Trabantská 290/31
190 15 Praha 9 - Satalice

Vnitropodniková směrnice společnosti PPDS Group s.r.o. ke GDPR

GDPR nařízení stanoví pravidla týkající se výhradně ochrany fyzických osob. Nařízení se obecně vztahuje na osobní údaje všech fyzických osob, včetně OSVČ.
PPDS Group s.r.o. (dále jen firma):

- Zaměstnává do 25 zaměstnanců (nemá povinnost speciální evidence dle čl.30 obecného nařízení)
- Má méně než 100 zákazníků - fyzických osob.
- Používá interní databázi kontaktů- uložena v úložišti dat – šifrovaném a zabezpečeném heslem.
- Listinná podoba osobních dat je uložena v zamykatelných skříních.
- Je správcem a zpracovatelem osobních údajů výše uvedených

Vzhledem k tomu, že platný zákon č. 101/2000 Sb., o ochraně osobních údajů, dosud nebyl odpovídajícím způsobem novelizován, nezbývá než odkazovat přímo na nařízení Evropského parlamentu a Rady č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení“)

Pojmy:
Osobní údaje – veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Prvky osobních údajů:
o obecné: jméno, pohlaví, věk, datum narození, osobní stav, občanství, IP adresa;
o organizační: pracovní nebo osobní adresa, telefonní číslo, email, ověřovací identifikační údaje;
o citlivé osobní údaje: speciální kategorie – ještě více zpřísněna – rasový původ, politické názory, genetické údaje (např. DNA), biometrické údaje (např. otisk prstu).
Citlivé údaje – jsou speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Dále ještě genetické a biometrické údaje, využívané za účelem jedinečné identifikace fyzické osoby.
Právo být zapomenut – subjekt údajů má právo na to, aby správce bez zbytečného 9 provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti fyzické osoby. Bez odkladu vymazal osobní údaje, které se dané fyzické osoby týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, zejména tehdy, pokud byl naplněn účel pro které byly zpracovány.
Souhlasem se dle textu nařízení rozumí **jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle subjektu údajů**, který dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.
Právo na přístup – fyzická osoba má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.
Právo na opravu – fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se jí týkají. S přihlédnutím k účelům zpracování má fyzická osoba práva na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

Právo na přenositelnost údajů – fyzická osoba má právo získat osobní údaje, které se jí týkají, jež poskytla správci ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.
Posuzování vlivu na ochranu osobních údajů – pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro právo a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.
Pověřenec pro ochranu osobních údajů – pro některé organizace je povinnost mít pověřence – správce a zpracovatel jmenují pověřence pro ochranu osobních údajů.
Porušení ochrany dat – závažnější porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu.
Zpracování – jakákoliv 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 jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
Profilování – jakákoli forma 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.

Povinnost vůči fyzické osobě

- Zavedení vhodných opatření k zajištění zpracovávání pouze nezbytných osobních údajů;
- poskytnout fyzické osobě tyto informace: o totožnosti a údaje správce (správcem je přímo právnická osoba, firma) a o kontaktní osobě/pověřenci pro ochranu osobních údajů – zde je statutární orgán, resp. jednatel – Svoboda Vladislav; o účelu zpracování a právním základu; o příjemci nebo kategorie příjemců; o případný úmysl správce předat osobní údaje do třetí země – v této firmě se nepředpokládá; o době uchování údajů;
- umožnit subjektu údajů přístup ke zpracovávaným a spravovaným údajům;
- na žádost subjektu údajů opravit údaj;
- na žádost subjektu údajů umožnit výmaz;
- ve stanovených případech omezit zpracování;
- umožnit přenos údajů jinému správci;
- po naplnění účelu osobní údaje zlikvidovat.

Povinnost vůči úřadu pro ochranu osobních údajů:

- Posouzení dopadu na ochranu osobních údajů (např. v případě zpracování citlivých údajů);
- povinnost předběžné konzultace (v případě, že by z posouzení dopadu vyplynulo, že zpracování je vysoce rizikové); - v této firmě se nepředpokládá
- povinnost vést záznamy o zpracováních osobních údajů; - v této firmě viz výše
- povinnost ohlašovat případy narušení bezpečnosti;
- povinnost jmenovat pověřence ochrany osobních údajů; - v této firmě jednatel
- zpracovatelé ani správci již nemají povinnost oznámit dozorovému orgánu zpracování

1. Interní audit – analýza/mapování

A. s osobními údaji jakých osob je nakládáno

- *zaměstnanci* (v případě pracovněprávních vztahů je pracovní smlouva hodnějším titulem nežli výslovný souhlas, jelikož nakládání s osobními údaji je nezbytnost pro plnění pracovní smlouvy a nezbytnost pro plnění právních povinností, tj. samotný podpis pracovní smlouvy je postačující jako souhlas) Firma tedy jako zaměstnavatel zpracovává osobní údaje zaměstnanců. Tyto údaje musí shromažďovat z důvodu zákonné povinnosti vést mzdovou a personální agendu (např. jméno a příjmení zaměstnance, rodné číslo, datum narození, mít informaci o tom u jaké zdravotní pojišťovny je zaměstnanec veden, osobní hodnocení zaměstnance, mzdy). Tyto údaje zpracovává v zákonem daném období a rozsahu.
- *obchodní partneři/zákazníci* (u fyzické osoby – firma získává souhlas se zpracováním osobních údajů od zákazníků pomocí e-mailu při komunikaci se zákazníkem, ale má-li firma uzavřenou se zákazníkem smlouvu o dílo, akceptovanou objednávku apod., výslovný souhlas se zpracováním osobních údajů není potřeba dávat do smlouvy/objednávky, protože osobní údaje obsažené ve smlouvě jsou nezbytné pro splnění smluvní povinnosti.),

B. s jakými osobními údaji dotyčných osob je nakládáno

- základní identifikační údaje – jméno, příjmení/název firmy, bydliště/sídlo, datum narození/IČ, u kontaktní osoby obchodního partnera – jméno, příjmení, telefonní spojení, adresa el. pošty,
- u zaměstnanců dále údaje pro potřeby naplnění zákonných povinností zaměstnavatele – údaje o rodinném stavu, počtu dětí a jejich základní údaje

C. v jaké formě

- listinné – v šanonu dle příslušné agendy –
* mzdové
*poptávko/nabídkové
*dodavatelsko/odběratelské
* smluvní/zakázkové
- elektronické – v souboru

Počítač je náležitě zabezpečen proti případným internetovým útokům, či zničení/ztrátě (heslem, instalací antivirového softwaru, šifrováním atp.)
* Účetní program POHODA
* externí sítový disk

D. jaké operace se s údaji provádí -získávání, zpracování a likvidace

- dle zákonných požadavků státní správy i zpřístupňování, resp. předávání
- pro potřeby uzavření a realizace kontraktu získávání, zpracování, uchování a likvidace

E. jaké osoby a kdy s údaji pracují

1) účetní (pověřená osoba) při plnění výkonu zaměstnavatelských povinností
2) správce, resp. statutární orgán/jednatel a z jeho pověření zpracovatelé, resp. obchodník nebo pracovník příslušného oddělení - pověřená osoba) při získávání, uzavírání a realizaci kontraktů
3) firma neposkytuje osobní údaje třetím subjektům ani externím firmám

2. Účel

Každé nakládání s osobními údaji má svůj legitimní a legální účel.
Účel zpracování osobních údajů -
a. personální a mzdová agenda; - *zákonná povinnost*
b. plnění zákonné/*právní povinnosti* (například vedení knihy úrazů podle předpisů pracovního práva)
c. poptávající/odběratelé a dodavatelé; - na základě oprávněného zájmu plnění, *smluvní povinnosti případně souhlasu*)

Údaje zpracovávané pro jednotlivé účely jsou vedeny odděleně. (může tudíž nastat situace, že jeden údaj bude veden v několika evidencích, resp. údaje jsou zpracovávány pouze za účelem, pro který byly shromážděny. Využití údajů k jinému účelu je možné pouze při splnění zákonných podmínek).

3. Právní podklad

Každé zpracování osobních údajů musí být v plném rozsahu, tedy z hlediska zejména
(a) dotčených lidí (subjektů údajů), jejichž osobní údaje jsou zpracovávány,
(b) osobních údajů, které se zpracovávají,
(c) doby, po kterou se zpracovávají
(d) jednotlivých operací s údaji, pokryto některým z šesti právních titulů pro zpracování;
Je pokryta každá osoba, každý údaj, každá operace a vždy po celou dobu.
Právní důvody pro zpracování jsou:
a. souhlas dotyčného člověka (subjektu údajů);
b. plnění právní povinnosti správce založené právním předpisem nebo rozhodnutím (například vedení evidence pro daňové účely nebo pro účely mzdové, sociální apod.)
c. plnění smlouvy s dotyčným člověkem (subjektem údajů) včetně nezbytných opatření před uzavřením smlouvy na žádost takového člověka (například nájemní smlouva, pracovní smlouva);
d. oprávněný zájem správce nebo třetí strany (například ochrana majetku, kontaktování obchodního partnera), kdy tyto zájmy mají větší váhu než dotčené zájmy (soukromí a ochrana osobních údajů) člověka, s jehož údaji se nakládá (subjektu údajů);
(získání platného souhlasu je relativně komplikované, navíc je souhlas odvolatelný; souhlas nemusí být (vyjma citlivých údajů) výslovný, musí však být vždy prokazatelný. Souhlasem není možné rozšířit zákonné účely. Není možné využít souhlas, pokud se jedná o údaje, které mají být získány a zpracovávány na základě zákona; takové jednání by mohlo být kvalifikováno jako nesprávní informování dotčeného člověka (subjektu údajů) a mohlo by být sankcionováno. I souhlas je limitován principem nezbytnosti. Po určení účelu je třeba identifikovat právní titul zpracování).

4. Nezbytnost

V návaznosti na účel a právní podklad nakládání (zpracování) s osobními údaji je třeba určit, jaké osobní údaje jsou nebytné; legálně lze nakládat pouze s údaji, bez nichž není možné dosáhnout účelu, a které jsou kryty právním podkladem zpracování – resp. společnost získává a nakládá jen s nezbytnými údaji.
Doba uchování údajů - nesmí být ani delší (jednalo by se o neoprávněn zásah) a ani kratší (nebylo by možné dosáhnout účelu). Po uplynutí doby jsou údaje vymazány nebo alespoň trvale vyloučeny z dalšího zpracování. Případně lze, při splnění zákonných podmínek, navázat dalším zpracováním osobních údajů.

5. Přesnost

Osobní údaje jsou z hlediska účelu zpracování přesné. Přesností se v tomto případě míní i komplexnost údajů, pokud je například rozsah určen právním předpisem. S nepřesnými údaji není možné dosáhnout sledovaného účelu. Přesnost se zajišťuje pravidelnou aktualizací při komunikaci s dotyčným před naplněním daného účelu

6. Bezpečnost

Rizika jednotlivých fází nakládání s údaji
Zpracování = operace nebo soubor operací s osobními údaji prováděných pomocí či bez pomoci automatizovaných postupů, jako je:
o Shromažďování – sběr dat, získávání či vytěžování dat z různých zdrojů (přihlášky, veřejné rejstříky atd.)

o Zaznamenání – zápis dat (údajů) do předem definovaných polí
o Uspořádání – zvolený způsob organizace dat
o Strukturování – zápis dat podle předem definovaných standardů
o Uložení – zapsání dat do souboru či dokumentu, požadavek na uchování dat
o Přizpůsobení nebo pozměnění – upravení dat dle potřeby
o Vyhledání – nalezení správných údajů dle zadaného požadavku či kritéria
o Nahlédnutí – možnost podívat se na požadované informace bez možnosti získání papírové či elektronické formy výstupu
o Použití – aplikování dat dle potřeby
o Zpřístupnění přenosem – zaslání/předání elektronickou formou (e-mail, internet)
o Šíření nebo jiné zpřístupnění – poskytnutí dat veřejnosti papírovou či elektronickou formou
o Seřazení či zkombinování – třídění/zobrazení dat dle zadaného kritéria či vytažení dat z více zdrojů a složení dle pravidel
o Omezení – získání či poskytnutí pouze určitých dat
o Výmaz nebo zničení – zrušení záznamu či poškození nosiče dat, vymazání osobních dat z databáze
Předpokládá se, že v této firmě k rizikovým zpracováním údajů nedochází.

Bezpečnostní opatření
Určení a provedení odpovídajícího bezpečnostního opatření tak, aby byla rizika minimalizována a aby se pokud možno předešlo nepříznivým důsledkům
A) ztráta listinných údajů – málo pravděpodobné – nakládá s nimi jen pověřená osoba a data jsou fyzicky uložena v uzamykatelných spisovnách, archivech apod.
B) ztráta údajů/dat při jakékoliv fází nakládání s údaji – pravděpodobné - s daty smí nakládat jen pověřené osoby, nesmí je vynášet mimo firmu ani pořizovat opisy, či kopie, dodržují pravidla bezpečné komunikace
B) ztráta elektrických dat v důsledku zneužití nebo poškození disku – pravděpodobné – disk je zabezpečen heslem, příp. zašifrován, dochází k pravidelnému zálohování disku (zálohy jsou v zabezpečených úložištích), je pravidelně aktualizován antivirový program
C) ztráta dat při likvidaci – pravděpodobné – zajišťuje pověřený pracovník dle přesné specifikace prostřednictvím skartovacího stroje

Určení odpovědnosti, k přístupu a nakládání s údaji:
a. Osobní – řízení přístupu k osobním údajů
kdo - pověřené osoby příslušných oddělení
kdy – při vyřizovaní daného účelu
z jakého důvodu - při vyřizovaní daného účelu
(například personalista při zpracování mezd)
b. Prostorové – řízení přístupu k údajům:
- klíče od spisovny a přístup k zálohám dat má jen statutární orgán, který je vydává a zpět přebírá od pověřených osob
c. Výpočetní techniky - řízení přístupu k údajům
- uživatelsky oprávněn spravovat zálohy dat jen statutární orgán, resp. s pomocí IT specialisty – řeší potřebná bezpečnostní opatření jako jsou hesla, antivirové programy atp.).

Smluvní doložky:
Mezi prvky k zajištění bezpečnosti spadá i uzavíraní smluv odběratelsko/dodavatelských. Smlouva má předepsané náležitosti podle čl. 28 odst. 3 obecného nařízení. Měla by však obsahovat i pravidla pro komunikaci, spolupráci stran, rozdělení úkolů ve vztahu k plnění povinností vůči subjektům údajů, pravidla k zajištění bezpečnosti informací o zabezpečení a informací o parametrech zpracování atp.

Do budoucna by měly existovat (schválené Komisí EU nebo Úřadem pro ochranu osobních údaj) tzv. standardní smluvní doložky, které by měly pokrývat základní náležitosti smlouvy. Dále je třeba zajistit bezpečnost vůči třetím osobám (poskytovatelům služeb), které se pohybují (fyzicky nebo online) ve sféře správce, jejichž úkolem však není zpracovávat osobní údaje, ale mohou mít k údajům přístup nebo mohou mít přístup k informacím o jejich zabezpečení nebo informacím o zpracování jako takovém.

Vnitropodniková směrnice:

určuje, pro všechny interní i externí pracovníky firmy (mimo zaměstnanců se jedná např. o IT podporu, úklidovou službu apod.) smluvní garance k zajištění bezpečnosti. Jedná se o vhodná organizačně technická opatření k zajištění bezpečnosti údajů a informací tzv. kodex chování. Všichni zaměstnanci berou na vědomí, že se v prostorách firmy se nachází osobní údaje a jsou povinni chovat se tak, aby při realizaci předmětu smlouvy (tj. při své práci) nedošlo k jejich odcizení, zničení či ztrátě. Všichni pracovníci firmy jsou součástí přijatých bezpečnostních opatření a jsou pravidelně školeni, jak se chovat, přichází-li do kontaktu s danými údaji a informacemi. Bezpečnostní opatření, jejich efektivita a spolehlivost, je pravidelně prověřována a bezpečnostní opatření jsou upravována, obnovována a doplňována dle potřeby. (Ve stanovených případech bude třeba provádět tzv. posouzení vlivu na ochranu osobních údajů viz čl. 35 an. obecného nařízení)

Samostatnou oblastí vyžadující zvláštní záruky (například standardní smluvní doložky) je využití služeb mimo EU – zde jde o tzv. předávání osobních údajů do třetích zemí, což se v této firmě nepředpokládá.

(V této fázi je tedy třeba formulovat informaci pro jednotlivá zpracování a určit vhodný způsob plnění informační povinnosti. Informace musí být formulována srozumitelně, jednoduchým jazykem; v této souvislosti je vhodné využívat jednak mnohovrstevnost informací a jednak, až budou vydány, standardizované ikony.)

8. Práva Subjektu údajů vůči správci v souvislosti se zpracováním osobních údajů náleží řada práv (právo na informace, právo přístup k osobním údajů, včetně kopie zpracovávaných osobních údajů, právo na opravu údajů, právo na výmaz údajů, právo na omezení zpracování, právo na námitku atd.). V návaznosti na povahu jednotlivých zpracování (zda se realizují elektronicky nebo v listinné formě, zda jsou povinná podle právního předpisu nebo se realizují na základě souhlasu subjektu údajů) může být rozsah práv různý. K žádosti (uplatnění práva) musí správce reagovat v zákonné lhůtě. Uplatňování práv je bezplatné. Jen v předepsaných případech je možné žádost odmítnout či vyřízení žádosti zpoplatnit. Je tudíž třeba ve vztahu ke každému ze zpracování osobních údajů určit práva, která člověku náleží. Tuto informaci je třeba zahrnou do informační povinnosti (bod 7). Dále je třeba určit proces, jehož prostřednictvím bude žádost o uplatnění práva vyřizována, včetně procesu, jímž budou realizována opatření, kterými se bude reagovat na žádost subjektu údajů (například se provede oprava). Subjektu údajů náleží mj. právo podat stížnost k Úřadu pro ochranu osobních údajů ohledně vyřízení jeho žádosti o uplatnění práv. 5

9. Úřad pro ochranu osobních údajů – komunikace

Správce (resp. statutární orgán) je schopen po celou dobu zpracování osobních údajů prokázat (v případě kontroly), že řádně plní jednotlivé povinnosti plynoucí z právní úpravy (zásada odpovědnosti), jak jsou popsány v bodech 1 až 8 shora.

Firma vede dokumentaci k jednotlivým zpracováním, rozdělenou podle účelů (viz program POHODA – příslušné sestavy – evidují základní parametry zpracování a zaznamenávají další podstatné skutečnosti, jako je například uplatnění práva ze strany subjektu údajů a související reakci a opatření správce.

Právě popsaná evidence není záznamem o činnostech zpracování. Záznamy o činnostech zpracování (čl. 30 obecného nařízení) jsou speciální evidence jednotlivých zpracování s předepsanou strukturou, kterou musí správce (až na předepsané výjimky) vést primárně pro případ kontroly ze strany Úřadu pro ochranu osobních údajů; jedná se o evidenci obdobnou stávajícím záznamům ve veřejném registru zpracování (viz www.uoou.cz – sekce registr).

Výjimku z povinnosti vést záznamy o činnostech zpracování mají malé a střední podniky, které zaměstnávají méně než 250 zaměstnanců. Uvedená výjimka se nevztahuje na malé a střední podniky, jestliže jejich zpracování pravděpodobně představuje riziko pro práva a svobody fyzických osob, zpracování není příležitostné nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Správce musí zaznamenat každé porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů (například ztrátu zabezpečeného nosiče s osobními údaji, který neobsahuje jejich jedinou kopii). Pokud takový bezpečnostní incident představuje riziko pro práva a svobody subjektu údajů je povinností jej způsobem určeným Úřadem pro ochranu osobních údajů (zatím nebyl způsob určen) oznámit jmenovanému úřadu; oznamované informace se uvádí v čl. 33 odst. 2 obecného nařízení. Oznámení se činí bez zbytečného odkladu, nejpozději však do 72 hodin od chvíle, kdy se o něm správce dozví.

Ohlášení musí přinejmenším obsahovat:

- popis povahy daného případu porušení zabezpečení osobních údajů (např. hackerský útok na internetové bankovnictví);
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů (např. pravděpodobnost neoprávněného přístupu k bankovním účtům);
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů (např. dočasné zablokování internetového bankovnictví a výzva klientům k bezodkladné změně hesel).

Pokud by takový bezpečnostní incident představovat vysoké riziko pro subjektu údajů (například nahlédnutí do personálního spisu neoprávněnou osobu, kdy spis obsahuje krom jiného jméno, příjmení, datum narození, rodné číslo a bydliště subjektu údajů, nebo ztráta přístupových údajů do elektronického bankovnictví subjektu údajů), oznámí se vedle úřadu i dotyčnému člověku, včetně opatření, která by měl přijmout k tomu, aby předešel možným negativním důsledkům.

V Praze dne 25/5/18

Odpovědný zástupce PPDS při zpracování této směrnice postupoval s odbornou péčí:

Zdroje:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- 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 pobytu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Internetové stránky:
  - o http://eur-lex.europa.eu/legalcontent/CS/TXT/HTML/?uri=CELEX:32016R0679&from=en
  - o www.uoou.cz
  - o https://www.uoou.cz/obecne-narizeni-eu-gdpr/ds3938/p1=3938
  - o http://ec.europa.eu/newsroom/just/itemdetail.cfm?item_id=52946
  - o www.komora.cz