Úřad pro ochranu osobních údajů

Základní příručka k GDPR

Přehled základních pojmů a informací vztahujících se k obecnému nařízení.
Obsah

1. Obecné nařízení

Co znamená obecné nařízení o ochraně osobních údajů?

Obecné nařízení představuje aktualizovaný právní rámec ochrany osobních údajů v evropském prostoru, který bude od 25. května 2018 přímo stanovovat pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak obecné nařízení od 25. května 2018 nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů, který v současné době stanovuje povinnosti a práva při zpracování osobních údajů.

V souvislosti s nutností adaptovat český právní řád na obecné nařízení vyvstane nutnost upravit některé dílčí aspekty nezbytné k dotvoření celého rámce ochrany osobních údajů na zákonné úrovni. Je to z toho důvodu, že obecné nařízení například umožňuje, aby se v jím definovaných případech členský stát odchýlil od úpravy v obecném nařízení nebo dokonce i stanovuje, že některé aspekty mají být upraveny ve vnitrostátním právu členského státu. Nepůjde již ale o svébytný zákon, ale jen o doplňkový k obecnému nařízení, dotvářející komplexní úpravu ochrany osobních údajů při jejich zpracování a to např. i v oblasti zpracování osobních údajů za účelem předcházení, vyhledávání nebo odhalování trestné činnosti atd. Návrh adaptačního zákona je již v legislativním procesu a je dostupný veřejnosti.

Charakteristická pro obecné nařízení je jeho univerzální použitelnost ve všech státech Evropské unie (a Islandu, Norsku a Lichtenštejnsku) a tudíž i sjednocující účinek právní úpravy, jelikož jednotná pravidla pro zpracování osobních údajů budou platit v každém státě EU a v předchozí větě třech vyjmenovaných. Právě zajištění větší jednotnosti pravidel ochrany osobních údajů bylo i jedním z cílů přijetí obecného nařízení.

Celý název předpisu je 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).

Anglická zkratka obecného nařízení, se kterou se lze setkat v odborných textech či hovoru, je GDPR (z anglického názvu General Data Protection Regulation).

Proč muselo dojít k revizi právního rámce ochrany osobních údajů?

K revizi bylo přikročeno z toho důvodu, že současný právní rámec, založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současné době, zejména pokud jde o prostředky, které jsou ke zpracování využívány a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami let (např. v oblasti profilování, automatizace zpracování osobních údajů atd.) a tudíž je i rizikovější pro práva a svobody fyzických osob. Zároveň v jednotlivých zemích Evropské unie nebyla Směrnicí 95/46/ES dosažena požadovaná míra sjednocení právní úpravy, což správcům působícím ve více zemích činilo problémy.

Cílem obecného nařízení je tedy přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektů údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady.

Je obecné nařízení revolucí, tak jak jsem o něm několikrát slyšel hovořit?

V základních bodech obecné nařízení není revolucí, jelikož jde o kontinuitu se zmíněnou Směrnicí 95/46/ES, která jím bude zrušena. Je nutné si uvědomit, že od roku 2000 upravuje zpracování osobních údajů v České republice zákon č. 101/2000 Sb., o ochraně osobních údajů, který vychází ze zmíněné směrnice. Každá organizace by již tedy měla zpracovávat osobní údaje podle tohoto zákona. Za revoluci bychom mohli označit pouze přímou použitelnost obecného nařízení, což vyplývá z jeho charakteru, jakožto nařízení.

Obecné nařízení nemění základní zásady zpracování osobních údajů či základní pojmy jako jsou např. osobní údaj, subjekt údajů, správce, zpracovatel či zpracování. Nerozšiřuje ani svoji působnost oproti současné právní úpravě. Pro některá zpracování, resp. subjekty, však klade vyšší nároky při zpracování osobních údajů. Typicky jde o velké správce osobních údajů typu bank, telekomunikačních operátorů atd., tj. pro správce, kteří zpracovávají rozsáhlé množství osobních údajů a které je současně ze své podstaty rizikové pro práva a svobody subjektů údajů, tedy fyzických osob, o nichž jsou osobní údaje zpracovávány.

Na druhou stranu pro drobné živnostníky apod., kteří de facto zpracovávají osobní údaje svých zákazníků pouze pro účely poskytnutí služby či výrobku, nepřináší obecné nařízení zásadní změny oproti stávající úpravě a v takových případech je nutné zejména sledovat dodržování základních zásad zpracování.

S nařízením jsem nikdy nepracoval, má nějaké zvláštnosti?

Pokud jde o stanovení práv a povinností, není mezi nařízením a zákonem rozdíl, oba dva právní

předpisy přímo adresátům stanovují práva a povinnosti a. Jistou zvláštností nařízení je jeho Preambule, která obsahuje tzv. recitály, což jsou ustanovení předcházející vlastnímu textu nařízení a jsou v některých případech výkladem či do jisté míry důvodovou zprávou k vlastnímu textu nařízení. Je tak vhodné při práci s nařízením sledovat i příslušné recitály.

Dále je nutné vzít v potaz, že celý právní rámec bude dotvářet adaptační zákon, který bude obsahovat i drobné (povolené) odchylky či zvláštní úpravy k obecnému nařízení. Kompletní právní rámec ochrany osobních údajů tak bude tvořen obecným nařízením a adaptačním zákonem.

Co znamená datum použitelnosti obecného nařízení?

Použitelnost znamená jinými slovy účinnost obecného nařízení, tedy datum, od kdy se obecné nařízení začne používat neboli aplikovat.
Byť je obecné nařízení v současné době platné, není ještě účinné (použitelné), tj. prošlo již legislativním procesem, je to tudíž schválený platný dokument, ale jeho účinnost nastane 25. května 2018. Od tohoto dne se tedy všechny subjekty zainteresované na zpracování osobních údajů budou řídit obecným nařízením.

Nyní běží pro správce a zpracovatele dvouletá lhůta, aby uvedli ke dni použitelnosti obecného nařízení svá zpracování osobních údajů do souladu s obecným nařízením. Tato lhůta skončí dnem použitelnosti obecného nařízení, kdy uskutečňované zpracování s ním musí být již v souladu (tedy 25. května 2018).

Co bude se současným zákonem o ochraně osobních údajů?

Jelikož obecné nařízení stanovuje práva a povinnosti při zpracování osobních údajů, v tomto rozsahu zákon č. 101/2000 Sb., o ochraně osobních údajů nahrazuje. Práva a povinnosti v současném zákoně o ochraně osobních údajů budou nahrazeny právy a povinnostmi přímo vyplývajícími z obecného nařízení. Zákon o ochraně osobních údajů bude účinností adaptačního zákona zrušen.

Vyvstane pouze nutnost přijmout tzv. adaptační zákon, který bude přijat v souvislosti s přímou použitelností obecného nařízení. Tento zákon bude upravovat např. aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho opětovné zákonné ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou obecným nařízením upraveny nebo které obecné nařízení umožňuje upravit na vnitrostátní úrovni. U některých aspektů obecné nařízení výslovně předpokládá vnitrostátní úpravu. Mezi ně patří například aspekty zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby.

Kdo se bude muset obecným nařízením řídit?

Obecným nařízením se bude především, pokud jde o povinnosti, řídit subjekt, který provádí zpracování osobních údajů. Takový subjekt je nazýván správcem osobních údajů. Obecným nařízením se řídí i zpracovatel, což je subjekt, který pro správce osobní údaje zpracovává. Pokud jde o práva vyplývající z obecného nařízení, ta vyplývají fyzické osobě, což je subjekt údajů. Dále se obecným nařízením budou řídit i dozorové úřady, tj. i Úřad pro ochranu osobních

údajů, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů.

Musí se obecným nařízením řídit i drobný živnostník nebo malý internetový obchod?

Ano, pokud při jejich činnosti dochází ke zpracování osobních údajů, což z povahy věci zpravidla dochází (nejčastěji osobní údaje zákazníků – fyzických osob, či osobní údaje zaměstnanců nebo obchodních partnerů). Je však nutné si uvědomit, že obecné nařízení klade vyšší nároky především na subjekty, které zpracovávají osobní údaje ve velkém rozsahu či zvláštní kategorie osobních údajů, resp. pokud jsou osobní údaje hlavním bodem činnosti. To jsou například banky, telekomunikační operátoři, velké nemocnice atd.

Pokud při činnosti určitého subjektu dochází k běžné práci s osobními údaji nezbytnými např. k provedení služby či prodeji výrobku, lze zpravidla konstatovat, že obecné nařízení nepřináší rozdíly oproti současnému zákonu č. 101/2000 Sb., o ochraně osobních údajů. U těchto subjektů (malý internetový obchod, živnostník – opravář, mající klientelu z řad fyzických osob), které tedy neprovádí rozsáhlé či rizikové zpracování, je nezbytné zejména dodržovat zásady zpracování osobních údajů. Nutné je především sledovat legitimní účel, pro který byly osobní údaje shromážděny (např. uzavření kupní smlouvy a s tím spojené dodání zboží či poskytnutí služby) a osobní údaje adekvátně zabezpečit.

Na jaké činnosti obecné nařízení nedopadá?

Z působnosti obecného nařízení jsou vyloučeny činnosti fyzické osoby [viz článek 2 odst. 2 písm. c) obecného nařízení], při kterých jsou zpracovávány osobní údaje výlučně pro osobní či domácí činnost. Např. na zpracování osobních údajů pro účely tvorby rodinného rodokmenu se na fyzickou osobu, která tento rodokmen vytváří pro osobní potřebu, nevztahuje obecné nařízení.

Dále je z působnosti obecného nařízení vyloučeno zpracování prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. To je předmětem úpravy Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Jelikož jde o směrnici, je nutné její provedení, které bude vesměs v adaptačním zákoně.

2. Nové přístupy a povinnosti

Co znamená přístup založený na riziku a jaké nové instituty přináší?

Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. Tento přístup platí v současné době za účinnosti zákona č. 101/2000 Sb., o ochraně osobních údajů.

V pojetí obecného nařízení tento přístup navíc znamená aplikaci dodatečných povinností pro některé správce, kdy zpracování osobních údajů či porušení zabezpečení (bezpečnostní incident) představuje riziko či vysoké riziko pro práva a svobody fyzické osoby a je tedy důvodné aplikovat tyto povinnosti. Mezi tyto nové povinnosti, o kterých nelze hovořit, že se plošně vztahují na všechny správce či zpracovatele patří:

• záznamy o činnostech zpracování,
• jmenování pověřence pro ochranu osobních údajů,
• posouzení vlivu na ochranu osobních údajů,
• předchozí konzultace s dozorovým úřadem.

Tyto zmíněné povinnosti mají pouze určený okruh správců či zpracovatelů, především v závislosti na jejich činnosti týkající se zpracování osobních údajů.

Novou povinností je i

• povinnost ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů.

Tato povinnost se z povahy věci může týkat každého správce či zpracovatele (ten oznamuje správci), a to tehdy, pokud je porušení zabezpečení už závažnějšího charakteru, tj. musí z něj vyplývat riziko pro práva a svobody fyzických osob. Pro uplatnění povinnosti oznámit porušení zabezpečení subjektu údajů musí být takové porušení vysoce rizikové pro práva a svobody fyzických osob.

Jak budu jako správce dokládat soulad zpracování?

Ke splnění stanovené odpovědnosti správce za soulad zpracování se zásadami zpracování a schopnost tento soulad prokázat, mají správcům, jak výslovně zmiňuje obecné nařízení, napomáhat mimo jiné záznamy o činnostech zpracování a pověřenec pro ochranu osobních údajů, kodexy, osvědčení (pečetě, známky).

Základním instrumentem pro většinu správců by měly být záznamy o činnostech zpracování dle článku 30 obecného nařízení. Záznamy o činnostech zpracování obsahují obecné informace o prováděném zpracování, což správci umožní lehčí orientaci ohledně zpracování, která provádí.

Pověřenec pro ochranu osobních údajů má u některých správců a zpracovatelů sloužit jako prvek, který má dbát, aby zpracování osobních údajů u některých správců bylo v souladu s obecným nařízením.

Kodexy mají správcům, zejména na sektorové úrovni, sloužit jako vodítko správné praxe při zpracování osobních údajů právě s ohledem na specifičnost daného sektoru (např. bankovnictví, telekomunikace, internetové obchody, zdravotnictví). Vypracování kodexu není povinné, ani se k jeho dodržování přihlásit. Jde o fakultativní možnost.

Osvědčení má sloužit k prokázání souladu zpracování s obecným nařízením. Není stanovena povinnost získat osvědčení, jde o fakultativní možnost, kterou správce či zpracovatel může deklarovat soulad zpracování osobních údajů s obecným nařízením. Osvědčení budou moci vydávat pouze k tomu akreditované subjekty.

Dokládání souladu zpracování však nelze omezit pouze na shora uvedené možnosti, ale

dokládání souladu je komplexní činnost, zahrnující dílčí činnosti, mezi které lze zařadit nejen shora uvedené kodexy, osvědčení a záznamy o činnostech zpracování, ale například i zveřejňování informací, které obecné nařízení ukládá správci zveřejňovat, vyhotovením vnitřních předpisů až po řádnou spolupráci s příslušným dozorovým úřadem.

Dokládání souladu ve shora uvedeném smyslu se uplatní zejména u organizací, na které se vztahují dodatečné povinnosti založené na riziku.

Soulad zpracování však musí být i u ostatních správců, na které se nevztahují dodatečné povinnosti. Ti zejména musí plnit základní zásady zpracování, adekvátní zabezpečení osobních údajů a dodržovat práva subjektu údajů.

Kdo bude vydávat kodexy a osvědčení?

Kodexy budou moci vydávat sdružení či jiné subjekty zastupující různé kategorie správců nebo zpracovatelů přičemž návrh kodexu musí být předložen Úřadu pro ochranu osobních údajů, který vydá stanovisko, zdali je daný kodex, či návrh na jeho změnu, v souladu s Obecným nařízením a pokud shledá, že ano, schválí jej. Schváleným kodexem se pak můžou řídit správci v daném sektoru, např. bankovnictví či zdravotnictvím.

Osvědčení o souladu zpracování bude moci vydávat k tomu akreditovaný subjekt. V současné době probíhají práce na stanovení formy a postupů pro akreditaci a pro vydávání osvědčení ze strany akreditovaných subjektů.

Kdy musí správce provést posouzení vlivu na ochranu osobních údajů?

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. Posouzení se musí provést před započetím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek.

Posouzení vlivu na ochranu osobních údajů se vyžaduje především:

u systematického a rozsáhlého 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
u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech
u rozsáhlého systematického monitorování veřejně přístupných prostorů

Jak vidno, aby nastala tato povinnost, musí se již skutečně jednat o zpracování, které přináší vysoké riziko pro práva a svobody fyzických osob. Netýká se tedy každého zpracování.

Podrobněji k této povinnosti viz schválené pokyny Pracovní skupiny WP29 k posouzení vlivu na ochranu osobních údajů.

Kdy musí správce konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů?

Správce je povinen konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů, pokud z posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika. Jinými slovy, pokud správci i po přijetí opatření ke zmírnění vysokého rizika toto vysoké riziko přetrvává. Účelem předchozí konzultace je tak korigovat hrozící vysoké riziko s dozorovým úřadem. K této povinnosti viz schválené pokyny Pracovní skupiny WP29 k posouzení vlivu na ochranu osobních údajů.

Co jsou záznamy o činnostech?

Záznamy o činnostech zpracování představují do jisté míry náhradu za oznamovací povinnost, která byla obecným nařízením zrušena. Správce a zpracovatel, pokud se na ně nevztahuje výjimka z povinnosti vést záznamy o činnostech zpracování, jsou povinni vést záznamy s určitými informacemi. Tyto záznamy následně umožní správci prokázat soulad zpracování s obecným nařízením. Jde o obecné záznamy. Nejde o záznamy každodenní činnosti s osobními údaji, ale skutečně o obecné záznamy zpracování, které správce nebo zpracovatel provádějí. Není stanovena forma těchto záznamů a je předpoklad, že záznamy o činnostech zpracování se budou lišit i v závislosti na rozpětí prováděného zpracování. Nezbytné minimum záznamů je uvedeno v článku 30 odst. 1 obecného nařízení.

Kdo nemusí vést záznamy o činnostech zpracování?

Povinnost vést záznamy o činnostech zpracování nedoléhá na podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech. Do tohoto počtu se počítají i zaměstnanci na dohody o pracích konaných mimo pracovní poměr či agenturní zaměstnanci.

S ohledem na praktičnost záznamů o činnostech zpracování lze doporučit jejich vyhotovení i organizacím, u nichž není zcela zřejmé, že s ohledem na jejich činnost dojde k aplikaci výjimky z této povinnosti.

Je pravda, že bude zrušena oznamovací povinnost?

Ano, obecné nařízení oznamovací povinnosti nepřebírá. Roli oznamovací povinnosti budou přebírat především záznamy o činnostech zpracování (do jisté míry si správce informace, které by zasílal Úřadu pro ochranu osobních údajů prostřednictvím této povinnosti, ponechá pro své účely) a v některých případech povinnost provést posouzení vlivu na ochranu osobních údajů.

3. Nejdůležitější pojmy

Definice pojmů jsou obsaženy v článku 4 odst. 1 obecného nařízení.

Co je zpracování osobních údajů?

Zpracování je jakákoli operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Zpracování ve smyslu obecného nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování.

Pojem zpracování má stejný význam, jako měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů.

Co se rozumí pojmem automatizovaně?

S pojmem automatizace se lze setkat u vymezení působnosti obecného nařízení, které se vztahuje na zpracování osobních údajů, které je prováděno zcela či částečně automatizovaně a dále na zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

Definice evidence je obsažena v článku 4 odst. 6 obecného nařízení.

Definice automatizace však obsažena není. Automatizaci lze vyložit tak, že jde o zpracování pomocí informačních systémů, tj. prostřednictvím softwaru, který je z logiky věci automatizovaný. Lze tedy zjednodušit, že automatizovaně znamená prostřednictvím výpočetní techniky.

Co je osobní údaj?

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Pojem osobní údaj nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů de facto změněn.

Podstatné pro definici osobního údaje je nutné uvědomění, že osobním údajem je jakákoli informace týkající se identifikované či identifikovatelné fyzické osoby a skutečnost, že identifikace, resp. identifikovatelnost může nastat různými způsoby, ne vždy pouze podle jména, příjmení, adresy a data narození, ale i např. kódem, který je třeba zaměstnanci přidělen či IP adresou atd.

Byť je definice osobního údaje poměrně široká, je nutné vzít v potaz, že aplikace zákona o ochraně osobních údajů, resp. obecného nařízení nastává až při zpracování osobních údajů.

Kdo je subjekt údajů?

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se výlučně k právnické osobě tak nejsou osobními údaji. Osobním údajem však již je např. e-mailová adresa zaměstnance právnické osoby, typicky ve tvaru jmeno.prijmeni@firmaabcxyz.cz

Osobní údaje mohou být osobními údaji pouze ve vztahu k žijící fyzické osobě, jelikož obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách.

Definice subjektu údajů je obsahově totožná jako v zákoně č. 101/2000 Sb., o ochraně osobních údajů.

Kdo je správce?

Správcem je subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Z povahy věci musí být u každého zpracování správce. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely, např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob.

Správcem může být jakýkoli subjekt. Správcem může být i fyzická osoba, pokud zpracovává osobní údaje způsobem, že tento způsob již vylučuje uplatnění výjimky osobní či domácí činnosti, resp. pokud nejde o nakládání s osobními údaji, které ještě nesplňuje definici jejich zpracování.

V případě právnické osoby je správcem daná právnická osoba, nikoli její některý zaměstnanec či společník nebo jednatel. Odpovědnost za zpracování osobních údajů má právnická osoba jako taková. Pojem správce nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů změněn.

Kdo je zpracovatel?

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Není povinností správce najmout si zpracovatele, tj. zpracovatel není nutný prvek zpracování. Zpracovatelem není jednotlivý zaměstnanec správce (např. účetní či personalista správce a ani jeho vnitřní útvar).

Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen. Je nutné poznamenat, že zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají (např. je správcem při zpracování osobních údajů vlastních

zaměstnanců). Typickým zpracovatelem je např. externí mzdová účetní firma (či živnostník) nebo poskytovatel cloudu (úložiště apod.)

Stejně jako u správce, ani u zpracovatele není určující jeho právní forma.

Pojem zpracovatel nebyl oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů změněn.

Co se rozumí profilováním?

Jde o formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu.

Byť je profilování nově definováno, nejde de facto o žádnou novinku, jelikož k profilování dochází i v současné době. Profilování není a priori zákonem o ochraně osobních údajů či obecným nařízením zakázáno, nevyžaduje se a priori souhlas subjektu údajů. Je však důležité, aby se dělo v předvídaných případech a na základě stanovených pravidel. Profilování je běžné např. ve finančních službách, kdy finanční subjekty profilují např. klienta žádajícího o hypotéku, u kterého hodnotí schopnost splácet.

4. Zásady a právní důvody zpracování

Na jakých zásadách je obecné nařízení postaveno?

Zásady lze ve stručnosti shrnout na:

zákonnost, korektnost, transparentnost - správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně,
omezení účelu - osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
minimalizace údajů - osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
přesnost - osobní údaje musí být přesné,
omezení uložení - osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
integrita a důvěrnost - technické a organizační zabezpečení osobních údajů.

Jednotlivé zásady jsou rozvinuty v článku 5 odst. 1 obecného nařízení. Vymezení, resp. dodržování těchto zásad, je pro správce zásadní, nejen z toho důvodu, že to jsou de facto zároveň povinnosti, ale i proto, že v článku 5 odst. 2 obecného nařízení je stanovena odpovědnost správce za jejich dodržování a zároveň povinnost správce být schopen dodržování těchto zásad (povinností) doložit. Jde o vyjádření tzv. principu odpovědnosti správce. K prokazování souladu s těmito zásadami budou sloužit záznamy o činnostech zpracování a též kodexy a osvědčení.

Zásady zpracování zároveň můžeme označit za základní stavební kameny každého zpracování. Jde o souhrn zásad, které musí být při zpracování osobních údajů dodržovány.

Co se rozumí právními důvody zpracování osobních údajů?

Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat. Právní důvody tak jsou nezbytným předpokladem, aby vůbec mohlo být hovořeno ze strany správce o legálním zpracování, jelikož pokud by správce nedisponoval řádným právním důvodem ke zpracování osobních údajů, bylo by dále nerozhodné, zdali plní ostatní povinnosti, jelikož by osobní údaje zpracovával nezákonně a musel by osobní údaje zlikvidovat.

Je důležité vědět, že i osobní údaje může správce zpracovávat pro různé účely, přičemž pro každý účel potřebuje právní důvod zpracování osobních údajů. Zpracování osobních údajů se vždy váže k účelu, na základě kterého se určí právní důvod zpracování. Není vyloučeno, že „jedny“ osobní údaje (nebo jejich určitý souhrn) bude správce zpracovávat pro různé účely, přičemž tyto účely mohou v čase vznikat či zanikat, aniž by to představovalo povinnost osobní údaje likvidovat. Povinnost likvidace osobních údajů nastane v případě, kdy správce pozbude poslední právní důvod ke zpracování osobních údajů.

Jaké jsou právní důvody zpracování osobních údajů subjektu údajů?

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních důvodů:

subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,
zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

Co znamená souhlas se zpracováním osobních údajů?

Souhlas (viz definice článek 4 odst. 1 bod 11 obecného nařízení) je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Jde o aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen.

Souhlas je jedním z právních důvodů, na základě kterého může správce osobní údaje zpracovávat a nastupuje tehdy, pokud zpracování nelze podřadit pod účely, pro které není nutné souhlas vyžadovat.

Souhlas se vždy poskytuje k určitému účelu zpracování, který musí subjekt údajů znát.

Souhlas je odvolatelný. Nikoli vždy odvolání souhlasu znamená povinnost správce osobní údaje zlikvidovat, jelikož odvolání souhlasu se děje k určitému účelu, pro který jsou osobní údaje zpracovávány, přičemž správce může osobní údaje zpracovávat pro jiné účely, pro které využije

jiný právní důvod zpracování než souhlas subjektu údajů. Jinými slovy, v případě odvolání souhlasu je správce povinen přestat zpracovávat osobní údaje pro účely definované v souhlasu. Pokud souhlas byl jediným právním důvodem zpracování, bude zpravidla následovat i likvidace osobních údajů.

Pracovní skupina WP29 vydala k tématu své pokyny.

Musím mít ke každému zpracování osobních údajů souhlas subjektu údajů?

Ne, nemusíte. Zejména tam, kde je zpracování nezbytné pro plnění smlouvy se subjektem údajů či k plnění právní povinnosti se souhlas se zpracováním osobních údajů nevyžaduje. Souhlas se nevyžaduje ani k dalším účelům zpracování, které jsou uvedeny výše (vyjma prvního bodu). V případě zpracování pro účely, které nelze podřadit pod výše uvedené účely, je nutné zpracování provádět na základě souhlasu subjektu údajů.

Souhlas subjektu údajů není vyžadován pro účely zpracování nezbytné např. pro dodání zboží v rámci objednávky v e-shopu nebo pro zpracování osobních údajů zaměstnanců pro pracovněprávní účely (pro plnění pracovní smlouvy či plnění zákonem stanovených povinností ze strany zaměstnavatele).

Jaké jsou podmínky udělení souhlasu se zpracováním osobních údajů?

Aby bylo možné dosáhnout svobodnosti, konkrétnosti, informovanosti a jednoznačnosti projevu vůle subjektu údajů, stanovuje obecné nařízení v článku 7 podmínky vyjádření souhlasu. Zásadní je tzv. odlišitelnost souhlasu, což znamená, že souhlas musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje. Pro názornost, souhlas tak musí být oddělený např. od smlouvy či obchodních podmínek, resp. již není možné, aby byl jejich nedílnou součástí. Zároveň nesmí být uzavření smlouvy (např. na poskytnutí služby) podmiňováno poskytnutím souhlasu se zpracováním osobních údajů. Je však samozřejmé, že v závislosti na službě či výrobku bude správce muset zpracovávat (bez souhlasu) určité množství osobních údajů subjektu údajů právě pro účely plnění smlouvy či plnění zákonem stanovené povinnosti, což činí bez souhlasu subjektu údajů.

Je souhlas odvolatelný?

Subjekt údajů má právo svůj souhlas kdykoli odvolat, na což by měl být správce připraven, a to i na jeho další kroky s odvoláním souhlasu spojené (např. provedení likvidace osobních údajů). Odvoláním není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Je nutné si uvědomit, že souhlas byl dáván k určitým účelům a odvolání souhlasu nemusí vždy představovat pro správce povinnost osobní údaje zlikvidovat, ale bude představovat pro správce pouze povinnost přestat osobní údaje zpracovávat pro určitý účel, ke kterému byl souhlas udělen. Stejně tak i v případě, kdy správce použil souhlas pro případy, kdy mu svědčí jiný právní důvod zpracování osobních údajů, neznamená odvolání souhlasu (tedy úkonu, který nebyl nezbytný pro zpracování) povinnost osobní údaje zlikvidovat či je přestat zpracovávat např., pokud osobní údaje musí mít pro zákonem stanovené účely.

Jak to bude se současnými souhlasy za použitelnosti obecného nařízení?

Obecné nařízení v recitálu 171 předpokládá přechod souhlasu, avšak s podmínkou, že souhlas byl udělen způsobem a v souladu s podmínkami obecného nařízení. To bude pro mnoho správců problematické, jelikož jimi získávaný souhlas nebude splňovat podmínky stanovené v článku 7 obecného nařízení, například podmínku odlišitelnosti souhlasu (souhlas nesmí být neoddělitelnou součástí obchodních podmínek) či podmínku nepodmiňovat poskytnutí služby vyžadováním udělení souhlasu se zpracováním osobních údajů. Presumovaný souhlas, který někteří správci využívali (typicky v oblasti finančních služeb, velcí poskytovatelé energií či telefonní operátoři), nepřejde do použitelnosti obecného nařízení. Na poskytování služeb to však nemůže mít žádný vliv. Případné vyžadování udělení nového souhlasu nesmí být prezentováno jako povinnosti pro subjekt údajů.

Můžu zpracovávat osobní údaje zveřejněné na internetu?

V některých případech, zejména v zákonem stanovených případech, musí subjekt údajů strpět jejich zveřejnění např. ve veřejném rejstříku, čímž je i dán účel jejich zveřejnění (např. publicita podnikání, veřejnost katastru nemovitostí atd.). Osobní údaje ve veřejném rejstříku jsou zveřejněny na základě zákona, jelikož tak zákon stanoví (typicky např. živnostenský rejstřík, obchodní rejstřík, katastr nemovitostí). Skutečnost, že je stanovena veřejnost rejstříku, neznamená, že zveřejněné osobní údaje lze dále neomezeně přebírat a zpracovávat, např. jejich dalším zveřejňováním a tím na nich profitovat. Je nutné si uvědomit, že i další zveřejňování údajů z veřejných rejstříků je zpracováním osobních údajů a k tomu musí správci svědčit právní důvod, tj. zákonem předpokládané oprávnění. Jelikož obecné nařízení oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů, neobsahuje ekvivalent právního důvodu oprávněně zveřejněné osobní údaje, který je v zákoně o ochraně osobních údajů obsažen v § 5 odst. 2 písm. d), bude další zveřejňování z veřejných rejstříků převzatých osobních údajů za použitelnosti obecného nařízení problematické, jelikož správce bude muset využít některý z právních důvodů v článku 6 odst. 1 obecného nařízení.

Obdobná situace je i u osobních údajů, které subjekty údajů dobrovolně zveřejňují na internetu za určitým účelem. Ani tyto údaje, byť jsou dobrovolně zveřejněné, nelze bez dalšího zpracovávat, jelikož i v tomto případě by správce neměl právní důvod k jejich zpracování. Veřejnost údajů nikdy a priori neznamená možnost jejich dalšího bezmezného zpracovávání.

5. Zvláštní kategorie osobních údajů (citlivé údaje)

Proč se rozlišují zvláštní kategorie osobních údajů?

Některé osobní údaje jsou takového charakteru, že mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Z tohoto důvodu je taxativně (úplným výčtem) vymezena skupina údajů, které jsou považovány vůči subjektu údajů za citlivé a jimž je poskytnuta zvýšená ochrana při jejich zpracování.

Zvýšená ochrana se projevuje zejména ve stanovených zvláštních právních důvodech, na základě kterých je lze zpracovávat, vázanost některých institutů na jejich zpracování (např. posouzení vlivu, ustavení pověřence, vyhotovit záznamy o činnostech zpracování), důraz na

jejich zvýšené zabezpečení.

Jaké údaje spadají do zvláštní kategorie osobních údajů?

Zvláštní kategorie osobních údajů jsou takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby.

Jejich výčet je téměř totožný s výčtem citlivých údajů v zákoně č. 101/2000 Sb., o ochraně osobních údajů, až na údaj o odsouzení za trestný čin, který již nebude považován za zvláštní kategorii osobních údajů, ale podmínky pro zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů mají zvláštní režim v článku 10 obecného nařízení.

Kdy lze zvláštní kategorie osobních údajů zpracovávat?

Zvláštní kategorie osobních údajů lze zpracovávat, pokud:

subjekt údajů udělil výslovný souhlas,
zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,
zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
zpracování je nezbytné z důvodu významného veřejného zájmu,
zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.,
zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.

Velmi často bude zmocnění pro zpracování zvláštní kategorie osobních údajů obsaženo v příslušném právním předpise, kterým se správce musí řídit, či bude vyplývat z oprávněné činnosti správce.

Například pro zaměstnavatele pro zpracování zvláštních kategorií osobních údajů (typicky údaj o zdravotním stavu) v případě nezbytnosti představuje oprávnění druhý, zvýrazněný bod.

Je fotografie nositelem citlivých údajů? Vždyť z ní dokážu vydedukovat údaj o zdravotním stavu či rase.

Fotografie může být nositelem různých informací. Podstatné je, jak je s těmito informacemi nakládáno a zdali vůbec. Nakládání s fotografií není a priori zpracování citlivých údajů o subjektu údajů. O zpracování zvláštních kategorií osobních údajů by se jednalo až tehdy, pokud by z fotografie byly tyto údaje cíleně zpracovávány ve vztahu ke konkrétní fyzické osobě. Např. by fotografie sloužily jako zdroj získávání informací o nemoci pleti pro lékařský výzkum ve vztahu k identifikovaným či identifikovatelným osobám.

6. Práva subjektu údajů

Proč má subjekt údajů práva?

Obecné nařízení, ostatně tak jako i zákon č. 101/2000 Sb., o ochraně osobních údajů, přiznává subjektům údajů práva. Jejich účelem je vybalancovat vztah mezi správcem a subjektem údajů. Jsou základním pilířem modelu ochrany osobních údajů v evropském prostoru. Nutno podotknout, že obecné nařízení posiluje systém práv subjektů, oproti zákonu o ochraně osobních údajů, a to jak v aktualizaci stávajících práv, tak i některými novými právy, jako je např. právo na přenositelnost.

Je nějaká lhůta, do kdy musí správce reagovat na podanou žádost subjektu údajů?

Pokud se jedná o žádost podle článků 15 až 22 obecného nařízení, musí být informace o přijatých opatřeních poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.

Jaká jsou práva subjektu údajů?

Subjekt údajů má právo na to být informován o zpracování svých osobních údajů. Tím se rozumí právo na určité informace o zpracování jeho osobních údajů, tak aby byla především naplněna zásada transparentnosti zpracování. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. V tomto případě jde o pasivní právo, jelikož aktivitu musí vůči subjektu údajů vyvinout správce, aby požadované informace stanovené v obecném nařízení subjektu údajů poskytl, resp. zpřístupnil.

Úplný výčet informací, které správce poskytuje při shromažďování osobních údajů, lze nalézt v článcích 13 a 14 obecného nařízení. Obecné nařízení formálně rozlišuje poskytování informací v případě, že osobní údaje jsou získány od subjektu údajů, resp. nejsou získány od subjektu údajů. Právo na informování je ekvivalentem práva na informace o zpracování stanoveném v § 11 současného zákona č. 101/2000 Sb., o ochraně osobních údajů.

Mezi další práva subjektu údajů, která jsou mnohdy založena na aktivitě (žádosti) subjektu údajů, patří
• právo na přístup k osobním údajům,
• právo na opravu, resp. doplnění,
• právo na výmaz,
• právo na omezení zpracování,
• právo na přenositelnost údajů,
• právo vznést námitku,
• právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování.

Co se rozumí přístupem k osobním údajům?

Přístupem k osobním údajům se rozumí oprávnění subjektu údajů na základě jeho aktivní žádosti získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

účely zpracování,
kategorie dotčených osobních údajů,
příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
plánovaná doba, po kterou budou osobní údaje uloženy,
existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
právo podat stížnost u dozorového úřadu,
veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce.

Jde o ekvivalent práva přístupu k osobním údajům, stanoveném v § 12 současného zákona č. 101/2000 Sb., o ochraně osobních údajů.

Co když jsou údaje nepřesné?

Subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají. Toto právo vyvěrá ze zásady přesnosti. Neznamená to povinnost správce aktivně vyhledávat nepřesné údaje (avšak nic mu v tom ani nebrání), ani to neznamená povinnost správce např. každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že správce zpracovává jeho nepřesné údaje, upozorní jej na to. Je povinností správce, pokud mu subjekt údajů oznámí, že požaduje opravu jeho osobních údajů, zabývat se jeho žádostí.

Co znamená právo být zapomenut?

Právo na výmaz (být zapomenut) představuje v obecném nařízení jinými slovy vyjádřenou povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
osobní údaje byly zpracovány protiprávně,
osobní údaje musí být vymazány ke splnění právní povinnosti,
osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení.

Právo na výmaz se tedy uplatní jen ve vyčtených bodech, tj. když nastane daná okolnost.

Většina vyjmenovaných případů je součástí i současného zákona č. 101/2000 Sb., o ochraně osobních údajů, nebo vyplývají z jeho podstaty.

Právo na výmaz není absolutní právo, které by subjektu údajů dávalo možnost žádat kdykoli a za jakékoli situace o vymazání osobních údajů. Nelze např. v rámci práva být zapomenut žádat likvidaci všech osobních údajů např. při ukončení zaměstnání či poskytování finančních služeb, jelikož na správce se vztahují povinnosti o dalším uchování některých osobních údajů.

Co znamená právo na přenositelnost údajů?

Právo na přenositelnost je zcela nové právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému správce, je-li to technicky proveditelné.

Společné podmínky k aplikaci práva na přenositelnost:

musí jít o zpracování založené na právním důvodu souhlasu či smlouvě,
zpracování se provádí automatizovaně.

Výkonem práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob.

K právu na přenositelnost údajů byl ze strany Pracovní skupiny WP29 vydán výkladový materiál dostupný v rubrice Schválené pokyny:

Kdy lze vznést námitku proti zpracování osobních údajů?

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:

zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků. Do jisté míry jde o ekvivalent práva na vysvětlení dle §

21 současného zákona č. 101/2000 Sb., o ochraně osobních údajů.

Námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

Jak chápat právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném rozhodování?

Toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Jinými slovy, jde o zajištění, aby se o právních účincích nerozhodovalo automatizovanými postupy bez lidské ingerence, kromě možných výjimek.

Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, pokud je povoleno právem EU nebo členským státem nebo pokud je založeno na výslovném souhlasu subjektu údajů.

Nelze tak například automatizovaně pokutovat řidiče překračující rychlost, aniž by pokutu nepřezkoumal člověk.

Zákaz automatizovaného individuálního rozhodování je stanoven i v § 11 odst. 6 současného zákona č. 101/2000 Sb., o ochraně osobních údajů.

Mohu si jako správce účtovat náklady v souvislosti s výkonem práv subjektu údajů?

Zásadně platí, že informace podle článků 13 a 14 a veškerá sdělení a úkony podle článků 15 až 22 a 34 obecného nařízení se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce.

Co když subjekt údajů zneužívá své právo?

Zneužitím nelze a priori rozumět výkon práv subjektu údajů. O zneužití práva subjektem údajů lze hovořit zejména tehdy, pokud se žádosti opakují a jsou zjevně nedůvodné či nepřiměřené. V takovém případě může správce uložit přiměřený poplatek nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost dokládá správce.

7. Správce, zpracovatel

Za co správce odpovídá?

Správce odpovídá za dodržování povinností kladených obecným nařízením. Zcela zásadní je dodržování zásad zpracování, jejichž dodržování zároveň musí být správce schopen doložit.

Základním nezbytným předpokladem je existence řádného právního důvodu zpracování osobních údajů, kterým správce musí disponovat, aby vůbec mohl osobní údaje zpracovávat. Zároveň je nutné osobní údaje dostatečně zabezpečit. Samozřejmostí však musí být plnění i dalších povinností stanovených obecným nařízením. Každý správce by si měl ověřit, v jakém rozsahu na něj obecné nařízení dopadne, zejména pokud jde o nové povinnosti založené na přístupu na riziku (např. může dopadat povinnost jmenovat pověřence, posoudit vliv na ochranu osobních údajů).

Mohou být společní správci?

Ano, nově obecné nařízení výslovně počítá i s možností tzv. společných správců. Jde o případ, kdy účel a prostředky zpracování stanoví společně dva nebo více správců, kteří si mezi sebou transparentním ujednáním vymezí své podíly na odpovědnosti za plnění povinností.

Jak se mě, jako správce, dotkne obecné nařízení?

Každého správce se obecné nařízení dotkne jiným způsobem, a to v závislosti na aspektech zpracování, které provádí. Tomu musí odpovídat i přípravy správce na obecné nařízení. Přístup založený na riziku váže některé povinnosti pouze na riziková či vysoce riziková zpracování, tudíž některé povinnosti mnoho správců nebude muset plnit, zatímco na jiné správce budou dopadat více méně všechny stanovené povinnosti. Každý správce by si měl udělat vlastní analýzu zpracování, které provádí, čímž zjistí, jaké eventuální povinnosti se na něj vztahují. Součástí analýzy je i vytipování slabých míst správce, např. v zabezpečení, či provedení revize právních důvodů a jejich uvedení do souladu s podmínkami obecného nařízení (např. pokud správce využívá souhlas se zpracováním osobních údajů, provést zhodnocení, zdali udělené souhlasy budou použitelné i v době účinnosti obecného nařízení).

Pokud správce řádně plní povinnosti vyplývající ze současného zákona č. 101/2000 Sb., o ochraně osobních údajů, nemělo by pro něj obecné nařízení představovat výrazný problém, se kterým by si neporadil.

Důležité též je nezapomenout na osvětu zaměstnanců, aby především věděli, co se rozumí osobním údajem a byli si vědomi povinností, které musí dodržovat. Též je vhodné zmínit povinnost mlčenlivosti.

Jak na vztah správce – zpracovatel?

Správce může ke zpracování osobních údajů přibrat jiný subjekt, který pro něj bude osobní údaje zpracovávat. Správce by měl využít pouze takového zpracovatele, který s ohledem na povahu, kontext, kategorii osobních údajů a jejich možností, poskytuje dostatečné záruky vhodných technických a organizačních opatření, tak aby zpracování osobních údajů prostřednictvím zpracovatele splňovalo požadavky obecného nařízení a byla zajištěna ochrana práv subjektů údajů. Za tím účelem musí být mezi správcem a zpracovatelem uzavřena písemná smlouva, v níž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Smlouva dále musí zaručovat určité okolnosti zpracování, viz článek 28 odst. 3 obecného nařízení.

Není nutné, aby se jednalo o samostatnou smlouvu, požadované náležitosti lze zakomponovat i do jiné smlouvy, kterou správce se zpracovatelem uzavírá v rámci např. obchodního či jiného vztahu.

Správce se přizváním zpracovatele a priori nezbavuje odpovědnosti za zpracování osobních údajů.

Může zpracovatel zapojit do zpracování jiného zpracovatele?

Jde o tzv. řetězení zpracovatelů, které není a priori zakázáno, nicméně je nutné, aby správce k tomuto dal písemné svolení zpracovateli. Svolení může být dáno k dalšímu konkrétnímu zpracovateli, nebo může být dáno obecné svolení, v takovém případě však zpracovatel musí správce informovat o veškerých přijetích dalších zpracovatelů nebo jejich nahrazení, přičemž u přibrání nového zpracovatele může správce vznést námitku. Účelem tak je, aby správce, který za zpracování osobních údajů primárně odpovídá, věděl, které subjekty pro něj osobní údaje zpracovávají.

Musí být měněny „staré“ smlouvy o zpracování osobních údajů mezi správcem a zpracovatelem?

V případě, že smlouvy odpovídají obsahově požadavkům obecného nařízení, resp. nemají s ohledem na kontext a účel zpracování výrazné nedostatky, není nutné je nově uzavírat. V opačném případě je nutné provést jejich nové sjednání, resp. aktualizaci tak, aby odpovídaly požadavkům obecného nařízení.

8. Zabezpečení osobních údajů

Jak musí správce zabezpečit osobní údaje?

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační. Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s obecným nařízením. Každý správce tak bude muset přijmout adekvátní bezpečnostní opatření a u každého správce takové opatření může být, právě s ohledem na povahu, rozsah a účely zpracování, odlišné.

Jedním z prvků zabezpečení osobních údajů je např. jejich pseudonymizace nebo šifrování. Tyto prvky však nejsou povinné. Jejich dobrovolné nasazení však správci může přinést i zproštění např. povinnosti ohlásit případ porušení zabezpečení osobních údajů subjektu údajů.

Co se rozumí porušením zabezpečení osobních údajů?

Za porušení zabezpečení osobních údajů se považuje porušení zabezpečení, které vede k

náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Pokud dojde k porušení zabezpečení osobních údajů, měl by správce zvážit, zdali nejde o okolnost, kterou je nutné ohlásit dozorovému úřadu, resp. oznámit subjektu údajů. Tyto povinnosti nastanou tehdy, pokud porušení zabezpečení představuje riziko, resp. vysoké riziko pro práva a svobody fyzických osob.

Kdy a co musí správce při bezpečnostním incidentu ohlásit Úřadu pro ochranu osobních údajů?

Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu (Úřadu pro ochranu osobních údajů), ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Oznamují se jen rizikové incidenty pro práva a svobody fyzických osob, nikoli bagatelní záležitosti, které jsou nerizikové.

Například používání pseudonymizace či šifrování může případné riziko zcela eliminovat a tudíž i zbavit správce nutnosti případ ohlásit dozorovému úřadu. Vždy je však nutné míru rizika posoudit, a to i v případě, že byla použita pseudonymizace či šifrování.

V oznámení správce subjektu údajů musí popsat povahu porušení zabezpečení, přijatá opatření, pravděpodobné důsledky a též musí sdělit kontaktní údaje na pověřence pro ochranu osobních údajů, byl-li ustaven.

Pokud nastane porušení zabezpečení u zpracovatele, hlásí jej správci, pro kterého dotčené osobní údaje zpracovává.

Pracovní skupiny WP29 vydala k ohlašování porušení zabezpečení osobních údajů své pokyny. Jejich neoficiální český překlad je v rubrice Schválené pokyny.

Kdy a co musí správce při bezpečnostním incidentu oznámit subjektu údajů?

V případě, že porušení zabezpečení představuje **vysoké riziko** pro práva a svobody subjektu údajů, vzniká správci povinnost zpravit o této události subjekt údajů. Správce tak nemusí činit, pokud použil předběžná opatření, která činí osobní údaje nečitelnými pro všechny neoprávněné osoby (např. šifrování nebo unikly pseudonymizované údaje bez vazby na subjekt údajů) či použil následná opatření, která zajistí, že vysoké riziko se již pravděpodobně neprojeví. Povinnost oznámit bezpečnostní incident subjektu údajů správci nenastane ani tehdy, pokud by to vyžadovalo nepřiměřené úsilí. V takovém případě však musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení.

Pracovní skupiny WP29 vydala k ohlašování porušení zabezpečení osobních údajů své pokyny. Jejich neoficiální český překlad je v rubrice Schválené pokyny.

Jak se určí riziko porušení zabezpečení?

Při určování rizika porušení zabezpečení bude nutné vycházet zejména z kategorie osobních

údajů, které byly porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovnictví).

Dalším rozhodným prvkem může být i okolnost, zdali došlo k porušení zabezpečení úmyslně či nedbalostně, přičemž úmyslný čin výrazně zvyšuje riziko takového činu, jelikož osobní údaje byly terčem útoku. Porušení zabezpečení se tak musí provést komplexně, nikoli izolovaně a vyšlé riziko následně určí eventuální povinnost oznámit porušení zabezpečení Úřadu pro ochranu osobních údajů nebo i oznámit subjektu údajů.
Modelové situace jsou popsány ve schválených pokynech Pracovní skupiny WP29.

Musí být vždy osobní údaje u správce v šifrované nebo pseudonymizované podobě?

Šifrování ani pseudonymizace nejsou výslovnou podmínkou zpracování osobních údajů. Jsou bezpečnostním prvkem, který i v některých případech může správci zlepšit jeho postavení v případě úniků těchto údajů, jelikož v takovém případě se na něj nemusí (v závislosti na případu, neznamená to, že pokaždé) vztahovat povinnost ohlašovat případ porušení zabezpečení osobních údajů dozorovému úřadu, resp. jej oznamovat subjektu údajů. Vždy je však nutné míru rizika posoudit, a to i v případě, že byla použita pseudonymizace či dostatečně silné šifrování a zdali nedošlo i ke kompromitaci šifrovacího klíče.

Lze proto doporučit správcům, jejichž povaha zpracování osobních údajů jim to umožňuje, uchovávat (zpracovávat) údaje v šifrované či pseudonymizované podobě, k čemuž i obecné nařízení nabádá.

9. Pověřenec pro ochranu osobních údajů

Jako doplňující informace k této kapitole lze využít:

Schválené pokyny Pracovní skupiny WP29 k pověřencům pro ochranu osobních údajů,
metodický materiál MV, kde naleznete informace ohledně pověřenců pro obce,
důležitý materiál MŠMT k pověřencům pro školská zařízení.

Kdo musí jmenovat pověřence pro ochranu osobních údajů?

Pověřence musí jmenovat správce a zpracovatel pokud:

zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,
hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobích údajů a osobních údajů týkajících se rozsudků v trestních věcech.

Jak vidno, povinnost jmenovat pověřence pro ochranu osobních údajů se netýká všech správců

nebo zpracovatelů.

Skupina podniků může jmenovat jediného pověřence, avšak musí být pro každý podnik snadno dosažitelný. Stejně tak lze i pro jmenování pověřence pro orgán veřejné moci či veřejný subjekt přihlédnout k jejich organizační struktuře a jejich velikosti a ve vhodných případech pro ně jmenovat jednoho pověřence.

Musí být pověřenec organizačně podřízen přímo vedení organizace?

Pověřenec pro ochranu osobních údajů musí být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele. Nejde však o podmínku organizační, tj. že pověřence musí řídit přímo vedení organizace, ale jde o podmínku, aby pověřenec měl přímý přístup k vedení organizace, tj. aby při předávání informací vedení organizace nebyl mezi pověřencem a vedením další mezičlánek a pověřenec se tak na vedení organizace mohl kdykoli obrátit v záležitostech ochrany osobních údajů.

Jaké jsou úkoly pověřence pro ochranu osobních údajů?

Především poskytování informací a poradenství správci či zpracovateli, včetně zaměstnancům, kteří se na zpracování podílejí. Pověřenec dále monitoruje soulad zpracování s obecným nařízením a dalšími předpisy. Pověřenec poskytuje na vyžádání poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů. Pověřenec může vypracovat záznamy o činnostech zpracování. Nedílnou součástí výkonu funkce pověřence je dále spolupráce s Úřadem pro ochranu osobních údajů a působení jako kontaktní místo.

Pověřenec může plnit i ostatní úkoly, ale při jejich plnění se nesmí dostat do střetu zájmů s funkcí pověřence.

Kdy může docházet ke střetu zájmu u pověřence?

Především tehdy, pokud by určoval účel zpracování osobních údajů (např. jako statutární orgán). Zároveň střet zájmů může představovat zvláštní zákon, pokud by pověřenci v určitých momentech mohl znemožňovat jeho činnost (např. zvláštní mlčenlivost pro některá svobodná povolání).

Jaké má mít pověřenec pro ochranu osobních údajů vzdělání?

Obecné nařízení nestanovuje přesné požadavky na vzdělání pověřence ve smyslu akademických titulů. Pověřenec musí být osoba disponující profesními kvalitami a odbornou znalostí práva a praxe v oblasti ochrany osobních údajů a musí dostatečně ovládat obecné nařízení. Každému správci může vyhovovat pověřenec s jiným vzděláním (např. právní vzdělání versus technické).

Musí být pověřenec pro ochranu osobních údajů certifikován?

Obecné nařízení nestanovuje certifikaci pověřence jako předpoklad výkonu funkce pověřence. Obecné nařízení ani nijak s certifikacemi pověřenců nepracuje, tj. ani je nepředpokládá. Pověřenec tak certifikát mít nemusí a správce může jako pověřence vybrat i necertifikovanou osobu, která disponuje dostatečným právním povědomím o ochraně osobních údajů a obecném nařízení. Do budoucna není vyloučen vznik subjektů, které se „certifikace“ pověřenců chopí, nicméně využití certifikace pověřence bude na dobrovolné bázi, a to jak ze strany pověřence, tak ze strany správce, který nemá povinnost vybírat certifikovaného pověřence. Takto pojatá certifikace však nebude certifikací ve smyslu článku 42 obecného nařízení.

Může poskytnout pověřence i právnická osoba? Např. jako službu?

Obecné nařízení tuto možnost nevylučuje, resp. umožňuje i jeho fungování na základě smlouvy o poskytování služeb. Vždy však musí být, v případě, že pověřence jako službu poskytuje právnická osoba, určena konkrétní fyzická osoba, která pověřence bude vykonávat. Při uvažování o využití služby pověřence by měl správce vzít v úvahu i to, že pověřencem by měla být osoba, která zpracování osobních údajů u správce detailně pozná a pouze tak dokáže identifikovat případná riziková místa či slabiny, což u najatého pověřence být vždy nemusí. Také je vhodné zvážit konkurenční hledisko, kdy jeden poskytovatel pověřence může poskytovat stejného pověřence i pro konkurenta a hrozí tak i vyzrazení know-how.

10. Předávání osobních údajů do jiných zemí

Jak lze předávat osobní údaje do zemí Evropské unie?

Platí zásada, že volný pohyb osobních údajů v Evropské unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán. Tuto premisu však nelze považovat za právní důvod k předávání osobních údajů jakémukoli správci či kdykoli. Možnost předávat osobní údaje bez omezení v Evropské unii se týká institucionálního zabezpečení, tj. je vyjádřeno to, že v zemích Evropské unie platí stejný vysoký standard právního rámce ochrany osobních údajů při jejich zpracování a není tak nutné dodatečně zajišťovat jejich institucionální bezpečnost. K samotnému předání jinému správci musí mít správce právní důvod, jelikož i předání je jednou z činností zpracování či lze osobní údaje předat zpracovateli. Právní důvod musí mít správce i tehdy, pokud předává osobní údaje do země mimo Evropskou unii (nebo pokud předává osobní údaje zpracovateli), kdy ještě navíc musí být splněny podmínky pro předání osobních údajů i z hlediska jejich institucionálního zabezpečení. Nesmíme opomenout, že nařízení bude platit navíc i na Islandu, Norsku a Lichtenštejnsku, tudíž i na tyto země je nutné pohlížet v tomto kontextu jako na součást Evropské unie.

Jaké jsou možnosti předávání osobních údajů do zemí mimo Evropskou unii?

Pokud správce chce předat jinému správci osobní údaje do země mimo Evropskou unii, musí být zajištěna jejich institucionální ochrana, tj. nelze (až na výjimky) předávat osobní údaje do zemí, kde není zajištěna dostatečná právní ochrana osobních údajů, resp. správce nepřijal

instrumenty, které tuto ochranu při předávání zajistí.

Možnosti předávání:

předání založené na rozhodnutí o odpovídající ochraně,
předání založené na vhodných zárukách,
o závazná podniková pravidla,
o standardní smluvní doložky
výjimky pro specifické situace, kdy nelze aplikovat jeden ze dvou shora uvedených bodů.

Co se rozumí předáním založeném na rozhodnutí o odpovídající ochraně?

Komise může rozhodnout, že konkrétní země zajišťuje odpovídající úroveň ochrany osobních údajů. V takovém případě se nevyžaduje zvláštní povolení a předání osobních údajů nejsou kladeny žádné administrativní překážky. Tato rozhodnutí jsou k dispozici na https://www.uoou.cz/prehled-pripadu-predavani-osobnich-udaju-do-zahranici-u-nichz-neni-nutne-zadat-urad-o-povoleni/ds-1649/archiv=0&p1=1633 v bodě 3.

Co se rozumí předáváním založeném na vhodných zárukách?

Pokud neexistuje rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů v dané zemi, mohou být osobní údaje do třetí země předány, pouze pokud přijímající správce poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektu údajů. Mezi tyto vhodné záruky patří zejména závazná podniková pravidla a standardní smluvní doložky.

Co jsou závazná podniková pravidla?

Závazná podniková pravidla je koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazen na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost. Jde tak o pravidla platící uvnitř správců, tvořících skupinu podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.

Co jsou standardní smluvní doložky?

Standardní smluvní doložky jsou instrumentem, na základě kterého lze předávat osobní údaje do třetích zemí (tedy mimo Evropskou unii, resp. státy, o nichž bylo Evropskou komisí rozhodnuto, že poskytují adekvátní ochranu). Jde o standardizovaný text, kterým se příjemce osobních údajů zavazuje dodržovat pravidla odpovídající pravidlům platícím v Evropské unii. Jinými slovy díky použití tohoto instrumentu se nesníží ochrana předávaných osobních údajů. Text standardních smluvních doložek viz https://www.uoou.cz/standardni-smluvni-dolozky/ds-3505

A co specifické situace? Např. když cestovní kancelář předává osobní údaje hotelům do různých zemí světa?

Vyjma shora uvedených případů (instrumentů) předávání osobních údajů lze osobní údaje do třetí země předat, pokud je splněna alespoň jedna z podmínek uvedených v článku 49 odst. 1 obecného nařízení. Např. v případě informovaného výslovného souhlasu subjektu údajů, nebo pokud je takové předání nezbytné pro splnění smlouvy mezi subjektem údajů a správcem osobních údajů.
Více ke specifickým výjimkám zmíněné ustanovení článku 49 odst. 1 obecného nařízení a též i vodítka Pracovní skupiny WP29 http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846.

11. Sankce, pokuty

Pracovní skupina WP29 vydala k této oblasti oficiální dokumenty. K dispozici jsou v rubrice Schválené pokyny.

Jaké jsou podmínky pro ukládání pokut?

Ukládání správních pokut musí být účinné, přiměřené, ale zároveň odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu, a to kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j) obecného nařízení. Podstatné tedy je, že nikoli za každé porušení obecného nařízení musí být udělena pokuta, ale správce může být například nejprve upozorněn, že zamýšlené operace zpracování pravděpodobně porušují obecné nařízení, nebo může být správci, jehož operace zpracování porušily obecné nařízení, uděleno napomenutí nebo mu může být nařízeno, aby vyhověl žádosti subjektu údajů. Správci může být mezi dalšími též nařízeno uvést zpracování do souladu s obecným nařízením atd.

Není tak pravdou, že každé porušení obecného nařízení bude představovat uložení správní pokuty.

Jak vysoká může být udělená pokuta?

V souvislosti s obecným nařízením je často skloňována výše pokut, kterou lze za porušení udělit. Výše pokut je rozdělena do dvou skupin dle porušení, jakého se správce dopustil. Pokutu lze udělit buď do výše 10 000 000 EUR (nebo až do 2% celkového ročního celosvětového obratu, jde-li o podnik) nebo do výše 20 000 000 EUR (nebo až do 4% celkového ročního celosvětového obratu, jde-li o podnik). Rozdělení do dvou skupin odráží důležitost porušených povinností, kdy ve skupině s vyšší sazbou jsou povinnosti, u jejichž porušení je očekávána vyšší intenzita zásahu do práva na ochranu osobních údajů, které obecné nařízení zajišťuje. Do nižší sazby spadá např. porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, zatímco do vyšší sazby jsou například zahrnuta porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva

subjektu údajů.

Jsou při ukládání pokut polehčující či přitěžující okolnosti?

Polehčující a přitěžující okolnosti jsou vyjmenovány v čl. 83 odst. 2 písm. a) až k) obecného nařízení. Brána v úvahu bude zejména povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu a účelu zpracování, kategorií údajů a počtu dotčených subjektů údajů, zda se jednalo o úmyslné či nedbalostní porušení, kroky podniknuté správcem a spolupráce s Úřadem pro ochranu osobních údajů atd. Viz úplný výčet okolností, které se při rozhodování o výši pokuty zohledňují.

Jak může postupovat subjekt údajů, pokud mu vznikla v souvislosti se zpracováním jeho osobních údajů škoda?

Pokud vznikla subjektu údajů hmotná či nehmotná újma v důsledku porušení obecného nařízení ze strany správce či zpracovatele, má právo na úhradu újmy. Nejčastěji to bude znamenat obrátit se přímo s žádostí o náhradu na správce či zpracovatele, a pokud ten nebude dobrovolně plnit, bude se subjekt údajů muset obrátit na soud.

12. Různé

Co je to Pracovní skupina WP29?

Pracovní skupina WP29 je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie. Mezi její činnosti patří mimo jiné posuzování otázek týkajících se uplatňování vnitrostátních předpisů přijatých k provedení směrnice 95/46/ES s cílem přispívat k jejich jednotnému uplatňování. Pracovní skupina WP29 může z vlastního podnětu podat doporučení k jakékoli otázce týkající se ochrany osob v souvislosti se zpracováním osobních údajů. Výstupem známým veřejnosti tak jsou stanoviska a doporučení této skupiny, týkající se oblasti zpracování osobních údajů či aktuálních témat. Stanoviska a doporučení Pracovní skupiny WP29 lze nalézt zde: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

V souvislosti s obecným nařízením nyní pracovní skupina WP29 vydává k jednotlivým institutům obecného nařízení metodické materiály, které obsahují vodítka pro správce a zpracovatele. Vydaná vodítka jsou k dispozici v českém překladu na: https://www.uoou.cz/schvalene-pokyny/d-28603

Pracovní skupina WP29 nabytím použitelnosti obecného nařízení bude transformována na Evropský sbor pro ochranu osobních údajů. Úkolem Sboru bude především zajišťování jednotného uplatňování obecného nařízení a za tím účelem monitorovat jeho uplatňování a vydávat pokyny, doporučení a osvědčené postupy, a to i pro některé stanovené oblasti a instituty obecného nařízení.

Poskytuje Úřad konzultace k obecnému nařízení?

S ohledem na možnosti Úřadu pro ochranu osobních údajů jsou konzultace ohledně obecného nařízení zaměřeny zejména na sdružení či asociace zastupující sektorově jednotlivé správce, s nimiž jsou projednávána specifika daného sektoru. Předpokládá se, že tyto subjekty, zastupující své členy, na ně následně přenesou nabytou znalostní bázi a tito členové v pozicích správců či zpracovatelů se nebudou muset samostatně obracet na Úřad pro ochranu osobních údajů. Konzultace Úřad však poskytuje i jednotlivým správcům či zpracovatelům a subjektům údajů.

Umístění: Složky dokumentů > Mapa stránek > Hlavní menu > GDPR (obecné nařízení) > Základní příručka k GDPR
