Doporučení Ministerstva dopravy k implementaci Nařízení Evropského parlamentu a rady EU č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Verze 01.00

OBSAH

ÚVOD

Ministerstvo dopravy ČR v rámci své informační a metodické činnosti předkládá k využití materiály pro usnadnění zajišťování souladu s Nařízením Evropského parlamentu a rady EU č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „Nařízení GDPR“). Svou roli zprostředkovatele tématu GDPR pro organizace v působnosti Ministerstva dopravy ČR vnímáme v kontextu metodické podpory a dokumentů vydávaných zejména Ministerstvem vnitra ČR, Ministerstvem průmyslu a obchodu ČR a Úřadem pro ochranu osobních údajů.

Základními oblastmi, kterým se informační a metodický materiál věnuje, jsou:

I. Manažerské shrnutí
II. Zmapování zpracování osobních údajů
III. Analýza rizik a posouzení vlivu na ochranu osobních údajů
IV. Práva subjektů osobních údajů
V. Vztah správce – zpracovatel
VI. Inspirace k doplnění smluv se zpracovateli
VII. Zdroje informací k Nařízení GDPR

ČÁST I. MANAŽERSKÉ SHRNUTÍ

GDPR - o co se jedná?

Předně nejedná se o revoluci ve zpracování osobních údajů. Je zřetelná kontinuita s předchozí evropskou legislativou a návaznost na náš zákon č. 101/2000 Sb. o ochraně osobních údajů. Definice klíčových pojmů (osobní údaj, subjekt údajů, zpracování), zásady zpracování i povinnosti jsou obdobně formulované a obsahově velmi blízké. GDPR však reaguje na rychlý technologický pokrok a nové možnosti zpracování osobních údajů automatizovaným způsobem, kdy mohou být osobní údaje fyzických osob využity nebo i zneužity v měřítku, který může zásadně zasáhnout do života jim samotným nebo dokonce i celé společnosti.

Nařízení GDPR je podrobnější a přináší fyzickým osobám větší záruky i práva ve vztahu k jejich osobním údajům. Tato práva a záruky se odráží v nových a širších povinnostech pro organizace zpracovávající osobní údaje a v požadavcích na jejich zabezpečení.

Je důležité si uvědomit, že nařízení GDPR je obecné, vztahuje se na organizace různé velikosti a rozličného zaměření. Vztahuje se na ministerstva, kraje, malé obce, velké dopravce i jejich „malé“ dodavatele, včetně podnikatelů OSVČ zpracovávajících osobní údaje. Zároveň nebudou různé organizace čelit stejným rizikům a budou tedy přijímat rozdílná opatření k eliminaci rizik, právě ve vztahu ke svým specifickým podmínkám, možnostem a mj. dostupnosti zdrojů.

Proto nemůže existovat žádný univerzální kompletní seznam povinností a povinných opatření, která má organizace provést, aby dosáhla souladu s Nařízením GDPR.

Plnění požadavků GDPR musí umět prokázat každá organizace a mít zdokumentováno, že byla přijata opatření, která bylo možné realizovat a že systém ochrany osobních údajů v organizaci má jasný plán na další zlepšování.

Co jsou osobní údaje, subjekt údajů, správce a zpracovatel

Je třeba mít na zřeteli, že osobním údajem může být jakákoli informace o fyzické osobě, kterou dokážeme přiměřenými prostředky identifikovat, viz článek 4, odstavec 1) Nařízení GDPR.

Subjektem údajů je žijící fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba.

Správce osobních údajů je podle Nařízení GDPR každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování, viz článek 4, odstavec 7) Nařízení GDPR.

Zpracovatel osobních údajů je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který jménem správce zpracovává osobní údaje. Jinými slovy, v pozici

zpracovatele je každý, kdo má systematický a plánovaný a v důsledku toho často zasmluvněný přístup k osobním údajům správce, viz článek 4, odstavec 8) Nařízení GDPR.

Hlavní zásady

Prakticky je třeba uvést ve vaší organizaci v život zásady zpracování osobních údajů, které jsou uvedeny v článku 5 Nařízení GDPR:

- Omezení účelem - pro zpracování osobních údajů platí, že zpracování probíhá vždy za jasným účelem. Účel limituje, co všechno a jak dlouho můžeme zpracovávat.
- Korektnost a transparentnost - o zpracování osobních údajů musí být lidé, jejichž data zpracováváte, informovaní srozumitelným způsobem.
- Minimalizace údajů – máte zpracovávat jen údaje nezbytně potřebné pro stanovený účel a jen po nezbytně dlouho dobu. Nezpracováváte a neuchováváte data jen pro „strýčka Příhodu“.
- Přesnost - osobní údaje musejí být aktuální, máte povinnost údaje aktualizovat jednak na žádost těch, kterých se týkají, ale také aktivně ověřovat jejich platnost, případně je mazat.
- Zákonnost zpracování (viz dále).
- Integrita a důvěrnost, dostupnost (viz dále).

Kdy smíme osobní údaje zpracovávat

Osobní údaje smíme zpracovávat jen na základě zákonných důvodů. Nezákonné zpracování není dovoleno. Zákonnými důvody dle článku 6 Nařízení GDPR jsou:

- Souhlas se zpracováním pro jeden či více účelů – a to v případech, kdy není možné zpracovávat osobní údaje z jiných zákonných důvodů – viz následující body.
  U souhlasů se zpracováním musí být uveden účel zpracování, doba, na kterou se souhlas uděluje a jeho odvolání musí být stejně snadné jako jeho udělení.
- Plnění právní povinnosti – pokud vám ukládá zpracování osobních údajů zákon či vyhláška, nepotřebujete souhlas fyzické osoby se zpracováním.
- Plnění smlouvy se subjektem údajů – včetně zpracování, které předchází bezprostředně uzavření smlouvy, pokud vám osobní údaje poskytla sama fyzická osoba za účelem uzavření smlouvy – ani v tomto případě nepotřebujete souhlas osoby.
- Ochrana životně důležitých zájmů subjektu údajů.
- Veřejný zájem.
- Oprávněný zájem vaší organizace – různá práva mají být v rovnováze.
  Vedle práva na ochranu osobních údajů a na ochranu osobnosti (viz občanský zákoník č. 89/2012 Sb.) leží mj. právo na podnikání a další práva. Je dobré si

uvědomit, že žádné právo není absolutní. Tento institut oprávněného zájmu umožňuje zpracování osobních údajů, pokud organizace provede „balanční test“ a zdokumentuje, že převažuje oprávněný zájem organizace nad právem na soukromí a ochranu osobních údajů fyzické osoby. Takový oprávněný zájem může být například ochrana majetku, péče řádného hospodáře, ochrana před žalobami či soudními spory apod.

Zabezpečení osobních údajů

Nařízení GDPR vychází z principu založeného na hodnocení rizika. Požaduje zabezpečit důvěrnost, dostupnost, integritu a odolnost systémů, kde se osobní údaje nacházejí. Jinými slovy organizace ve vztahu ke svým specifickým podmínkám má zhodnotit rizika, kterým jsou osobní data vystavena a přijmout přiměřená opatření. Organizace má zabezpečit:

- integritu osobních údajů - aby jim mohla věřit (jsou aktuální a správné),
- důvěrnost osobních údajů - že k nim může jen ten, kdo je k tomu oprávněn,
- dostupnost osobních údajů - že se k datům organizace dostane, že nejsou ztracena, nevratně zašifrována apod.

Pro hodnocení rizik a uplatňování opatření lze využít různě komplexní metodiky. Rámec GDPR v oblasti zabezpečení osobních údajů byl vybudován na standardu rodiny ISO 27000 tedy především norem ISO 27001 a ISO 27002 - Systém managementu bezpečnosti informací (ISMS). Nicméně menší organizace zřejmě nevyužijí plnou šíři této normy a zhodnotí rizika své organizace způsobem, který odpovídá jejich složitosti, množství zpracovávaných osobních údajů, jejich citlivosti a dalším faktorům.

Na základě analýzy rizik organizace přijme vhodná opatření. V řadě případů nepůjde o finančně nebo procesně náročná opatření, ale může se jednat o fyzická zabezpečení dokumentů v zamykatelných skříních nebo zabezpečení dat přenášených na médiích pomocí šifrování. Naopak tam, kde jde o masivní zpracování osobních údajů se značnými riziky pro subjekty údajů, bude třeba nasadit odpovídající technická, procesní a organizační opatření v celé šíři.

Nové povinnosti

Nařízení GDPR přináší nové povinnosti, nikoli plošně, ale pouze pro organizace, která splní určitá definovaná kritéria.

Mezi nové povinnosti patří především:

- Povinnost vést záznamy o činnostech zpracování.
- Posouzení vlivu (dopadu) zpracování na ochranu osobních údajů (Data Protection Impact Assessment neboli DPIA).
- Konzultace s Úřadem pro ochranu osobních údajů (dále jen „ÚOOÚ“), pokud z DPIA vychází vysoké riziko.
- Ohlašování případu porušení zabezpečení osobních údajů ÚOOÚ.
- Oznamování případu porušení zabezpečení osobních údajů subjektu údajů (pokud dopady pro subjekty údajů jsou významné).
- Ustavení a jmenování Pověřence.
- Záměrná a standardní ochrana dat /data protection by design, by default) od samého počátku (například při novém zpracování osobních údajů a budování nového informačního systému).

ČÁST II. ZMAPOVÁNÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Aby správce nebo zpracovatel doložil soulad s Nařízením GDPR, měl by za splnění definovaných podmínek vést záznamy o činnostech zpracování, za které odpovídá. Každý správce a zpracovatel by měl být povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány. Cílem tohoto kroku je „pořádek v datech na jednom místě".

Výčet povinných informací, resp. nezbytné minimum záznamů předkládá článek 30 Nařízení GDPR. K tomuto účelu je možno využít vzoru vypracovaného MV „Záznam o činnostech zpracování osobních údajů", který je dostupný na adrese:

http://www.mvcr.cz/gdpr/soubor/zaznam-30gdpr-volby-docx.aspx

Tabulku, respektive záznam je nutno vyplnit pro každé zpracování osobních údajů. Většinou stačí tato úroveň podrobnosti. Pokud ne, je možné danou agendu rozpracovat podrobněji v samostatném dokumentu/dokumentech (například personální a mzdová agenda) a v tabulce uvést odkaz. Tyto záznamy umožní správci prokázat soulad zpracování s obecným Nařízením GDPR.

Obecně je nutné mít při vytváření záznamu o zpracování na paměti, že jedním z hlavních principů Nařízení GDPR je požadavek na minimalizaci osobních údajů – ze stanoveného účelu vyplývá přípustný:

- rozsah zpracování osobních údajů,
- způsob zpracování,
- doba uložení osobních údajů.

ČÁST III. ANALÝZA RIZIK A POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Analýza rizik

Standardní postup začíná u úvah, která zpracování mohou mít velký dopad na organizaci v tom případě, že se naplní nežádoucí rizikový scénář (například uniknou osobní údaje nebo se ztratí). Smyslem tohoto prvotního posouzení je identifikovat zpracování, u nichž bude potřebné provést analýzu rizik. U zpracování se zanedbatelným dopadem není třeba provádět náročné posouzení rizik.

Pokud však je dopad střední nebo vysoký, je potřeba pro danou agendu (dané zpracování) provést analýzu rizik. A v případě, že je výsledné riziko ohodnoceno prioritou „kritické“ nebo „vysoké“, je nutné navrhnout a realizovat taková opatření, která sníží riziko přinejmenším na úroveň „střední“.

Posouzení vlivu

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude představovat vysoké riziko pro práva a svobody fyzických osob. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

Posouzení vlivu na ochranu osobních údajů je nutné provést zejména v těchto případech:

a) pokud dochází k systematickému a rozsáhlému vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky;

b) pokud dochází k rozsáhlému zpracování zvláštních kategorií údajů uvedených v článku 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

c) u rozsáhlého systematického monitorování veřejně přístupných prostorů.

Je třeba, aby správce zajistil posouzení dopadu zpracování osobních údajů do práv a svobod subjektů osobních údajů. Provedení posouzení vlivu je nutné konzultovat s pověřencem pro ochranu osobních údajů dané organizace. V případě, že se nepodaří navrhnout opatření ke snížení rizik na akceptovatelnou úroveň, je nutná konzultace s ÚOOÚ.

Tématem se zabývají schválené pokyny Pracovní skupiny WP29 k posouzení vlivu na ochranu osobních údajů viz:

https://www.uoou.cz/schvalene-pokyny/d-28603

ČÁST IV. PRÁVA SUBJEKTŮ OSOBNÍCH ÚDAJŮ

Nařízení GDPR v rámci uplatňování principu transparentnosti zajišťuje subjektu osobních údajů řadu práv. Jedná se zejména o právo na informace podle článku 13 a 14 Nařízení GDPR a další práva podle článků 15-22 Nařízení GDPR.

Mezi práva subjektu údajů patří:

- informovanost o rozsahu a způsobu zpracování osobních údajů,
- přístup k osobním údajům a jejich oprava v případě nepřesností,
- znát plánovanou dobu, po kterou mají být údaje zpracovány,
- právo vznést námitku proti zpracování osobních údajů,
- zažádat o omezení zpracování,
- požadovat přenositelnost (pokud subjekt sám osobní údaj poskytl nebo je zpracování založeno na smlouvě)
- zažádat u správce o výmaz (pokud je relevantní),
- požadovat lidský zásah v případě automatizovaného zpracování včetně profilování
- právo podat stížnost u dozorového úřadu.

V případě, že subjekt svého práva využije, je správce povinen mu do 30 dnů odpovědět, v odůvodněných případech může tuto lhůtu správce prodloužit o maximálně další dva měsíce.

Měsíc je poměrně krátká lhůta, a proto je potřeba se na dotazy, námitky a žádosti připravit. Doporučujeme proto následující postup:

- vytvořit ideálně jedno vstupní místo s předpřipraveným formulářem
  (cílem je standardizace vstupů od subjektů osobních údajů za účelem zrychlení předání administrátorovi / odpovědnému pracovníkovi),
- nastavit interní procesy vyřízení žádosti
  (např. jednotný proces oslovení zodpovědných pracovníků a jednotný formulář pro odpověď),
- předpřipravit si typové odpovědi,
- nastavit proces opravy a výmazu.

Další informace na téma Transparentnost a postupy pro výkon práv subjektů údajů nabízí Kapitola III oddíl 1 článek 12 Nařízení GDPR.

ČÁST V. VZTAH SPRÁVCE – ZPRACOVATEL

Jak bylo již na začátku řečeno, správce je právnická nebo fyzická osoba, která určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá.

Zpracovatel je subjekt, kterého si správce najímá, aby pro něj jeho jménem prováděl s osobními údaji zpracovatelské operace.

Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Nařízení GDPR a aby byla zajištěna ochrana práv subjektu údajů.

Pokud tedy zpracovatel osobních údajů zpracovává pro správce osobní údaje (je externím dodavatelem nebo provozovatelem aplikace, případně poskytovatelem cloudových služeb), pak musí být činnost zpracovatele smluvně pokryta.

Protože Nařízení GDPR explicitně nařizuje, co musí taková smlouva garantovat, inspiraci v této oblasti nabízí následující bod - Část VI. Inspirace k doplnění smluv se zpracovateli.

ČÁST VI. INSPIRACE K DOPLNĚNÍ SMLUV SE ZPRACOVATELI

Obecně je třeba upravit smluvní vztahy se zpracovateli a to dodatky či doložkami ke smlouvám. Předložený text níže je nutno chápat jako modelový příklad, který je aplikován / modifikován dle potřeb organizace.

Modelový příklad

1. Účelem Smlouvy je stanovení práv a povinností Správce a Zpracovatele vyplývajících z Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
2. Zpracovatel je při zpracování osobních údajů povinen řídit se Smlouvou a zpracovávat osobní údaje pouze v rozsahu zpracování vymezeným Správcem.
3. Při zpracování osobních údajů je Zpracovatel povinen postupovat v souladu s Nařízením GDPR a dalšími právními předpisy, zejména:
   a) postupovat v souladu s písemnými pokyny Správce stanovenými pro zpracování osobních údajů, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právní předpisy Evropské unie nebo členského státu, které se na Správce vztahují; v takovém případě je Zpracovatel povinen Správce písemně informovat o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
   b) zavázat mlčenlivostí veškeré osoby podílející se na zpracování osobních údajů;
   c) přijmout veškerá opatření k ochraně zabezpečení zpracování osobních údajů uvedená zejména v článku 32 Nařízení GDPR;
   d) dodržovat podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4 článku 28 Nařízení GDPR.
   e) poskytovat Správci součinnost nezbytnou pro splnění povinností Správce vůči subjektům osobních údajů při výkonu jejich práv, podle kapitoly III. Nařízení GDPR, a pro zabezpečení ochrany osobních údajů podle článků 32 až 36 Nařízení GDPR;
   f) poskytnout Správci veškeré informace nezbytné k doložení splnění povinností dle článku 28 Nařízení GDPR;
   g) vést záznamy o činnostech zpracování osobních údajů, které Zpracovatel provádí pro Správce;

h) neprodleně Správci oznámit případnou ztrátu, poškození, nebo neoprávněné zpřístupnění osobních údajů, popř. jakýkoliv jiný bezpečnostní incident dle Nařízení GDPR ve svěřené oblasti zpracování osobních údajů;

i) umožnit provedení auditů, kontrol a inspekcí plnění povinností podle Nařízení GDPR Správcem nebo jím pověřenou osobou a poskytnout k tomu veškerou nezbytnou součinnost, a to bezplatně;

j) na základě pokynu Správce neprodleně, nejpozději však ve lhůtě XX kalendářních dnů, prokazatelně zlikvidovat nebo vrátit Správci veškeré poskytnuté osobní údaje.

4. Zpracovatel je povinen dodržovat veškeré další povinnosti a podmínky stanovené Nařízením GDPR a obecně závaznými právními předpisy týkajícími se ochrany osobních údajů v souvislosti se zpracováním a ochranou osobních údajů při plnění předmětu Smlouvy.

Odpovědnost za škodu

V případě, že bude Správci způsobena škoda v důsledku neplnění povinností Zpracovatele stanovených Smlouvou nebo vyplývajících z Nařízení GDPR anebo obecně závazných právních předpisů upravujících ochranu osobních údajů, je Zpracovatel povinen nahradit veškerou takto vzniklou škodu Správci ve lhůtě XX kalendářních dnů ode dne doručení písemné výzvy Správce k náhradě škody. Pro účely tohoto ustanovení se za škodu považují i peněžité sankce uložené jakýmkoliv národním orgánem nebo orgánem Evropské unie.

ČÁST VII. ZDROJE INFORMACÍ K NAŘÍZENÍ GDPR

Úřad pro ochranu osobních údajů
https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

Ministerstvo vnitra
http://www.mvcr.cz/gdpr/clanek/rozcestnik.aspx

Ministerstvo průmyslu a obchodu
https://www.mpo.cz/cz/podnikani/obecne-narizeni-o-ochrane-osobnich-udaju-gdpr--228672/

Hospodářská komora České republiky
https://www.komora.cz/prirucka-k-gdpr/

WP29 vydává dokumenty poskytující výklad významných prvků zaváděných, často i zcela nově, obecným nařízením o ochraně osobních údajů.

Na této stránce naleznete Pokyny a Vodítka:
https://www.uoou.cz/schvalene-pokyny/d-28603