Deloitte.
Legal

PŘÍRUČKA K PROBLEMATICE OCHRANY OSOBNÍCH ÚDAJŮ

Prosinec 2017

Obsah

1. Účel GDPR Příručky

Účelem příručky k problematice ochrany osobních údajů (dále jen „GDPR Příručka") je poskytnout vodárenským společnostem, jako členům Sdružení oboru vodovodů a kanalizací České republiky (dále jen „SOVAK"), základní informace o ochraně osobních údajů a o zásadách, které musejí dodržovat při jejich zpracování.

GDPR Příručka je zejména zaměřena na aspekty ochrany osobních údajů, které jsou relevantní pro vodárenské společnosti. Součástí GDPR Příručky je i vysvětlení nejdůležitějších pojmů (Příloha č. 1), které se v souvislosti s ochranou osobních údajů používají, jakož i odpovědi na nejčastěji kladené dotazy (Příloha č. 2).

GDPR Příručka dále vysvětluje, jaká jsou práva jednotlivých fyzických osob, tzv. subjektů osobních údajů, jaké jsou požadavky na správce osobních údajů i povinnosti pro zpracovatele, zejména pak s ohledem na požadavky Nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen "**GDPR**").

Zde uvedené informace, doporučení a metodika zcela vychází z relevantních právních předpisů pro oblast ochrany osobních údajů a vodárenství, stejně jako ze stanovisek Úřadu pro ochranu osobních údajů (dále jen „**ÚOOÚ**") k vybraným aspektům ochrany osobních údajů.

V rámci činnosti SOVAK a všech vodárenských společností, které jsou jeho členy (dále jen „**vodárenské společnosti**") dochází ke zpracování velikého množství osobních údajů, typicky odběratelů, zaměstnanců a dodavatelů, které jsou ukládány v příslušných databázích.

Účelem této GDPR Příručky je poskytnout ty nejdůležitější informace o problematice ochrany osobních údajů, s níž se vodárenské společnosti při výkonu své činnosti budou typicky setkávat.

Tato GDPR Příručka byla zpracována pro SOVAK. Jedná se tedy o metodickou pomůcku pro vodárenské společnosti, nikoliv však o kodex chování dle čl. 40 GDPR nebo o dokument popisující komplexní řešení požadavků vyplývajících z GDPR pro konkrétní společnost. S ohledem na skutečnost, že i SOVAK musí coby správce osobních údajů plnit své povinnosti dle GDPR, vztahují se na něj zde uvedená doporučení a metodika obdobně jako na vodárenské společnosti.

2. Ochrana osobních údajů v kontextu vodárenských společností aneb co bychom měli vědět

Osobní údaje v současné době představují jednu z nejcennějších hodnot, jakou vodárenské společnosti disponují. Tomu odpovídají i přísné sankce za nedostatečnou ochranu osobních údajů a porušení práv subjektů údajů.

Ochrana osobních údajů je v současné době velmi aktuálním tématem. S rozvojem moderních technologií, zejména pak v oblasti digitalizace, se předpokládá, že rozsah zpracovávaných osobních údajů se bude do budoucna dále zvětšovat.

Pokud by došlo k úniku osobních údajů z vodárenské společnosti, mohlo by dojít k jejich zneužití různými způsoby. Třetí osoby by za použití uniklých osobních údajů mohly nabízet nevyžádané služby a zboží. Určité údaje by mohly být zneužity dokonce i k žádosti o půjčku nebo objednání zboží jménem osoby, jejíž údaje z vodárenské společnosti unikly. Samotný únik osobních údajů by také mohl velmi poškodit dobré jméno vodárenské společnosti, stejně jako by mohl mít velmi negativní dopad na její obchodní vztahy a procesy. V neposlední řadě by porušení ochrany osobních údajů mohlo mít pro vodárenskou společnost negativní ekonomický dopad, pokud by pokuta uložená ÚOOÚ

byla obzvláště citelná. ÚOOÚ může totiž uložit sankce až do výše 20 000 000 EUR nebo 4 % celosvětového ročního obratu dotčené společnosti.

Všechny osobní údaje je tedy nutné pečlivě chránit. Ochrana osobních údajů, její funkčnost a soulad s právními předpisy ze strany všech vodárenských společností je prioritní. Jelikož celosvětový pokrok při zavádění nových technologií s sebou současně nese vyšší rizika útoků, jejichž cílem je neoprávněný přístup k osobním údajům, měla by být přijata vhodná a účinná opatření, jimiž se předejde incidentům, které by mohly vést k úniku osobních údajů.

Je proto důležité se ochraně osobních údajů pečlivě věnovat a dodržovat pravidla zakotvená v právních předpisech a procesních a organizačních dokumentech vodárenských společností.

3. Právní úprava ochrany osobních údajů a interní předpisy

Hierarchii právní regulace osobních údajů tvoří:
1. evropské nařízení GDPR,
2. český adaptační zákon doplňující GDPR, a
3. interní předpisy SOVAK a vodárenských společností.

První úroveň a základní právní rámec ochrany osobních údajů poskytuje od 25. května 2018 Nařízení EU známé pod označením GDPR, které se k tomuto datu stane přímo závazné ve všech zemích EU, a tím dojde i ke sjednocení ochrany osobních údajů v EU.

Druhou úroveň úpravy by měl od 25. května 2018 tvořit vedle GDPR v ČR i tzv. adaptační zákon, který bude blíže specifikovat a doplní některá ustanovení GDPR. Do přijetí adaptačního zákona a účinnosti GDPR se však uplatňuje výhradně úprava dle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Třetí úroveň úpravy ochrany osobních údajů tvoří konkrétní pokyny pro postup při nakládání s informacemi a osobními údaji v rámci SOVAK a vodárenských společností. Tyto pokyny jsou po jejich přijetí jako interních předpisů závazné pro všechny osoby, které v rámci dané společnosti přichází s osobními údaji do styku. Může se jednat se o následující procesní a organizační normy:

I. Organizační norma „Ochrana osobních údajů" upravující pravidla pro ochranu osobních údajů a práva a povinnosti při jejich zpracování.

II. Organizační norma „Bezpečnost informací" obsahující základní pravidla a postupy k zajištění bezpečnosti informací, která odpovídá úpravě relevantních právních předpisů a mezinárodních standardů.

III. Organizační norma „Spisový a skartační řád" stanovující zásady výkonu spisové služby, tj. zacházení s dokumenty a archivace.

Pokud vodárenské společnosti těmito vnitřními předpisy nedisponují, je v jejich nejlepším zájmu takové předpisy přijmout, aby došlo k přesnému nastavení pravidel ochrany osobních údajů ze strany těch osob, které s osobními údaji při výkonu své pracovní činnosti nakládají.

4. Co je osobním údajem a kdo je subjektem údajů?

Osobními údaji jsou veškeré informace týkající se konkrétní osoby, jež je díky těmto informacím identifikovaná nebo identifikovatelná. Osobním údajem je tedy každá informace, kterou lze přiřadit ke konkrétní osobě.

S ohledem na právní vymezení osobních údajů může být v oblasti vodárenství považován za osobní údaj např. údaj o spotřebě vody či informace o tom, kdy vodu příslušný odběratel využívá, pokud lze tento údaj přiřadit ke konkrétní identifikovatelné (či již identifikované) osobě.

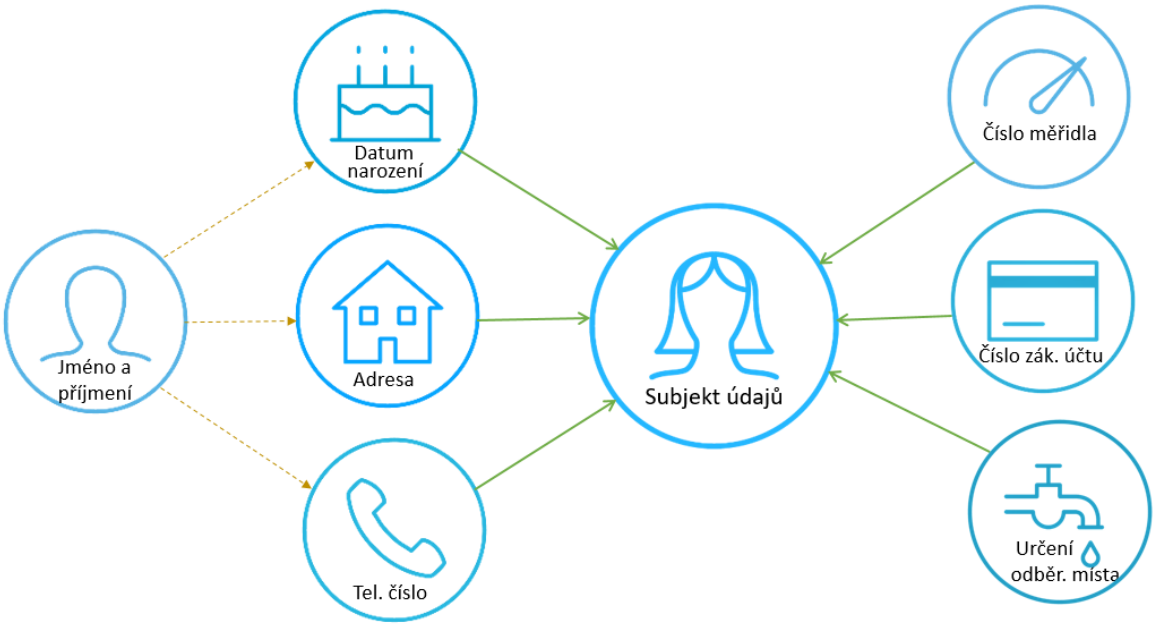
GDPR přitom poskytuje ochranu pouze osobám fyzickým, nikoliv osobám právnickým. Tyto osoby se označují jako subjekty údajů. O jejich právech pojednává podrobněji kapitola 8 této GDPR Příručky. Subjekty osobních údajů v oblasti vodárenství tak jsou zásadně tři skupiny fyzických osob:

1) Odběratelé,
2) Zaměstnanci,
3) Dodavatelé.

a. Osobní údaje odběratelů

Pokud je odběratelem nikoliv fyzická osoba, ale např. určitá obchodní korporace, společenství vlastníků jednotek či jakákoliv právnická osoba obecně, může být subjektem údajů fyzická osoba, která za tuto právnickou osobu jedná (např. člen výboru společenství vlastníků jednotek či jeho předseda, který z pozice statutárního orgánu uzavře odběratelskou smlouvu za toto společenství). Subjektem údajů však nikdy nemůže být ten odběratel, který je právnickou osobou nebo organizační složkou státu.

Schéma, kdy se určitý údaj stává osobním údajem:



Jméno a příjmení osoby samo o sobě zpravidla nestačí k identifikaci konkrétní osoby. V databázi odběratelů vodárenské společnosti se totiž může vyskytovat více fyzických osob se stejným jménem a příjmením. V takovém případě nelze pouze na základě tohoto údaje určit, o kterého konkrétního odběratele (coby fyzickou osobu) či zástupce odběratele (pokud je odběratel právnickou osobou)

se jedná. Pokud se však tento údaj spojí s jinými identifikátory (např. datum narození, adresa bydliště, telefonní číslo fyzické osoby), zpravidla již identifikaci konkrétní osoby provést lze. Některé údaje jsou oproti tomu natolik jedinečné, že nemusí být spojeny s jinými, aby došlo k jednoznačné identifikaci odběratele coby subjektu údajů (např. číslo vodoměru, číslo zákaznického účtu, určení odběrného místa).

Jedinečným údajem je i rodné číslo odběratele coby fyzické osoby. Jako u všech ostatních osobních údajů musí být i v případě rodného čísla naplněna zásada, že je tento údaj zpracováván zákonným způsobem (tedy pro konkrétně vymezený účel a na základě právního titulu). Pokud rodné číslo odběratele příslušná vodárenská společnost nepotřebuje za účelem plnění uzavřené odběratelské smlouvy, jedná se o nadbytečný (a tedy i nezákonně zpracovávaný) údaj, ledaže by k takovému zpracování udělil odběratel souhlas.

Osobním údajem nemůže být samotný údaj o spotřebě vody či informace o tom, kdy vodu příslušný odběratel využívá. Osobním údajem se tato informace stává až po jejím přiřazení ke konkrétnímu odběrateli, pokud je tento fyzickou osobou.

b. Osobní údaje zaměstnanců vodárenských společností

Subjektem osobních údajů jsou i zaměstnanci vodárenských společností. Tito zaměstnanci coby subjekty údajů požívají právní ochrany dle GDPR a mohou tak uplatňovat práva, která jím dle tohoto právního předpisu náleží. Osobním údajem zaměstnance bude typicky jeho jméno, příjmení, datum narození, kontaktní údaje, ale i např. číslo bankovního spojení pro účely zasílání mzdy či údaj o zdravotní pojišťovně, vůči níž bude vodárenská společnost coby zaměstnavatel plnit své zákonné povinnosti na úseku odvodu zdravotního pojištění. Osobním údajem je i záznam o docházce či hodnocení pracovní činnosti zaměstnance, pokud tento údaj lze ke konkrétnímu zaměstnanci přiřadit.

c. Osobní údaje dodavatelů vodárenských společností

Subjektem osobních údajů jsou i dodavatelé vodárenských společností, pokud se jedná o fyzické osoby. Pokud je dodavatelem právnická osoba, bude subjektem údajů typicky osoba, která je kontaktní osobou pro tohoto dodavatele. Osobním údajem tohoto subjektu pak typicky bude jeho jméno a příjmení, stejně jako jeho telefonní číslo či emailová adresa (či kontaktní údaje obecně).

d. Zvláštní kategorie osobních údajů

Zvýšenou pozornost je nutné věnovat tzv. zvláštní kategorii osobních údajů, do níž spadají např. údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, údaje o členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby. Zvláštní kategorie údajů je vysvětlena i v Příloze č. 1 této GDPR Příručky. V případě odběratelských smluv či dodavatelských vztahů lze předpokládat, že se se zvláštní kategorií osobních údajů ve vodárenství nepotkáme. V případě zaměstnaneckých vztahů je však evidence členství zaměstnance v odborech běžná.

Zpracování těchto osobních údajů podléhá přísnějšímu režimu a pro správce osobních údajů může znamenat dodatečné povinnosti (např. jmenování pověřence pro ochranu osobních údajů – pokud hlavní činnost správce nebo zpracovatele spočívá v rozsáhlém zpracování takových údajů, vedení záznamů o činnostech zpracování či vypracování posouzení vlivu na ochranu osobních údajů). Zvláštní kategorie osobních údajů lze zpracovávat pouze za splnění předpokladů stanovených GDPR (např. udělení výslovného souhlasu subjektem osobních údajů, plnění povinností a výkon zvláštních práv správce v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany či ochrana jeho životně důležitých zájmů).

5. Zásady zpracování osobních údajů a pravidla sdílení

Staronová pravidla nakládání s osobními údaji je nutné dodržovat všude v EU pod hrozbou milionových sankcí. Povinnost dodržování všech zásad ochrany osobních údajů se vztahuje na všechny správce a zpracovatele bezvýjimečně.

a. Zásada zákonnosti (Kdy mám právo zpracovávat osobní údaje)

Zpracování osobních údajů musí být vždy založeno na alespoň jednom z právních titulů (např. plnění smlouvy, zákonné povinnosti, udělení souhlasu, atd.). Zároveň zpracování osobních údajů nesmí probíhat za nelegálním či neoprávněným účelem.

b. Zásada korektnosti a transparentnosti (Informuji, co dělám)

Zpracování osobních údajů musí být vůči subjektu údajů otevřené a transparentní ohledně toho, jak je s osobními údaji nakládáno. Subjektům údajů musí být poskytnuty informace o způsobu zpracování jejich osobních údajů a o tom, komu budou údaje zpřístupněny. Subjekty údajů musí být v určitých případech informovány o porušení bezpečnosti či úniku osobních údajů, které má přímý dopad na práva subjektů údajů (např. vyzrazení finanční situace zaměstnance, omezení práv a svobod).

c. Zásada účelového omezení (Zpracovávám údaje pouze za určitým účelem)

Osobní údaje mohou být shromažďovány pouze pro určité a legitimní účely. Osobní údaje shromážděné např. pouze za účelem plnění odběratelské či pracovní smlouvy nelze komerčně prodávat třetím osobám.

d. Zásada minimalizace údajů" (Zpracovávám pouze údaje, které potřebuji, „need to know" princip)

Pro každý určitý účel lze zpracovávat pouze údaje nezbytné, relevantní a přiměřené. Je tedy možné zpracovávat pouze ty údaje, které potřebuji pro daný účel vědět (*„need to know*"). Není dovolené zpracovávat „nadbytečné" osobní údaje, jako například výpisy z rejstříku trestů zaměstnanců, ledaže jsou k tomu naplněny podmínky stanovené zákoníkem práce. Nadbytečným údajem by byly i údaje o majetkových poměrech odběratelů či rodná čísla dodavatelů jako fyzických osob.

e. Zásada přesnosti (Zpracovávám aktuální a přesné údaje)

Zpracovávané osobní údaje musí být přesné, tj. odpovídající skutečnosti, a musí být pravidelně aktualizované. Nepřesné osobní údaje je nutné vymazat, resp. opravit (např. na podnět odběratele je nutné provést změnu kontaktních údajů, změnu příjmení apod.). Aktuálnost osobních údajů by se měla pravidelně ověřovat a v případně nutnosti aktualizovat.

f. Zásada omezení uložení (Údaje zpracovávám jen po nezbytnou dobu)

Zpracovávané osobní údaje mohou být uchovávány pouze po dobu, která je nezbytná pro daný účel zpracování. Jakmile uplyne doba pro zpracování osobního údaje nebo pomine účel, za kterým byl zpracováván, je nutné jej vymazat nebo anonymizovat. Ve vztahu k osobním údajům v dokumentech je nezbytné postupovat podle pravidel uvedených ve skartačním řádu vodárenské společnosti, pokud takový vnitřní předpis existuje.

Doba uchování může např. vyplývat ze smlouvy, z uděleného souhlasu či ze zákona. Osobní údaje z odběratelských či dodavatelských smluv musí být uchovávány minimálně po dobu trvání smluvního vztahu (v takovém případě bude zpracování založeno na právním titulu plnění uzavřené smlouvy), případně i po přiměřenou dobu po skončení smluvního vztahu, např. v tříleté promlčecí lhůtě pro případné nároky z odběratelské smlouvy (v takovém případě bude zpracování založeno na právním titulu oprávněného zájmu vodárenské společnosti). Příkladem povinnosti uchovávat osobní údaje dle ustanovení zákona může být archivace evidenčních listů důchodového pojištění zaměstnance

vodárenské společnosti po dobu 3 kalendářních let po roce, v němž byly vyhotoveny, a to v souladu se zákonem o organizaci a provádění sociálního zabezpečení.[1]

g. *Zásada integrity a důvěrnosti, „need to know" princip (Údaje musím chránit)*

Osobní údaje musí být zabezpečeny, chráněny před neoprávněným či protiprávním zpracováním, před ztrátou či zničením. Z těchto důvodů je nutné přijmout jak technická (např. nastavení dostatečné síly hesla a jeho pravidelná obměna či zálohování dat), tak i organizační (např. fyzické omezení přístupu, uzamykání místností, politika čistého stolu apod.) opatření.

K osobním údajům by měli mít přístup pouze vybraní zaměstnanci vodárenské společnosti, kteří s těmito údaji v rámci svého pracovního zařazení pracují (tzn. *„need to know"* princip, např. k osobním složkám zaměstnanců by měli mít přístup jen vybraní zaměstnanci z personálního oddělení).

6. Správce a zpracovatel – kdo je kdo a kdo co dělá?

Jednou z nejzásadnějších povinností správců i zpracovatelů je zabezpečení osobních údajů. Jedná se o doposud nejčastěji a téměř nejpřísněji sankcionovanou povinnost ze strany UOOÚ.

a. Správce

Pod pojmem správce osobních údajů se skrývá jakákoli entita, která určuje účel a prostředky zpracování osobních údajů, přičemž zpracováním se rozumí jakákoliv operace nebo soubor operací s osobními údaji, např. jejich shromažďování, zpracovávání, uspořádávání, strukturování apod. Správcem je tedy každá vodárenská společnost, bez ohledu, zda se jedná o vlastníka či provozovatele, a to jak ve vztahu k osobním údajům svých zaměstnanců, tak k osobním údajům případných odběratelů a dodavatelů.

Správce odpovídá za dodržení všech povinností upravených v GDPR, hlavně za bezpečnost údajů (tj. že nedojde k jejich ztrátě, úniku apod.) a za dodržení zásad zpracování, přičemž jejich dodržení musí být správce schopen doložit relevantními interními dokumenty či jinými postupy, z nichž bude tato skutečnost jasně vyplývat.

Klíčovým dokumentem k prokázání plnění těchto povinností společností může být vedení tzv. záznamů o činnostech zpracování. Za vyplňování záznamů o činnostech zpracování odpovídají správci, kteří je musí pravidelně aktualizovat při každé změně nebo zavedení nového procesu zahrnujícího zpracování osobních údajů. Záznamy o činnostech zpracování musí obsahovat velmi široký okruh informací, který je vymezen v čl. 30 GDPR. Mezi tyto informace patří např. identifikace správce a případného pověřence pro ochranu osobních údajů, účely zpracování či popis kategorií subjektů údajů a kategorie osobních údajů.

Povinnost vedení záznamů o činnostech zpracování se na vodárenskou společnost jako správce osobních údajů vztahuje pouze za podmínky, že zaměstnává více než 250 osob. Tato povinnost je dále dána i v situaci, kdy vodárenskou společností prováděné zpracování vykazuje následující znaky:

- Je pravděpodobně rizikové pro práva a svobody subjektů údajů, nebo
- Není příležitostné, nebo
- Zahrnuje osobní údaje spadající do tzv. zvláštní kategorie údajů (více viz kapitola 4 této GDPR Příručky), nebo
- Zahrnuje osobní údaje týkající se rozsudků v trestních věcech a trestných činů.

[1] § 35a odst. 4 písm. a) zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.

Pokud by zpracování prováděné vodárenskou společností některý z výše uvedených znaků skutečně naplňovalo, měla by dotčená vodárenská společnost jako správce povinnost k vedení záznamů o činnostech zpracování.

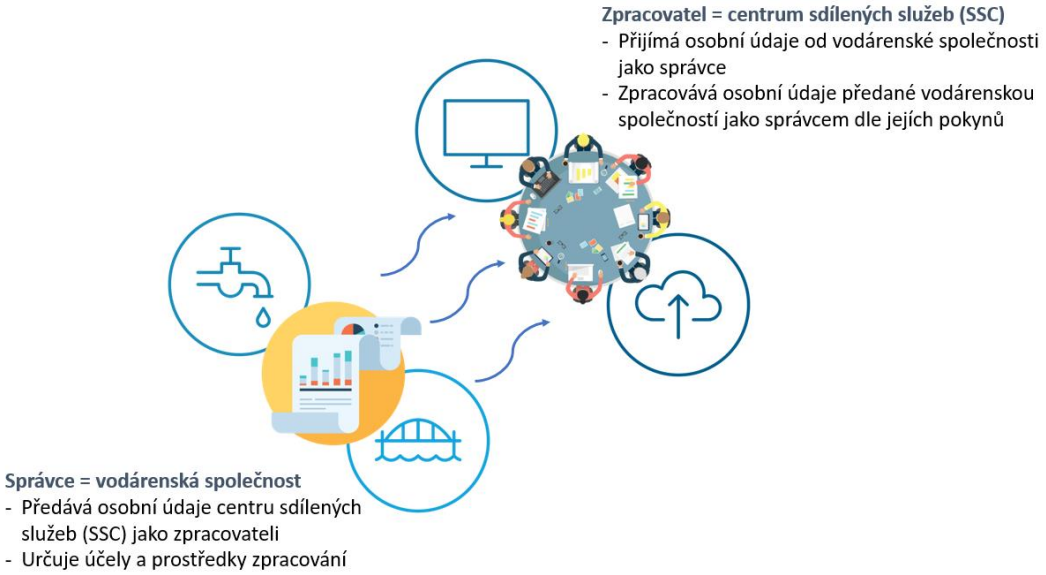
K základním povinnostem vodárenské společnosti coby správce patří dále povinnost zajistit dostatečnou ochranu osobních údajů. V případě narušení bezpečnosti osobních údajů (např. únik, ztráta apod.) musí správce takovýto incident nejpozději do 72 hodin ohlásit ÚOOÚ a pokud by daný případ porušení mohl mít za následek vysoké riziko pro práva a svobody fyzických osob, rovněž dotčenému subjektu údajů, a to bez zbytečného odkladu. Pokud tedy dojde k jakémukoliv porušení zabezpečení osobních údajů, je příslušný zaměstnanec povinen o této skutečnosti nejpozději do 24 hodin vyrozumět pověřence pro ochranu osobních údajů (více viz kapitola 11 této GDPR Příručky), pokud byl v této vodárenské společnosti ustanoven, který následně učiní další potřebné kroky. Pokud pověřenec pro ochranu osobních údajů vodárenskou společností ustanoven nebyl, měla by být informace o porušení osobních údajů poskytnuta jiné společností určené osobě, a pokud ani tato osoba určena nebyla, jejímu statutárnímu orgánu.

b. Zpracovatel

Společnost může jako správce předávat zpracovávané osobní údaje dalším příjemcům, které pro ni budou v souladu s jejími pokyny osobní údaje zpracovávat. Zpracovatelem je například společnost, která pro vodárenskou společnost poskytuje externí služby ve věci správy mzdové agendy či služby typu centra sdílených služeb (SSC). Zpracovateli jsou tedy společnosti (či jednotlivci, vyjma zaměstnanců těchto příslušných společností), které poskytují vodárenské společnosti služby a využívají přitom osobní údaje, vůči nimž je příslušná vodárenská společnost v postavení správce.

Aby mohli zpracovatelé služby poskytovat, musí jim příslušná vodárenská společnost osobní údaje předat. Za předané osobní údaje odpovídá nadále správce, a tato odpovědnost se vztahuje i na zajištění dostatečné úrovně ochrany a zabezpečení prostřednictvím vhodných technických a organizačních prostředků (např. vhodným nastavením síly hesel a jejich pravidelnou obměnou, šifrováním dat, dvoufaktorovou autentifikací nebo nastavením fyzického omezení přístupu do prostor, kde jsou osobní údaje uchovávány) ze strany zpracovatele.

Je nejenom v zájmu vodárenských společností, ale i jejich odpovědností, aby příslušný zpracovatel dodržoval požadavky kladené GDPR na ochranu osobních údajů. Z toho důvodu je nezbytné uzavřít s každým zpracovatelem písemnou smlouvu o zpracování osobních údajů (více viz kapitola 7 této GDPR Příručky), která přesně definuje povinnosti, které musí zpracovatel dodržovat.



7. Pravidla předávání osobních údajů

Náležitý výkon činnosti správce se často neobejde bez aktu předání osobních údajů jiným subjektům, které mohou být v pozici správce či zpracovatele. Předávání osobních údajů musí vždy probíhat za dodržení všech pravidel stanovených právními předpisy.

V oblasti vodárenství bude k předávání osobních údajů na úrovni EU docházet v rámci následujících vztahů:

a) Správce X Zpracovatel;
b) Správce a Správce (Společní správci);
c) Správce X Správce (Oddělení správci).

Každá z výše uvedených možností právního postavení a úpravy vzájemných vztahů znamená pro dotčené subjekty různé právní následky, které jsou popsány níže. Vodárenská společnost bude zpravidla při předávání osobních údajů v pozici správce, který osobní údaje předá jinému zpracovateli. Dále může být i v pozici správce, který osobní údaje předává jinému správci, s nímž je v pozici společného správce. K předání jinému správci může dojít i za situace, kdy tento jiný správce sám určuje vlastní účely a prostředky zpracování, a proto je v postavení odděleného správce.

a. Předávání (sdílení) osobních údajů mezi správcem a zpracovatelem

Patrně nejčastější situací, kdy dochází ke sdílení osobních údajů v rámci vztahu správce (tj. vodárenské společnosti) a zpracovatele, je vedení mzdové agendy a zaměstnanecké evidence či využívání služeb centra sdílených služeb (SSC) coby externího subjektu či subjektu ve skupině.

Za účelem předávání osobních údajů zpracovatelům v rámci EU je ze strany správců (tj. vodárenských společností) nutné:

1. Stanovit účel zpracování osobních údajů;
2. Stanovit rozsah osobních údajů pro účely předávání;
3. Uzavřít smlouvu o zpracování osobních údajů. Ve smlouvě je nutné uvést:
    a. předmět,
    b. dobu trvání zpracování,
    c. povahu a účel zpracování,
    d. typ osobních údajů (např. identifikační a kontaktní osobní údaje),
    e. kategorie subjektů údajů (např. odběratel coby fyzická osoba),
    f. práva a povinnosti správce (např. povinnost informovat zpracovatele o změnách osobních údajů, právo pravidelných auditů a inspekcí u zpracovatele).
4. V případě nejasností kontaktovat pověřence pro ochranu osobních údajů (více viz kapitola 11 této GDPR Příručky), pokud jej správce jmenoval, případně jinou osobu určenou vodárenskou společností, či její statutární orgán;
5. Smlouvu o zpracování osobních údajů musí podepsat osoba/osoby disponující podpisovými oprávněními;
6. Předávání osobních údajů musí probíhat zabezpečenou cestou (např. šifrováním emailů, pomocí zašifrovaných zařízení na přenos dat, zasílání souborů opatřených heslem, zasílání pseudonymizovaných údajů, atd.), která je podrobněji specifikována v kapitole 10 této GDPR Příručky.

Správce osobních údajů má povinnost k poskytnutí informace o příjemci či kategorií příjemců osobních údajů (tj. i zpracovatelů). Tato informační povinnost, která se dle okolností vztahuje i na řadu jiných informací vymezených v čl. 13 GDPR, může být splněna v rámci příslušného ustanovení odběratelské, dodavatelské či pracovní smlouvy.

b. Předávání (sdílení) osobních údajů mezi správci

Příslušná vodárenská společnost coby správce může předávat osobní údaje i jiné společnosti jako správci, kdy tento bude určovat odlišný účel a prostředky zpracování. Mohlo by se například jednat

o situaci, kdy by provozovatel předal údaje o odběratelích vlastníkovi. V takovém případě by byly dotčené subjekty v postavení oddělených správců.

I pro takové předávání je třeba dodržet specifické podmínky:

1. Uzavřít písemnou smlouvu se správcem osobních údajů a zajistit, aby smlouva s tímto dalším správcem obsahovala zejména:
    a. rozsah předávaných osobních údajů,
    b. povinnost zajištění mlčenlivosti,
    c. povinnost přijetí vhodných opatření k zabezpečení osobních údajů.
2. Smlouvu se správcem osobních údajů musí podepsat osoba/osoby disponující podpisovými oprávněními;
3. Sdílení osobních údajů musí proběhnout za dodržení stanovených bezpečnostních opatření (viz výše uvedený bod 6).

S ohledem na skutečnost, že i oddělený správce je příjemcem osobních údajů, měl by být subjekt údajů informován o možnosti předání jeho osobních údajů v rámci příslušného ustanovení odběratelské, dodavatelské či pracovní smlouvy.

Pokud by vodárenská společnost předala osobní údaje jiné společnosti (a to i jiné společnosti v rámci skupiny), s níž by však společně určovala účely a prostředky zpracování, byly by tyto dotčené subjekty v postavení společných správců. Mohlo by se jednat o případ, kdy by více vodárenských společností v rámci skupiny sdílelo jednu databázi odběratelů, k níž by každá společnost měla vlastní přístup. V takovém případě by dotčené subjekty byly v postavení společných správců. Pokud by došlo k předání osobních údajů mezi vlastníkem a provozovatelem vodovodu a kanalizace pro veřejnou potřebu, a tito v rámci přístupu k databázi odběratelů společně určovali účel a prostředky zpracování, bude se opět jednat o společné správce.

Takové uspořádání vzájemných vztahů předpokládá uzavření transparentního ujednání, v němž by měly být vymezeny:

1. Podíly odpovědnosti za plnění povinností dle GDPR, zejména ve vztahu k výkonu práv subjekty údajů,
2. Povinnosti k plnění informační povinnosti dle čl. 13 a 14 GDPR,
3. Kontaktní místo pro subjekty údajů.

8. Práva subjektů údajů

Posílená práva subjektů údajů představují velkou organizační a procesní zátěž pro správce i zpracovatele, jakož i riziko milionových sankcí v případě neschopnosti těmto právům vyhovět.

Ochrana osobních údajů výslovně přiznává subjektům údajů následující práva:

- právo na poskytnutí informací o zpracování osobních údajů,
- právo na přístup k osobním údajům;
- právo na opravu osobních údajů;
- právo na výmaz osobních údajů;
- právo na omezení zpracování osobních údajů;
- právo na přenositelnost osobních údajů;
- právo vznést námitku proti zpracování osobních údajů; a
  právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování.

a. Právo na poskytnutí informací subjektu údajů

Vodárenská společnost jako správce osobních údajů musí subjektu údajů poskytnout informace o jejich zpracování. Informace musí být poskytnuty stručným, transparentním, srozumitelným a snadno přístupným způsobem.

Do okruhu povinně sdělovaných informací patří identifikace správce, kontaktní údaje na pověřence osobních údajů, byl-li ustanoven, účel zpracování (např. identifikace odběratele za účelem řádného plnění odběratelské smlouvy), právní titul (např. uzavřená odběratelská smlouva) či informace o době uchování osobních údajů (typicky po dobu trvání smluvního vztahu a přiměřenou dobu po jeho zániku).

b. Právo na přístup k osobním údajům

Každý subjekt údajů má právo získat od správce informaci, zda jsou jeho osobní údaje zpracovávány, a případně i jejich rozsah a kopii. Správce na vyžádání musí poskytnout informace o účelu zpracování, kategoriích dotčených osobních údajů či jejich příjemcích a dalších skutečnostech.

c. Právo na opravu

Subjekt údajů má právo na opravu nepřesných osobních údajů. Správce však správnost osobních údajů nemusí aktivně zjišťovat, stačí, že je na nesprávný či nepřesný údaj upozorněn. V takovém případě se žádostí musí zabývat a údaj opravit. Vedle práva na provedení opravy má subjekt údajů právo na doplnění údajů, pokud jsou neúplné.

d. Právo na výmaz

Toto právo je též označováno jako „právo být zapomenut" a odpovídá mu povinnost správce osobní údaje zlikvidovat. Pokud je tedy vodárenská společnost v postavení správce, má povinnost vymazat dotčené osobní údaje ze všech svých systémů a databází (více viz kapitola 10 této GDPR Příručky). Právo na výmaz lze uplatnit zejména v následujících případech:

- Odpadnutí účelu zpracování (správce již údaje nepotřebuje);
- Odvolání souhlasu subjektem údajů (přičemž současně neexistuje žádný jiný právní důvod zpracování osobních údajů, např. odběratelská smlouva);
- Vznesení námitky proti zpracování subjektem údajů, přičemž současně neexistují oprávněné zájmy správce (např. potenciální vymáhání peněžní pohledávky správce soudní cestou), pro něž by bylo možné ve zpracování pokračovat, nebo vznesení námitky proti zpracování pro účely marketingu,
- Protiprávní zpracovávání osobních údajů;

e. Právo na přenositelnost údajů

Konkrétní subjekt údajů může zažádat o přenesení osobních údajů k jinému správci. V tomto případě musí správce poskytnout a předat tyto údaje ve strukturovaném, běžně používaném a strojově čitelném formátu. Právo lze uplatnit, jen pokud je zpracování založeno na souhlasu nebo smlouvě a současně se jedná o automatizované zpracování, tedy takové zpracování, které probíhá výlučně prostřednictvím technických prostředků na základě předem určeného algoritmu a bez jakéhokoliv zásahu člověka. S ohledem na přirozený monopol ve vodárenství si lze přenositelnost údajů mezi jednotlivými vodárenskými společnostmi jen těžko představit.

f. Právo vznést námitku

Toto právo je obdobou práva na odvolání souhlasu. Tam, kde byl udělen souhlas se zpracováním, lze takový souhlas odvolat [viz výše pod písm. d)]. Tam, kde dochází ke zpracování na základě oprávněného zájmu (např. za účelem ochrany vlastního majetku), lze vznést námitku. Vznést námitku lze i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování, rovněž

pro účely vědeckého či historického výzkumu nebo pro statistické účely. Pokud je taková námitka oprávněná, měly by být osobní údaje v takové situaci vymazány a neměly by být dále zpracovány. Vodárenská společnost by je mohla dále zpracovávat pouze v situaci, kdy by prokázala, že její oprávněné zájmy převažují nad zájmy nebo základními právy a svobodami subjektu údajů.

g. Právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování

Pokud subjekt údajů toto právo uplatní, nemůže být předmětem takového rozhodnutí, které by nepřezkoumal člověk, tedy které bylo učiněno výhradně na základě automatizovaného zpracování osobních údajů, včetně profilování (*např. rozhodnutí peněžního ústavu o poskytnutí či neposkytnutí úvěru žadateli výhradně prostřednictvím webové či jiné aplikace, tedy zcela bez zásahu člověka*).

9. Právní tituly, účely zpracování a souhlasy se zpracováním údajů

Doposud nejvyšší pokutu ve výši 4,25 milionů Kč uložil ÚOOÚ za rozesílání nevyžádaných obchodních sdělení bez souhlasu subjektů údajů. Zpracování osobních údajů bez právního titulu představuje jedno z nejflagrantnějších a nejčastějších porušení předpisů o ochraně osobních údajů.

Každé zpracování osobních údajů musí být zákonné, tj. musí být stanoven účel, pro který se osobní údaje zpracovávají, a právní titul, který opravňuje správce je sbírat.

a. Právní tituly pro zpracovávání osobních údajů

Předpokladem zpracování osobních údajů je existence alespoň jednoho právního titulu, který představuje zákonný důvod zpracování.

Právními tituly pro zpracovávání osobních údajů dle GDPR jsou:

- **Plnění smlouvy** - zpracování je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro provedení opatření přijatých v době před uzavřením smlouvy na žádost tohoto subjektu údajů (např. *osobní údaje zpracovávané vodárenskou společností o odběrateli za účelem plnění odběratelské smlouvy*),
- **Souhlas** - subjekt údajů udělil souhlas se zpracováním pro jeden či více konkrétních účelů (např. *vodárenskou společností realizovaný marketing v podobě zasílání obchodních sdělení či newsletterů odběratelům o dalších službách, které vodárenská společnost poskytuje),*
- **Plnění právní povinnosti** - zpracování je nezbytné pro splnění právní povinnosti správce (např. *vodárenskou společností coby zaměstnavatelem vedená evidence údajů za účelem splnění její zákonné povinnosti odvést zdravotní pojištění na účet příslušné zdravotní pojišťovny*),
- **Ochrana zájmů subjektů údajů** - zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (např. *v budově vodárenské společnosti vznikne požár, společnost sdělí hasičům a záchranářům seznam zaměstnanců pracujících v budově, jakož i seznam všech návštěv v budově*),
- **Veřejný zájem** - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce (např. *policejním orgánem vedená evidence osob, která se v určité lokalitě pravidelně dopouští výtržností*),
- **Oprávněný zájem** - zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, avšak s výjimkou případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů (např. *monitoring recepce zákaznického centra vodárenské společnosti prostřednictvím kamerového systému či zpracování osobních údajů odběratele i po skončení smluvního vztahu pro účely možného vymáhání pohledávek za tímto odběratelem soudní cestou*). Zpracování osobních údajů na základě oprávněného zájmu předpokládá provedení

tzv. balančního testu, kdy je správcem vyhodnoceno, zda je zpracování přiměřené a má skutečně prioritu před zájmy a základními právy a svobodami subjektů údajů.

b. Účely zpracování

Účel zpracování představuje důvod, proč ke zpracování dochází. Stejné osobní údaje může správce zpracovávat pro různé účely. Například osobní údaje uvedené v odběratelské smlouvě může správce využívat za účelem plněné této smlouvy. Pokud si však správce obstará separátní souhlas (nikoliv však v rámci odběratelské smlouvy) pro zasílání marketingových sdělení, bude stejné údaje zpracovávat pro různé účely současně.

Pokud jsou osobní údaje legitimně zpracovávány pro více účelů a na základě více právních titulů a jeden z těchto účelů či titulů odpadne, neznamená to automaticky, že správce musí osobní údaje vymazat, ale tyto může i nadále zpracovávat pro zbylé účely na základě zbylých právních titulů.

c. Souhlas se zpracováním osobních údajů

Souhlasem se dle GDPR rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává formou písemného, elektronického či ústního prohlášení své svolení ke zpracování svých osobních údajů.

Souhlas musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje. Například souhlas není možné začlenit do smlouvy či obchodních podmínek. Znění souhlasu by tedy mělo být uvedeno v samostatném dokumentu. Souhlas se zpracováním osobních údajů by tak neměl být obsažen např. v odběratelských smlouvách, které by měly vždy obsahovat pouze osobní údaje, které jsou pro účely plnění smlouvy nutné. Pokud tedy vodárenská společnost zpracovává osobní údaje, které jsou nutné k plnění odběratelské smlouvy (tedy osobní údaje zpracovává na základě právního titulu plnění smlouvy), je současné vyslovení souhlasu s tímto zpracováním ze strany odběratele nadbytečné a nemělo by v ní být obsaženo.

Ustanovení o souhlasu odběratele se zpracováním osobních údajů by tedy nemělo být, podle GDPR, obsaženo v odběratelské smlouvě. Pokud tomu tak je, s ohledem na množství odběratelských smluv zřejmě nebude k 25. květnu 2018 proveditelné vyčlenění souhlasů z textu odběratelských smluv. Proto by se tak mělo stát při nejbližší vhodné příležitosti, např. při uvádění odběratelských smluv do souladu s „novými" požadavky uvedenými v čl. II bodu 5 novely zákona o vodovodech a kanalizacích č. 275/2013 Sb.[2]

Odběratelská smlouva (stejně jako smlouva dodavatelská či pracovní) by však měla vždy obsahovat ustanovení, prostřednictvím něhož vodárenská společnost jako správce splní vůči subjektu údajů svou informační povinnost dle čl. 13 a 14 GDPR. Subjekt údajů by měl být informován primárně o těchto skutečnostech (ledaže subjekt údajů již těmito informacemi již disponuje):

- kontaktní údaje správce,
- kontaktní údaje na pověřence pro ochranu osobních údajů (pokud byl vodárenskou společností jmenován),
- účel zpracování a právní titul zpracování (pokud je právním titulem oprávněný zájem, mělo by být uvedeno jeho přesné vymezení a v čem tento oprávněný zájem spočívá),
- případní příjemci nebo kategorie příjemců osobních údajů,
- případný úmysl správce předat/předávat osobní údaje do třetí země nebo mezinárodní organizaci.

Pokud by vodárenská společnost jako správce zamýšlela zpracovávat osobní údaje uvedené v odběratelské smlouvě např. za účelem zasílání marketingových sdělení, měla by k tomuto zpracování obdržet separátní souhlas subjektu údajů. Tento souhlas by však neměl být součástí odběratelské smlouvy, ale mělo by se jednat o samostatný dokument. Text souhlasu musí být koncipován tak, aby bylo možné aktivně udělit souhlas pro jednotlivé účely zvlášť, resp. aby bylo možné pro kterýkoliv účel souhlas neudělit.

[2] Zákon č. 275/2013 Sb., kterým se mění zákon č. 274/2001 Sb., o vodovodech a kanalizacích pro veřejnou potřebu a o změně některých zákonů (zákon o vodovodech a kanalizacích), ve znění pozdějších předpisů, a zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon), ve znění pozdějších předpisů.

Subjekt údajů může svůj souhlas kdykoliv odvolat, a to i před uplynutím doby, na kterou byl původně udělen, samozřejmě s výjimkou situací, kdy jsou osobní údaje zpracovány pro účely plnění smlouvy. Odvolání souhlasu přitom musí být stejně jednoduché, jako jeho udělení. Pokud je souhlas udělen nad rámec plnění příslušné smlouvy, lze odvolat toliko souhlas se zpracováním těch osobních údajů, které pro plnění příslušné smlouvy nejsou potřeba.

10. Technická a organizační opatření

GDPR ukládá správci a zpracovateli přijmout vhodná technická a organizační opatření za účelem zabezpečení náležité ochrany osobních údajů. Tato opatření se týkají jak zabezpečení IT systémů, kde jsou osobní údaje uloženy, tak opatření spíše organizační povahy, včetně povinnosti vypracovat posouzení vlivu na ochranu osobních údajů (DPIA).

a. Záměrná a standardní ochrana osobních údajů

Záměrná ochrana (Privacy by Design) je princip ochrany soukromí začleněný přímo do organizační struktury správce a technické architektury systémů, jenž počítá s ochranou osobních údajů již od počátku návrhu praktického řešení jejich zpracování. Při návrhu nového systému, procesu či služby, v rámci nichž dochází ke zpracování osobních údajů, vzniká povinnost aplikovat pravidla ochrany osobních údajů. Tato povinnost platí už od rané fáze procesu navrhování projektu nebo změnového záměru a je nutné ji dodržovat během celého životního cyklu osobních údajů. Společnost tedy musí ve své dokumentaci k jednotlivým projektům a změnovým záměrům prokázat, že tuto povinnost zohlednila.

Standardní ochrana (Privacy by Default) má zajistit, aby v základním nastavení služby byly zpracovávány jen osobní údaje, které jsou zcela nezbytné pro její poskytování. Jde primárně o povinnost nastavit maximální ochranu osobních údajů v zájmu dotčených subjektů údajů. To znamená, že je povinností dotčené společnosti implicitně nastavit a přizpůsobit systémy tak, aby zpracovávaly pouze osobní údaje nezbytné pro naplnění specifikovaného účelu a jejich použití tak bylo minimalizováno. Zároveň je povinností správce specifikovat přístupová práva k údajům a neumožnit tak přístup k osobním údajům libovolnému počtu svých zaměstnanců, resp. třetích osob.

Pokud navrhovaný projekt či změnový záměr dá subjektu údajů na výběr, do jaké míry bude své osobní údaje sdílet s ostatními, je nejvhodnější z hlediska ochrany soukromí takové nastavení, které zahrnuje možnost nesdílet žádné osobní údaje. Takové nastavení se má aplikovat jako výchozí nebo standardní.

Příslušná opatření (technická či organizační) by měla být odpovídající vzhledem ke stavu techniky, nákladům na provedení, povaze, rozsahu a účelům zpracování, jakož i k různě pravděpodobným a různě závažným rizikům pro subjekt údajů, jež s sebou dané zpracování nese.

b. Zabezpečení osobních údajů během uchovávání a sdílení

Každý systém/technologie musí splňovat základní autorizační a autentizační mechanismy tak, aby nebyl umožněn přístup neautorizovaných osob ke zpracovávaným osobním údajům. V případě, že systém/technologie nemá tyto mechanismy, je nutné toto riziko ohlásit Pověřenci pro ochranu osobních údajů, pokud by ustanoven (více viz kapitola 11 této GDPR Příručky). Pokud pověřenec pro ochranu osobních údajů nebyl vodárenskou společností ustanoven, měla by být informace o porušení osobních údajů poskytnuta jiné společností určené osobě, a pokud tato osoba určena nebyla, jejímu statutárnímu orgánu. Všechny přístupy a manipulace s osobními údaji musí být logovány. Každý uživatel systému má svá přístupová práva, přičemž nesmí docházet ke sdílení uživatelských jmen nebo hesel.

Postup při nahlášení porušení ochrany osobních údajů nebo podezření z takového porušení by měl být podrobně popsán v interní směrnici vodárenské společnosti. Tato interní směrnice může například

odkázat na formulář dostupný na webových stránkách vodárenské společnosti, který by její zaměstnanec k takovému nahlášení porušení využil. Interní směrnice by dále měla určit, v jakém časovém horizontu má zaměstnanec vodárenské společnosti povinnost v ní popsané kroky učinit. Tato směrnice by měla být závazná pro všechny zaměstnance příslušné vodárenské společnosti.

Osobní údaje lze zpracovávat pouze za jednoznačným účelem zpracování. V případě, že k zpracovávaným osobním údajům neexistuje žádný účel a/nebo nejsou zpracovávané na základě platného právního titulu (více viz kapitola 9 této GDPR Příručky), je nezbytné tyto osobní údaje vymazat. Zneplatnění by mělo být realizováno vhodnou metodou, která je technicky realizovatelná a ekonomicky přijatelná. S ohledem na skutečnost, že technická proveditelnost kompletního výmazu není vždy jednoduchá či možná, měl by o takových případech být vyrozuměn pověřenec pro ochranu osobních údajů, pokud byl vodárenskou společností jmenován, který následně vyhodnotí rizika a zařídí nutná opatření (analýza rizik, výjimka ze zneplatnění, apod.), a to vždy v návaznosti na pokyny uvedené ve spisovém a skartačním řádu, který by měla každá vodárenská společnost přijmout, aby bylo zřejmé, podle jakých pravidel se má v případně nutnosti provedení výmazu postupovat. Pokud pověřenec pro ochranu osobních údajů nebyl vodárenskou společností ustanoven, měla by být informace o porušení osobních údajů poskytnuta jiné společností určené osobě, a pokud tato osoba určena nebyla, jejímu statutárnímu orgánu.

Každý systém by měl mít funkcionalitu logování, tj. vést záznamy o zpracování osobních údajů a pořizovat logy. Tyto logy by následovně měly být zpracovány centralizovaným systémem pro správu logů. Každý systém/technologie obsahující osobní údaje by měla pořizovat logové záznamy pro veškeré změny osobních údajů pro konkrétní subjekt:

a. identifikace subjektu osobních údajů, kterého se změna týká,
b. autor změny osobních údajů,
c. čas změny osobních údajů,
d. důvod změny osobních údajů.

Všechny komunikační kanály, jejichž prostřednictvím sdílí vodárenská společnost osobní údaje s jinými aplikacemi, stranami nebo systémy, by měly mít identifikované a ošetřené. I v tomto případě je třeba vzít v úvahu základní zásady ochrany osobních údajů a sdílet pouze ty údaje, které jsou potřebné k naplnění daného účelu, a to v pseudonymizované podobě (pojem je vysvětlen v Příloze č. 1 této GDPR příručky), pokud je to možné. Každá třetí strana, s níž jsou osobní údaje sdíleny, by měla mít vlastní uživatelskou roli a přístupová práva.

c. Posouzení vlivu na ochranu osobních údajů (DPIA)

Ne každé zpracování osobních údajů představuje riziko pro subjekty údajů. Vypracování posouzení vlivu na ochranu osobních údajů (dále jen „**DPIA**“) pomůže rizikové zpracování a slabá místa včas odhalit. Hlavním cílem DPIA je tedy posoudit, jaký vliv bude mít zpracování osobních údajů na subjekty údajů, včetně možných rizik, která z něj vyplývají. Jedná se o analýzu, která zohledňuje aspekty plánovaného, anebo již probíhajícího zpracování osobních údajů.

DPIA není nutné připravovat pro všechna zpracování osobních údajů. Povinnost vypracovat DPIA se vztahuje na zpracování, která mohou představovat vysoké riziko pro práva a svobody subjektů údajů, zejména pokud se při zamýšleném zpracování mají využívat nové technologie. Rizikovost zamýšleného zpracování musí být vždy hodnocena s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování.

GDPR ukládá dozorovým úřadům, aby sestavily a zveřejnily seznam druhů operací zpracování, které budou požadavku vypracování DPIA podléhat. Dozorové úřady mohou rovněž určit seznam druhů operací zpracování, které této povinnosti naopak nepodléhají. Tyto seznamy nebyly ÚOOÚ ke dni vydání této příručky vydány (viz https://www.uoou.cz/dokumenty-k-gdpr/ds-4720/p1=4720).

Ve vztahu k vodárenským společnostem by se však mohlo jednat zejména o následující situace, kdy bude DPIA nutné vypracovat:

- Provádění systematického monitorování veřejně přístupných prostor kamerovým systémem,

- Zpracování zvláštních kategorií osobních údajů (více viz kapitola 4 této GDPR Příručky a Příloha č. 1),
- Zpracování osobních údajů nabývá velkého rozsahu, tj. týká se velkého počtu subjektů údajů nebo velkého rozsahu osobních údajů o konkrétní osobě, kdy toto zpracování je založeno na automatizovaném zpracování, včetně profilování,
- Zpracování osobních údajů se týká zranitelných osob, jako jsou děti, nemocní nebo postižení,
- Při zpracování dochází k inovativnímu využití nových technologií nebo organizačních řešení.

Pokud jsou alespoň dvě výše uvedená kritéria splněna, mělo by být zpracování vyhodnoceno jako vysoce rizikové s povinností provést DPIA. Minimální náležitosti DPIA jsou vymezeny v čl. 35 odst. 7 GDPR a zahrnují systematický popis zamýšlených operací zpracování a jeho účely, posouzení jejich nezbytnosti a přiměřenosti, posouzení rizik pro práva svobody subjektů údajů a plánovaná opatření k řešení zjištěných rizik.

11. Klíčové kontakty: pověřenec pro ochranu osobních údajů – DPO

Pověřenec poradí v problematice ochrany osobních údajů. Je však individuální povinností každého zaměstnance se se svými povinnostmi v oblasti ochrany osobních údajů náležitě seznámit a dodržovat je.

Pověřenec pro ochranu osobních údajů (dále jen „**DPO**“) je osoba, která je zejména odpovědná za poskytování informací a poradenství pro zpracování osobních údajů, včetně provádění auditu nastavení ochrany a provádění jejího monitoringu.

DPO musí jmenovat ti správci či zpracovatelé, jejichž hlavní činnost spočívá v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů či jejichž hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů. Hlavní činnosti jsou chápány jako klíčové operace nezbytné k dosažení cílů správce nebo zpracovatele. S ohledem na skutečnost, že zpracování osobních údajů je vůči hlavní činnosti vodárenských společnostní toliko podpůrné, nedovozujeme v jejich případě obecnou povinnost jmenovat DPO, ledaže by tyto vodárenské společnosti prováděly rozsáhlé zpracování tzv. zvláštních kategorií osobních údajů (k jejich vymezení viz kapitola 4 této GDPR Příručky).

Dle GDPR musí DPO jmenovat orgány veřejné moci a veřejné subjekty. Dle pokynů týkajících se pověřenců pro ochranu osobních údajů, které vydala Pracovní skupina W29 coby nezávislý poradní orgán pro otázky ochrany osobních údajů (viz https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28336), může být úkol ve veřejném zájmu a výkon veřejné moci plněn nejen veřejným orgánem nebo subjektem, ale rovněž fyzickými a právnickými osobami řídícími se veřejným nebo soukromým právem v oblastech specifikovaných národními předpisy. Příkladný výčet těchto oblastí přitom uvádí i služby spočívající v zásobování vodou a energiemi. Subjekty, které takové služby poskytují, jsou při zpracování osobních údajů v obdobné pozici jako veřejné orgány, zejména s ohledem na podobnost účelů zpracování a skutečnost, že subjekty údajů mají často malý či žádný vliv na to, zda a jak jsou jejich osobní údaje zpracovány. Výše uvedené vodítko sice uvádí, že jmenování DPO není v takových případech povinné, nicméně jej Pracovní skupina W29 doporučuje jako osvědčený postup.

Pokud se tedy vodárenská společnost rozhodne tímto doporučením řídit a DPO skutečně jmenuje, musí plnit veškeré povinnosti, které jsou se zavedením této funkce spojeny, zejména zapojení DPO do veškerých záležitostí souvisejících s ochranou osobních údajů, jeho podpora při plnění úkolů, jimiž byl pověřen (zejména udržování odborných znalostí) či zveřejnění jeho kontaktních údajů.

Předpokladem jmenování určité osoby jako DPO jsou její profesní kvality, zejména pak ve vztahu k odborným znalostem a praxi v oblasti ochrany osobních údajů. DPO může být zaměstnanec správce či zpracovatele, který jej jmenoval, či svou funkci může vykonávat na základě smlouvy o poskytování služeb.

DPO nesmí být při výkonu jemu svěřených úkolů vázán žádnými pokyny, tedy nesmí být v souvislosti s plněním svých úkolů správcem či zpracovatelem propuštěn či sankcionován. DPO zásadně nenese osobní odpovědnost za nedodržování GDPR, neboť tu nesou správci či zpracovatelé. DPO je v rámci struktury společnosti vždy podřízen vrcholovým řídícím právníkům správce nebo zpracovatele, tj. musí mít vždy přístup k vedení organizace. DPO je při výkonu veškerých svých úkolů vázán tajemstvím a důvěrností.

DPO v rámci své činnosti vyřizuje zejména následující agendu:

- Sleduje soulad zpracování osobních údajů se všemi právními předpisy, stejně jako s koncepcemi správce či zpracovatele v oblasti ochrany osobních údajů.
- Podílí se na zvyšování povědomí a odborné přípravě pracovníků zapojených do zpracování osobních údajů a souvisejících auditů.
- Vykonává informační a poradenskou činnost ve vztahu ke správci či zpracovateli a zaměstnancům.
- Působí jako kontaktní místo pro ÚOOÚ, s nímž spolupracuje a konzultuje určité záležitosti týkající se zpracování osobních údajů.
- Plní roli supervize, s možnosti nahlédnutí do zpracování osobních údajů v rámci každého systému/technologie. V praxi to znamená, DPO musí být umožněn přístup do systému nebo přístup k logům každého dotčeného systému/technologie.

DPO zásadně nenese osobní odpovědnost za nedodržování GDPR, neboť tu nesou správci či zpracovatelé.

V případě jmenování by se měl DPO vodárenské společnosti věnovat zejména následujícím úkolům:

- stanovení a řízení metodiky ochrany osobních údajů a její rozvoj;
- provádění monitoringu a koordinace aplikace příslušných zákonů či jiných právních předpisů a dalších strategických dokumentů EU;
- informování o právních předpisech a soudních rozhodnutích ve věci ochrany osobních údajů;
- vyhodnocování rizika souvisejícího s ochranou a zpracováním osobních údajů, vyhodnocování upozornění na protiprávní jednání a/nebo porušení interních předpisů v souvislosti s ochranou a zpracováním osobních údajů;
- koordinace ostatních právních záležitosti souvisejících s ochranou osobních údajů;
- poskytování poradenství v oblasti ochrany a zpracování osobních údajů;
- komunikace s příslušnými dozorovými úřady;
- organizace nasazování, nastavení a údržby systémů souvisejících s ochranou a zpracováním osobních údajů;
- navrhování preventivních a nápravných opatření;
- vypracovávání informačních materiálů;
- provádění školení a vzdělávání zaměstnanců v oblasti ochrany a zpracování osobních údajů;
- provádění zpracování procesního a organizačního dokumentu ochrany osobních údajů.

12. Kamerové systémy

Pořizování kamerových záznamů se zpravidla považuje za zpracování osobních údajů. Proto jsou pro případy pořizování kamerových záznamů stanoveny zvláštní povinnosti, které musí správce zpracovávaných osobních údajů plnit.

Monitorování veřejně přístupných prostor kamerovými systémy zahrnuje v některých případech také zpracování osobních údajů. O zpracování osobních údajů se podle stanoviska Úřadu pro ochranu osobních údajů (viz https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22294) jedná, pokud:

- je vedle kamerového sledování prováděn také záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace,
- je účelem pořizovaných záznamů, či vybraných informací, jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

Údaje uchovávané v záznamovém zařízení, ať již obrazové nebo zvukové, jsou osobními údaji tehdy, pokud lze na jejich základě identifikovat konkrétní fyzickou osobu. Zejména tedy jde o případy, kdy je na záznamu zachycen obličej či jiné rozpoznávací znaky.

Kamerový systém lze využívat i bez souhlasu subjektů údajů, které jsou na něm zachyceny, a to za předpokladu, že je takové zpracování prováděno k ochraně oprávněného zájmu subjektu údajů. Takové kamerové sledování však nesmí nadměrně zasahovat do soukromí sledovaných osob. Použití kamerového systému je zásadně možné v případech, kdy sledovaného účelu nelze dosáhnout jiným způsobem (např. monitorovaný majetek nelze uchránit uzamčením v místnosti).

Zavedení kamerového systému by mělo předcházet vymezení účelu zpracování, kdy pořízené záznamy mohou sloužit pouze tomuto účelu, stejně jako doby pro uchování záznamu, která by měla vždy odpovídat potřebám pro dosažení stanoveného účelu. Subjekt údajů musí být o užití kamerového systému vhodným způsobem informován (typicky nápisem před vstupem do kamerou monitorovaného prostoru). Subjektu údajů musí být vždy umožněn výkon jeho práv. Pokud jsou záznamy pořizovány na základě právního titulu oprávněného zájmu (tedy nikoliv na základě souhlasu subjektu údajů), musí být subjektu údajů umožněno podat proti takovému zpracování námitku.

GDPR identifikuje systematické monitorování veřejných prostor ve velkém rozsahu, obzvláště v případě, kde se k monitorování používají optické elektronické přístroje, jako velmi rizikovou aktivitu.

Oznamovací povinnost ÚOOÚ, která se doposud na případy pořizování kamerových záznamů vztahovala, bude s účinností GDPR zrušena.

Na správce zpracovávající osobní údaje prostřednictvím kamerových systému se vztahují také následující povinnosti:

- vedení záznamů o činnostech zpracování (viz kapitola 10 této GDPR Příručky),
- jmenování DPO (pokud pořizování kamerového záznamu správcem či zpracovatelem lze zahrnout mezi jeho hlavní činnosti, a toto zpracování vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů),
- vypracovat posouzení vlivu na ochranu osobních údajů (viz kapitola 6 této GDPR Příručky).

Vedení kamerových záznamů např. v prostorách recepce, nebude pro vodárenskou společnost znamenat povinnost jmenovat DPO. Pokud by však tyto prostory střežila bezpečnostní agentura, jejíž hlavní činnost ve zpracování osobních údajů spočívá, bude se na ni povinnost jmenování DPO vztahovat.

Příloha č. 1 – Vysvětlení nejdůležitějších pojmů

Pojem	Definice	Příklad
Automatizované rozhodování	Automatizované rozhodování je rozhodování, které probíhá bez manuálního zásahu lidské osoby, nýbrž na základě daného algoritmu. Pokud je rozhodnutí přijato bez zásahu člověka a je založeno na automatizovaném zpracování a pro subjekt údajů může mít právní účinky (např. uzavření či neuzavření smlouvy), má subjekt údajů právo podat nebýt předmětem takového rozhodnutí.	Příkladem automatizovaného rozhodování může být automatizované rozhodnutí banky o poskytnutí či neposkytnutí úvěru s potenciálním zákazníkem na základě automatizovaně zpracovaných osobních údajů o této osobě. V oblasti vodárenství by příkladem automatizovaného rozhodování mohlo být provedení automatizovaného odečtu spotřeby vody z vodoměrů (zpracování), na jehož základě by bez jakéhokoliv lidského zásahu byla odběrateli vystavena faktura za spotřebované množství vody (automatizované rozhodnutí).
Bez zbytečného odkladu	Pojem bez zbytečného odkladu je neurčitou lhůtou, v rámci které je nutné povinnost splnit. Jedná se o krátký časový úsek, ve kterém má povinná osoba, například správce, konat. Pokud povinná osoba v tomto krátkém časovém úseku nejedná, musí mít důvod, kvůli kterému nebylo možné konat bez odkladu. Může se jednat o složitost problému nebo žádosti, případně o velký rozsah osobních údajů, kterých se povinnost týká.	Správce je dle ustanovení GDPR povinen bez zbytečného odkladu opravit nepřesné osobní údaje. Pokud se bude jednat o opravu osobních údajů ve velkém rozsahu, je možné, aby byl poskytnutý časový úsek delší.
Doba uchování	Správce není oprávněn osobní údaje uchovávat neomezeně dlouho, je proto nutné stanovit dobu, po kterou budou zpracované osobní údaje uchovávány. Doba uchování musí být přiměřená účelu, za jakým jsou osobní údaje zpracovávány. Správce je povinen sdělit subjektu údajů dobu, po kterou budou osobní údaje subjektu uchovávány. Pokud není možné takovou dobu uchování určit předem, je správce povinen informovat subjekt údajů alespoň o kritériích, pomocí kterých bude tato doba určena.	Doba uchování osobních údajů by měla být vždy vymezena ve skartační směrnici vodárenské společnosti. Např. v případě odběratelských smluv by měla minimální doba uchování odpovídat době trvání smluvního vztahu, případně přiměřenou dobu (odpovídající např. promlčecí době) po jeho zániku.
Dozorový úřad	Dozorovým úřadem v České republice pro oblast ochrany osobních údajů je Úřad pro ochranu osobních údajů.	
Hlavní činnost	Hlavní činnost je činnost, která je pro správce nebo zpracovatele naprosto stěžejní hospodářskou činností a souvisí s jeho primárním působením.	Hlavní činností vodárenských společností je zásobování pitnou vodou a odvádění odpadních a srážkových vod. Hlavní činností SOVAK tak je sdružovat právnické a fyzické osoby, jejichž předmětem činnosti je zejména zásobování vodou či odvádění a čištění či jiná likvidace odpadních vod, rozvoj nebo výstavba vodovodů a kanalizací

		pro veřejnou potřebu a spolupráce s oborem vodovodů a kanalizací pro veřejnou potřebu.
Informační povinnost	Informační povinnost je povinností správce vůči subjektu údajů. Správce je povinen subjekt údajů informovat před započetím zpracování nebo při prvním kontaktu se subjektem údajů. Subjekt údajů by měl být informován zejména o rozsahu zpracovávaných osobních údajů, účelu zpracování, době uchování zpracovaných osobních údajů, případných dalších osobách, kterým budou osobní údaje předány a o právech, které náleží subjektu údajů.	Pokud vodárenská společnost monitoruje své prostory, musí na viditelné místo umístit informaci o monitorování prostor kamerovým systémem.
Kategorie osobních údajů	GDPR vyjmenovává dvě kategorie, a to (i) osobní údaje a (ii) zvláštní kategorie osobních údajů. Dále lze osobní údaje členit v rámci subjektivního rozdělení správcem, například na kategorie identifikačních údajů nebo kategorie adresních údajů. Takové subjektivní rozdělení slouží jako další podskupina pod kategoriemi stanovenými GDPR.	U subjektu údajů můžeme např. vědět, že se jmenuje Karel Borovský, že má astma, a že je členem odborů. V takovém případě bude jméno a příjmení osobním údajem a údaj o zdravotním stavu a o členství v odborech bude spadat do zvláštní kategorie osobních údajů. Správce údajů si pak může tyto údaje dále rozdělit do jím libovolně stanovených kategorií.
Kodex/kodex chování	Kodexy chování jsou nepovinně vypracovávaná pravidla, která mají upřesňovat výklad či uplatňování GDPR a jsou schvalována ÚOOÚ (viz čl. 40 GDPR). Kodexy chování vydávají sdružení správců či zpracovatelů nebo jiné subjekty, které zastupují odlišné kategorie správců či zpracovatelů.	
Kontrolní opatření	Kontrolní opatření jsou opatření zaměřená na monitorování dodržování zavedených postupů a opatření sloužících k ochraně osobních údajů při jejich zpracování.	Každá vodárenská společnost by měla mít stanovena přístupová práva k systému, který obsahuje osobní údaje. Dále by měla být zavedena pravidelná kontrola těchto přístupových práv.
Minimalizace	Zásada minimalizace údajů patří mezi jednu ze zásad zpracování osobních údajů stanovených GDPR. Dle zásady minimalizace údajů musí být osobní údaje zpracovávané pro určitý účel přiměřené, relevantní a omezené na nezbytný rozsah. Správce nesmí zpracovávat osobní údaje ve větším rozsahu, než je pro daný důvod zpracování nezbytné („*need-to-know*").	Kamerový systém společnosti, který zabírá prostor recepce, zaznamenává i zvukový záznam. Vzhledem k účelu pořizování záznamu, kterým by byla např. ochrana majetku společnosti, by byl dostačující pouze obrazový záznam a zvukový záznam je již v rozporu se zásadou minimalizace.
Ohlašovací povinnost vůči dozorovému úřadu	GDPR klade na správce povinnost ohlašování porušení zabezpečení osobních údajů. Takové ohlášení musí proběhnout do 72 hodin od okamžiku, kdy se o porušení správce dozvěděl a podává se k Úřadu pro ochranu osobních údajů.	Do systému, který obsahuje osobní údaje, se dostane osoba, která k těmto údajům nemá mít přístup a část databáze obsahující osobní údaje dodavatelů či odběratelů si zkopíruje. Správce pak musí ohlásit porušení zabezpečení osobních údajů.

Oprávněný zájem	Oprávněný zájem je jeden z možných právních titulů zákonného zpracování osobních údajů. Na základě oprávněného zájmu je možné zpracovávat údaje pouze v situaci, kdy nad zájmy správce nepřevažují základní práva a svobody subjektu údajů. Přítomnost oprávněného zájmu je vždy třeba posoudit.	Příkladem zpracování na základě oprávněného zájmu může být zpracování za účelem prevence podvodů nebo monitorování areálu správce osobních údajů kamerovým systémem.
Osobní údaje	Osobními údaji mohou být jakékoliv informace, které mohou identifikovat konkrétní fyzickou osobu, ať již přímo nebo nepřímo. Možnými identifikátory fyzické osoby jsou například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo další prvky genetické, ekonomické, kulturní nebo společenské identity fyzické osoby. Uvedené identifikátory nemusí být osobními údaji vždy. Údaje je třeba vždy posuzovat v kontextu, například celé databáze, zda lze prostřednictvím jednotlivých identifikátorů určit konkrétní osobu.	Jestliže vodárenská společnost disponuje např. databází odběratelů, v níž jsou uvedena čísla zákaznických účtů, budou tato čísla vždy osobním údajem, pokud s nimi lze spojit konkrétní subjekt údajů. V případě, kdy budou v databázi obsažena pouze křestní jména, která se budou opakovat, nebudou tyto údaje považovány za osobní údaje, neboť na jejich základě nelze identifikovat konkrétní osobu. Jména budou osobním údajem až po jejich spojení s konkrétním identifikátorem, díky němuž se provede identifikace subjektu údajů.
Osobní údaje týkající se rozsudků v trestních věcech	Osobní údaje týkající se rozsudků v trestních věcech a trestných činů se dle GDPR řadí do speciální kategorie. Taková kategorie také podléhá odlišným podmínkám zpracování. Jedná se zejména o zpracování osobních údajů, které zahrnuje osobní údaje týkající se jakýchkoliv údajů spojených se soudními rozhodnutími v trestních věcech (zejména rozhodnutími týkajícími se rozhodnutí o vině a trestu subjektů zpracování osobních údajů, údaje reflektované ve výpisech z rejstříku trestů subjektů zpracování osobních údajů).	Může se jednat o situaci, kdy by vodárenská společnost požadovala od všech svých zaměstnanců plošně výpis z rejstříku trestů. Tyto údaje však může zaměstnavatel požadovat pouze v případě, kdy je to nezbytné pro výkon dané práce. Je zřejmé, že trestní bezúhonnost všech zaměstnanců příslušné vodárenské společnosti není nezbytná. Příslušná vodárenská společnost by tak měla rozhodovat o požadování výpisu z rejstříku trestu individuálně a pouze v případech, kde je to pro výkon dané práce nezbytné.
Osvědčení	Osvědčení o ochraně údajů je vydáváno pouze akreditovaným subjektem v členských státech Evropské unie a jeho cílem je prokázat, že správce či zpracovatel zpracovávají osobní údaje v souladu s GDPR.	
Posouzení vlivu na ochranu osobních údajů	GDPR stanoví činnosti zpracování, před jejichž započetím je správce povinen provést posouzení vlivu na ochranu osobních údajů. Obsahem posouzení je popis činností zpracování, jaké se správce chystá provádět, přiměřenost a nezbytnost těchto činností s ohledem na důvod, pro který jsou osobní údaje zpracovávány, a posouzení, jaká rizika přináší plánované činnosti zpracování pro subjekty údajů. Dále by měla být obsahem posouzení konkrétní opatření a záruky či mechanismy k minimalizaci vyhodnocených rizik. Posouzení vlivu	Pokud by se vodárenská společnost chystala zavést monitorování prostor recepce, měla by před započetím zpracování provést posouzení vlivu na ochranu osobních údajů, neboť systematické monitorování veřejně přístupných prostorů spadá do operací zpracování, před jejichž započetím je třeba provést posouzení vlivu na ochranu osobních údajů.

	na ochranu osobních údajů je nutné provést před započetím vybraných zpracování. Jedná se zejména o rozsáhlé systematické monitorování veřejně přístupných prostorů (například prostřednictvím kamerového systému) nebo systematické a rozsáhlé zpracování založené na profilování nebo automatizovaném rozhodování.	
Pověřenec pro ochranu osobních údajů	Pověřenec pro ochranu osobních údajů je osoba, kterou jsou povinni jmenovat vymezení správci nebo zpracovatelé, zejména ti, jejichž hlavní činnosti se skládají z rozsáhlého pravidelného a systematického monitorování subjektů nebo z rozsáhlého zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů, a orgány veřejné moci. Pověřenec musí disponovat odbornými znalostmi a musí plnit úkoly stanovené GDPR. Mezi takové úkoly patří například poskytování informací a poradenství, monitorování souladu s GDPR nebo spolupráce s dozorovým úřadem.	Pokud by vodárenská společnost jmenovala pověřencem pro ochranu osobních údajů vedoucího IT oddělení, který přislíbil, že se až následně seznámí s příslušnými předpisy na ochranu osobních údajů, nevyhovoval by takový zaměstnanec podmínkám dle GDPR, neboť by nedisponoval potřebnými znalostmi.
Práva subjektů údajů	Práva, která může subjekt údajů uplatnit vůči správci.	V rámci těchto práv může subjekt údajů požadovat například přístup k zpracovávaným osobním údajům (právo na přístup), opravení nepřesných údajů (právo na opravu) či vymazání osobních údajů (právo na výmaz). Každá společnost by měla zajistit nastavení verifikace žadatele (tj. zda právo uplatňuje skutečně subjekt údajů) a určit pravidla pro vyhodnocení oprávněnosti dané žádosti.
Pravidelné a systematické monitorování	Pojem pravidelného a systematického monitorování není v GDPR výslovně definován. Pravidelnost monitorování však můžeme spatřovat v průběžném, opakujícím se nebo opakovaném zpracování. Systematické zpracování je zpracování, které je nějakým způsobem přednastavené, organizované, probíhá dle určitého systému.	Příkladem může být opět situace, kdy by vodárenská společnost pořizovala kamerový záznam z oblasti recepce, tedy prováděla zpracování, které splňuje znaky pravidelnosti i systematičnosti.
Právní titul	Právní titul je právní důvod, který je podkladem pro předmětné zpracování osobních údajů, aby bylo zpracování zákonné. Výčet právních titulů je uveden v čl. 6 GDPR. Výčet právních titulů dle GDPR je uzavřený, proto, aby zpracování bylo zákonné, je nutné zpracování provádět pouze na základě důvodů uvedených v GDPR.	Patří sem například zpracování nezbytné pro plnění smlouvy (stranou smlouvy musí být subjekt údajů), které v oblasti vodárenství představuje primární právní titul pro zpracování osobních údajů), zpracování na základě souhlasu, či zpracování pro splnění právní povinnosti správce nebo zpracování prováděné ve veřejném zájmu.

Profilování	Profilování je způsob zpracování osobních údajů, který probíhá automatizovaně. Tento způsob zpracování hodnotí hlediska vztahující se k subjektu údajů za účelem analýzy ekonomické situace, zdravotního stavu, osobních preferencí, místa pohybu či pobytu nebo chování.	Příkladem může být situace, kdy subjekt žádá banku o poskytnutí úvěru a banka od něj vyžaduje informace o jeho ekonomických příjmech a výdajích, aby získala přehled o jeho ekonomické situaci. S ohledem na skutečnost, že profilování není způsob zpracování, který by byl typický pro vodárenské společnosti, je tento pojem uveden pouze pro úplnost pokrytí problematiky ochrany osobních údajů.
Příjemce	Příjemcem je jakákoliv fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterému jsou osobní údaje poskytnuty.	Pokud zaměstnanec vodárenské společnosti své osobní údaje jako zaměstnavateli, stává se tato příjemcem osobních údajů. Příjemcem dále může být i společnost, vodárenskou společnost připravuje marketingové kampaně a rozesílá obchodní sdělení, a tím pádem využívá databáze jejich odběratelů.
Přijetí žádosti	Přijetí žádosti je pojem, který souvisí s výkonem práv subjektů údajů. Je to proces, v rámci kterého by nejprve měl správce identifikovat subjekt údajů, který žádost odesílal a následně posoudit, zda má subjekt údajů nárok na výkon práva, který žádá.	Prostřednictvím žádosti mohou subjekty údajů žádat například o přístup k osobním údajům, opravu osobních údajů nebo jejich výmaz.
Rozhodnutí Komise o odpovídající ochraně	Rozhodnutí Komise o odpovídající ochraně je dalším způsobem, jakým je možné předávat osobní údaje do třetích zemí mimo území Evropské unie. Aby mohlo předání osobních údajů do třetích zemí proběhnout, musí Komise *ad hoc* stanovit, že daná třetí země, určité území nebo odvětví zajišťuje dostatečnou ochranu.	V případě, kdy mají být osobní údaje poskytnuty např. do Demokratické republiky Kongo, musí předávající subjekt, např. správce zjistit, zda bylo Komisí rozhodnuto, že tato země poskytuje odpovídající ochranu osobním údajům. Pokud toto rozhodnutí bylo vydáno, mohou být osobní údaje do dané země poskytnuty, neboť je zaručena jejich ochrana.
Rozsáhlé zpracování	Rozsáhlé zpracování osobních údajů není GDPR výslovně definované, při jeho určení se bere v potaz několik faktorů, jako je například počet dotčených subjektů údajů, velikost území nebo doba trvání zpracování.	O rozsáhlé zpracování údajů se bude jednat např. v případě vodárenské společností, která disponuje databázemi odběratelů obsahující osobní údaje o tisících odběratelů.
Služby informační společnosti	Služby informační společnosti jsou služby poskytované za úplatu na dálku, tedy při poskytnutí služby není ani jedna ze stran přítomna, dále služby poskytované prostřednictvím elektronického zařízení a na žádost toho, kdo službu přijímá.	
Souhlas	Souhlas je projevem vůle subjektu údajů a současně jedním z právních titulů, na základě kterých je možné osobní údaje zpracovávat. GDPR na souhlas klade určité požadavky - souhlas musí být svobodný a konkrétní pro určitou činnost zpracování a současně musí obsahovat informace o zpracování, ke kterému je souhlas udělován (zejména kdo bude	Souhlas se zpracováním osobních údajů může být typicky udělován pro marketingové účely, tj. zejména pro zasílání informací o novinkách nebo marketingových kampaní.

	zpracování provádět, jaký rozsah osobních údajů bude zpracováván nebo informace o právech, které subjektu údajů náleží). O udělení souhlasu nemůže být pochyb, musí být vyjádřen aktivním prohlášením nebo potvrzením subjektu údajů se zpracováním. V tomto případě nelze aplikovat konkludentní souhlas, tj. souhlas mlčky či faktickým jednáním.	
Správce	Správce je subjekt, který určuje účely (proč) a prostředky (jak) zpracování osobních údajů. Správce tedy určuje důvod, pro který jsou osobní údaje zpracovávány, a způsob, jakým budou zpracovány. Správcem může být fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt.	Typickým správcem osobních údajů je např. zaměstnavatel, který určuje důvod a způsob, jakým jsou osobní údaje o zaměstnancích zpracovány.
Standardní doložky o ochraně osobních údajů	Standardní doložky o ochraně osobních údajů představují jeden ze způsobů, jak je možné osobní údaje předávat do třetích zemí mimo Evropskou unii. Doložky definovala Evropská komise ve svých rozhodnutích a je možné je uzavřít jak mezi správcem a zpracovatelem, tak při předání osobních údajů mezi dvěma správci. Při uzavření standardních doložek o ochraně osobních údajů je odpovědností správce zajistit bezpečnost údajů, které jsou předávány do třetích zemí.	
Strukturovaný, běžně používaný a strojově čitelný formát	GDPR nestanovuje konkrétní formát, ve kterém má správce osobní údaje poskytnout, stanovuje však minimální požadavky kladené na tento formát. Musí jít o formát strukturovaný, tedy uspořádaný. Dalším požadavkem je běžné používání formátu, mělo by jít o formát rozšířený, jehož používání nepřináší značné náklady a strojově čitelný formát, což znamená formát se strukturou, ze které mohou aplikace snadným způsobem získat data a použít je.	Příkladem může být soubor ve formátu MS excel.
Subjekt údajů	Subjektem údajů je ta konkrétní identifikovatelná fyzická osoba, jejíž osobní údaje jsou zpracovávány.	Subjektem údajů je např. každý zaměstnanec, potenciální zaměstnanec, odběratel nebo dodavatel (coby fyzické osoby), jehož osobní údaje vodárenská společnost zpracovává.
Test proporcionality (balance test)	Test proporcionality je test, v rámci kterého se porovná zpracování osobních údajů za účelem oprávněného zájmu se základními právy a svobodami subjektu údajů. Zpracování osobních údajů pro oprávněný zájem musí být přiměřené ve vztahu k základním právům a svobodám, nesmí tedy významným způsobem zasahovat nebo porušovat základní práva a svobody subjektu	

	údajů. Pokud zpracování pro oprávněný zájem takovým způsobem do základních práv a svobod údajů nezasahuje, je přiměřené a zákonné.	
Typ osobních údajů	Typy osobních údajů jsou jednotlivé osobní údaje, které lze dále subjektivně řadit do dalších kategorií nebo do hlavních dvou kategorií stanovených GDPR, a to kategorie osobní údaje a zvláštní kategorie osobních údajů. Jde například o jméno, bydliště nebo rodné číslo. Tyto vyjmenované typy osobních údajů lze dále seskupit v různých kategoriích.	U subjektu údajů můžeme např. vědět, že se jmenuje Karel Borovský, že má astma, a že je členem odborů. V takovém případě bude jméno a příjmení osobním údajem a údaj o zdravotním stavu a o členství v odborech bude spadat do zvláštní kategorie osobních údajů. Správce údajů si pak může tyto údaje dále rozdělit do jím určených kategorií.
Účel zpracování	Důvod, pro který jsou osobní údaje zpracovávány.	Takovým důvodem zpracování může být například zasílání marketingových sdělení, plnění závazků z pracovní smlouvy nebo jednání před uzavřením smlouvy s potenciálním dodavatelem či odběratelem.
Výmaz	Výmaz osobních údajů je kompletní odstranění osobních údajů ze všech databází, systémů a jakýchkoliv dalších úložišť správce či zpracovatele, kde jsou osobní údaje zpracovávány, včetně fyzických dokumentů. Výmaz musí správce zajistit také ze všech systémů zpracovatele, pokud mu byly osobní údaje daného subjektu údajů poskytnuty.	Pokud např. bývalý zaměstnanec požádá o výmaz osobních údajů, kterými disponuje vodárenská společnost coby bývalý zaměstnavatel, a tato žádost je zároveň oprávněná, má dotčená vodárenská společnost povinnost vymazat veškeré osobní údaje v elektronické i fyzické podobě. Výmaz pak musí být zajištěn také u zpracovatele, kterým může být např. společnost poskytující služby centra sdílených služeb.
Zabezpečení zpracování osobních údajů (podle čl. 32)	GDPR klade na správce i zpracovatele požadavek, aby zpracovávané osobní údaje byly zabezpečeny a chráněny. Jedná se o souhrn organizačních a technických opatření, která by měl správce nebo zpracovatel přijmout a dodržovat.	Může jít například o šifrování, omezení přístupu k osobním údajům nebo pravidelná testování již zavedených opatření.
Zákonnost zpracování	GDPR stanoví podmínky, které je třeba splnit, aby zpracování osobních údajů bylo zákonné, jedná se o tzv. právní tituly zpracování stanovené v čl. 6 GDPR. Pokud zpracování neprobíhá na základě těchto právních titulů, je nezákonné a dochází tak k porušení povinností stanovených GDPR.	Jde například o zpracování na základě souhlasu nebo zpracování nezbytné pro plnění smlouvy.
Závazná podniková pravidla	Závazná podniková pravidla si mezi sebou mohou stanovit společnosti působící v rámci skupiny podniků, které vykonávají společnou hospodářskou činnost. Tato pravidla schvaluje úřad ÚOOÚ a obsahují zejména seznam společností, které se k dodržování pravidel zavázaly, dále	

	podmínky předávání osobních údajů nebo třeba nastavenou ochranu osobních údajů, případně jejich zabezpečení.	
Zpracování osobních údajů	Za zpracování osobních údajů se považuje jakékoliv nakládání s osobními údaji.	Za zpracování osobních údajů se považuje například shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jiné zpřístupnění, seřazení, zkombinování, omezení, výmaz nebo zničení osobních údajů. Veškeré zmiňované činnosti mohu být prováděny manuálně nebo pomocí automatizovaných postupů bez manuálního zásahu.
Zpracování osobních údajů pro konkrétně stanovený účel	Zpracování osobních údajů musí probíhat pouze pro ten důvod, který správce stanovil jako účel zpracování. Takto zpracované údaje nelze dále používat i pro jiný účel, tedy pro jiné důvody, než které byly původně stanoveny, s výjimkou účelů slučitelných s účelem, pro který byly osobní údaje shromážděny (za splnění dalších podmínek).	
Zpracování ve veřejném zájmu	Zpracování ve veřejném zájmu je jeden z právních titulů, tedy důvodů, na základě kterých je možné zpracovávat osobní údaje. Zpracování ve veřejném zájmu provádí orgány veřejné moci nebo další subjekty, které plní úkoly ve veřejné moci. Právním základem pro oprávněné zpracování ve veřejném zájmu je plnění veřejného úkolu, ať již ze strany subjektu soukromého nebo veřejného práva. Osobní údaje získané pro tento účel není možné využít jinak než pro dané plnění veřejného úkolu.	
Zpracovatel	Zpracovatel je subjekt (třetí osoba odlišná od správce), který zpracovává osobní údaje pro správce, který již určil, proč se osobní údaje zpracovávají a jak se zpracovávají. Zpracovatelem může být právnická nebo fyzická osoba, orgán veřejné moci, agentura nebo další subjekt, který zpracovává osobní údaje. Zpracování osobních údajů zpracovatelem je prováděno na základě písemné smlouvy. Za zpracovatele se nepovažuje zaměstnanec správce nakládající s osobními údaji.	Zpracovatelem osobních údajů tak může být poskytovatel služby centra sdílených služeb.

Zvláštní kategorie osobních údajů	Do zvláštní kategorie osobních údajů spadají osobní údaje, které jsou vnímány jako citlivé pro subjekt údajů. I proto jim GDPR přiznává speciální podmínky ochrany.	Může se jednat například o údaje o rasovém či etnickém původu, vypovídající o politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech. Dále jde o genetické údaje, biometrické údaje, pokud jsou zpracovány za účelem jedinečné identifikace fyzické osoby, a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Příloha č. 2 – Nejčastěji kladené dotazy

1. Kdy vstupuje GDPR v účinnost?

GDPR vstoupí v účinnost dne 25. května 2018. Od tohoto dne bude nařízení závazné v celém svém rozsahu a zároveň přímo použitelné ve všech členských státech EU.

2. Co to znamená, že GDPR je nařízením a nikoliv směrnicí?

Nařízení EU není třeba transponovat do právního řádu České republiky ani ostatních členských států EU, neboť po 25. květnu 2018 bude přímo účinné ve všech členských státech EU a společnosti se jím budou muset řídit. Naopak směrnice musí být transponovány do právních řádů všech členských států dalším vnitrostátním zákonem, teprve poté se jimi musí ostatní řídit.

3. Na koho se právní úprava ochrany osobních údajů vztahuje?

Právní úprava se použije nejenom na subjekty se sídlem v EU, které zpracovávají osobní údaje fyzických osob, ale také na subjekty, které mají sídlo mimo EU, pokud nabízejí zboží nebo služby fyzickým osobám v EU, nebo sledují jejich chování.

4. Jaká je sankce za nedodržení GDPR?

Společnosti lze v určitých případech uložit správní pokutu až do výše 20 000 000 EUR nebo až do výše 4 % celosvětového ročního obratu za předchozí finanční rok (tj. obratu celé skupiny společností, do které patří).

5. Co představuje pojem osobní údaj?

Osobními údaji mohou být jakékoliv informace, které mohou identifikovat konkrétní fyzickou osobu, ať již přímo nebo nepřímo. Možnými identifikátory fyzické osoby jsou například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo další prvky genetické, ekonomické, kulturní nebo společenské identity fyzické osoby. Uvedené identifikátory nemusí být osobními údaji vždy. Údaje je třeba vždy posuzovat v kontextu, například celé databáze, zda lze prostřednictvím jednotlivých identifikátorů určit konkrétní osobu. Některé identifikátory musí být propojené se jménem a příjmením, případně adresou, aby bylo možné jejich prostřednictvím identifkovat fyzickou osobu. Osobním údajem tak bude např. jméno a příjmení odběratele vodárenské společnosti, ve spojení s adresou jeho bydliště, díky níž jej bude možné jednoznačně identifikovat.

6. Jaký je rozdíl mezi zpracovatelem a správcem osobních údajů?

Správce osobních údajů určuje za jakým účelem a prostřednictvím jakých prostředků jsou osobní údaje zpracovávány. Zpracovatel pouze zpracovává osobní údaje pro správce a je povinen řídit se při tomto zpracování jeho pokyny.

7. Jsem subjekt údajů? Jaká jsou má práva?

Subjektem údajů je každá fyzická osoba, k níž se vztahují osobní údaje, které jsou zpracovávány, tj. které zpracovává společnost.

Mezi hlavní práva subjektu údajů patří:

- právo být informován o zpracování jeho osobních údajů,
- právo na přístup k osobním údajům,
- právo na opravu osobních údajů,
- právo na výmaz osobních údajů,
- právo na omezení zpracování osobních údajů,

- právo na přenositelnost osobních údajů,
- právo vznést námitku proti zpracování osobních údajů a
- právo nebýt předmětem automatizovaného individuálního rozhodování.

8. Jak mohu svá práva jako subjekt údajů žádat o výkon svých práv?

O výkon svých práv můžete žádat jak správce, tak zpracovatele osobních údajů, prostřednictvím žádosti, kterou jim zašlete. V žádosti popíšete, výkon jakého práva požadujete a správce je povinen Vám na žádost bez zbytečného odkladu odpovědět, popřípadě jí vyhovět, pokud se nejedná o komplikovaný případ.

9. Jaké přináší GDPR výhody pro subjekty osobních údajů?

Nařízení poskytuje nástroj k získání kontroly nad vlastními osobními údaji. Za zmínku pak stojí především:

- právo být zapomenut, tj. právo na to, aby správce při splnění daných podmínek vymazal veškeré osobní údaje, jejichž účel zpracování pominul,
- snadnější přístup k osobním údajům a k informacím o jejich zpracování,
- právo vědět, zda nedošlo k úniku osobních údajů (pokud by porušení zabezpečení znamenalo pro práva a svobody subjektu údajů vysoké riziko),
- nastavení ochrany osobních údajů od počátku vytváření produktů a poskytování služeb.

10. Co je to právo být zapomenut?

Pokud se jedinec rozhodne, že už si nadále nepřeje, aby jeho osobní údaje byly zpracovávány, a zároveň není žádný další důvod pro jejich uchování, údaje musí být vymazány. Správce by měl vymazat osobní údaje nejen ve svých systémech, ale měl by informovat i další příjemce, jimž osobní údaje předal.

11. Kdo to je Pověřenec pro ochranu osobních údajů a s čím se na něj obracet?

Pověřenec pro ochranu osobních údajů je osoba, jejímž hlavním úkolem je výkon poradenské a informační činnosti v oblasti ochrany osobních údajů ve vztahu ke správci nebo zpracovateli a jejich zaměstnancům, stejně jako výkon dohledu nad dodržováním GDPR a souvisejících právních předpisů v oblasti ochrany osobních údajů. Vodárenské společnosti podléhají povinnosti jmenovat Pověřence pouze za předpokladu, že provádí rozsáhlé zpracování zvláštních kategorií osobních údajů. Agenda pověřence zahrnuje i působení v pozici kontaktní osoby v procesu komunikace a konzultace s dozorovým úřadem, jemuž usnadňuje činnost tím, že mu zajistí přístup k jím vyžádaným dokumentům a informacím a umožní mu uplatnění jeho vyšetřovacích, nápravných, povolovacích a poradních pravomocí. Zaměstnanci vodárenské společnosti se tedy na tuto osobu mohou obracet ve všech záležitostech týkajících se ochrany osobních údajů, zejména pak s žádostmi o poskytnutí rady a konzultace.

Klíčové kontakty

Martin Bohuslav

Advokát, partner

Tel: +420 724 583 971
Email: mbohuslav@deloittece.com

Jaroslava Kračúnová

Advokátka – oblast ochrany osobních údajů

Tel: +420 724 705 824
E-mail: jkracunova@deloittece.com

Zdeněk Horáček

Advokát – oblast vodárenství

Tel: +420 725 001 424
E-mail: zhoracek@deloittece.com

Mobilní aplikace Deloitte CZ

Android iOS

Zpravodaje I Studie I Semináře I Novinky I Videa

Deloitte.
Legal

„Deloitte Legal" označuje právní oddělení přidružených členských firem společnosti Deloitte Touche Tohmatsu Limited poskytující právní služby. Z právních a regulatorních důvodů ne všechny členské firmy poskytují právní služby.

Deloitte označuje jednu či více společností Deloitte Touche Tohmatsu Limited, britské privátní společnosti s ručením omezeným zárukou („DTTL"), síť jejích členských firem a jejich spřízněných subjektů. Společnost DTTL a každá z jejích členských firem představuje samostatný a nezávislý právní subjekt. Společnost DTTL (rovněž označovaná jako „Deloitte Global") služby klientům neposkytuje. Více informací o naší globální síti členských firem je uvedeno na adrese www.deloitte.com/cz/onas.

Společnost Deloitte poskytuje služby v oblasti auditu, poradenství, právního a finančního poradenství, poradenství v oblasti rizik a daní a související služby klientům v celé řadě odvětví veřejného a soukromého sektoru. Díky globálně propojené síti členských firem ve více než 150 zemích a teritoriích má společnost Deloitte světové možnosti a poznatky a poskytuje svým klientům, mezi něž patří čtyři z pěti společností figurujících v žebříčku Fortune Global 500 ®, vysoce kvalitní služby v oblastech, ve kterých klienti řeší své nejkomplexnější podnikatelské výzvy. Chcete-li se dozvědět více o způsobu, jakým zhruba 244 000 odborníků dělá to, co má pro klienty smysl, kontaktujte nás prostřednictvím sociálních sítí Facebook, LinkedIn či Twitter.

Společnost Deloitte ve střední Evropě je regionální organizací subjektů sdružených ve společnosti Deloitte Central Europe Holdings Limited, která je členskou firmou sdružení Deloitte Touche Tohmatsu Limited ve střední Evropě. Odborné služby poskytují dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited, které jsou samostatnými a nezávislými právními subjekty. Dceřiné a přidružené podniky společnosti Deloitte Central Europe Holdings Limited patří ve středoevropském regionu k předním firmám poskytujícím služby prostřednictvím téměř 6 000 zaměstnanců ze 41 pracovišť v 18 zemích.