ**") nadbytečné a matoucí.

Mimo výše uvedené nařízení GDPR obsahuje speciální úpravu pro **zpracování tzv. zvláštních kategorií osobních údajů**, což je pojem, který nahradil dříve užívaný termín „citlivé osobní údaje" obsažený v ZOOÚ. Jedná se však o ustálenou terminologii, kterou je při intepretaci nařízení GDPR nadále možné využívat.

➢ GDPR VYMEZUJE PRÁVA SUBJEKTŮ ZPRACOVÁVANÝCH ÚDAJŮ

a) **právo na informace o zpracování,**
b) **právo na přístup k osobním údajům,**
c) **právo na opravu, právo na výmaz,**
d) **právo na omezení zpracování,**
e) **právo na přenositelnost údajů,**
f) **právo vznést námitku,**
g) **právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování.**

Celá řada těchto práv byla obsažena již ve stávajícím ZOOÚ, nicméně nařízení stanoví nově správcům kratší lhůty pro umožnění výkonu těchto práv, neumožňuje jim za výkon těchto práv požadovat úplatu (pokud se nejedná o opakované či šikanózní návrhy) apod.

Mezi tzv. nová práva subjektů dle GDPR lze řadit právo na přenositelnost údajů, na základě kterého má subjekt právo získat údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.

A dále právo vznést námitku, které umožňuje subjektu údajů podat proti zpracování námitku v případě, kdy je toto zpracování prováděno na základě veřejného zájmu či oprávněného zájmu správce. V případě podání takové námitky není správce oprávněn osobní údaje dále zpracovávat, pokud neprokáže oprávněné důvody pro zpracování, které převažují nad zájmy subjektu údajů.

Posledním z práv subjektu údajů je právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování. Automatickým individuálním rozhodováním se přitom rozumí takové zpracování, které je prováděno bez zásahu lidského prvku, a které má právní účinky pro subjekt údajů nebo se ho obdobným způsobem významně dotýká.

Pro to, aby mohl správce umožnit výkon práv subjektů, je samozřejmě zcela nezbytné mít ve zpracování osobních údajů „pořádek", tj. **mít jednoznačně zmapovaná, evidovaná a dokumentovaná jednotlivá zpracování v rámci jednotlivých účelů**.

➢ GDPR MĚNÍ POVINNOSTI SPRÁVCŮ OSOBNÍCH ÚDAJŮ

GDPR upřesňuje postavení správce osobních údajů a ukládá mu celou řadu nových povinností. **Základní povinností správce je zavést v souvislosti se zpracováním osobních údajů taková technická a organizační opatření, která zajistí a umožní správci doložit, že zpracování je prováděno v souladu s nařízením GDPR.**

Správce by měl přijmout **vhodnou koncepci v oblasti ochrany osobních údajů**. Touto koncepcí rozumíme opatření ve směru dovnitř organizace, tedy zavedení interních pravidel a směrnic, které by řídily činnost, omezený přístup a nakládání s údaji zaměstnanci správce.
Veškerá opatření k ochraně osobních údajů a zajištění souladu správce s požadavky nařízení GDPR přitom bude nezbytné řádně dokladovat v **záznamech o činnostech zpracování**, vedených u správce, resp. případně i doložit ÚOOÚ. Obsahové náležitosti záznamů o činnostech zpracování prováděného správcem jsou uvedeny v čl. 30 odst. 1 nařízení GDPR.

Mezi nové povinnosti správce dle GDPR patří **povinnost hlásit případy porušení zabezpečení osobních údajů do 72 hodin ÚOOÚ**. Součástí ohlášení narušení musí být popis povahy daného případu narušení, popis pravděpodobných důsledků narušení, popis opatření přijatých či navržených s cílem vyřešit dané narušení apod. Tato nová povinnost si pravděpodobně vyžádá úpravu v procesech zpracování osobních údajů a související úpravu smluv s osobami poskytujícími služby podpory či provozu informačních systémů.

Správce bude konečně též povinen **zavést evidenci všech případů porušení zabezpečení**, kterou bude mimo jiné ve vztahu k ÚOOÚ dále dokládat řádné plnění ohlašovací povinnosti.

Další z nových povinností uložených nařízením GDPR správcům osobních údajů je **povinnost provést posouzení dopadů na ochranu osobních údajů**. Povinnost provést posouzení dopadů na ochranu osobních údajů má dle GDPR vést k usnadnění identifikace rizik, která by bez jeho posouzení mohla být přehlédnuta. Z úpravy čl. 35 nařízení GDPR lze dále usoudit, že se povinnost posuzování vlivu bude vztahovat až na ta zpracování, která budou zahájena po nabytí účinnosti nařízení GDPR. U stávajících zpracování je však vhodné provést identifikaci rizikových operací zpracování a připravit si tak základ pro případné požadavky na posouzení ze strany ÚOOÚ.

GDPR také upravuje postavení zpracovatele, když požaduje, aby správce využil pouze takové zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky GDPR a byla zajištěna ochrana práv subjektu údajů. GDPR též stanoví detailní požadavky na smlouvu o zpracování osobních údajů uzavíranou mezi správcem a zpracovatelem, a to v čl. 28 odst. 3 nařízení GDPR. Podobně jako správce je i zpracovatel povinen vést záznamy o činnostech zpracování, jejichž obsahové náležitosti jsou uvedeny v čl. 30 odst. 2 nařízení GDPR.

Konečně jednou ze zásadních novinek, které nařízení GDPR přináší, je zavedení **funkce pověřence pro ochranu osobních údajů** (dále také jen „pověřenec"). Pověřence budou povinny jmenovat orgány veřejné správy provádějící zpracování osobních údajů, popř. též další osoby provádějící zpracování ve velkém rozsahu.

Jako pověřenec přitom může být jmenována jak fyzická osoba, tak osoba právnická, což je vhodné zejména v případě velkých organizací provádějících rozsáhlá zpracování osobních údajů. Pověřenec má být styčným bodem mezi správcem (orgánem veřejné moci) a dozorovým úřadem; navíc i mezi správcem a subjekty osobních údajů, jejichž údaje orgán zpracovává. Ačkoliv samotné nařízení GDPR nijak nespecifikuje kvalifikační požadavky na funkci, pověřenec musí splňovat dostatečně profesní kvality, aby mohl svou funkci řádně vykonávat; musí tedy znát vnitrostátní i evropskou legislativu, která upravuje zpracovávání a nakládání s osobními údaji, doporučené je též technické vzdělání, které umožňuje plně porozumět a chápat technickoorganizační opatření, zavedené pro ochranu dat v rámci instituce. Přestože to tak není nezbytné, je vhodné pro osoby pověřence vybírat osoby s právním či technickým vzděláním.