STATUTÁRNÍ MĚSTO LIBEREC

Poznámka: Zveřejněna je pouze upravená verze dokumentu z důvodu dodržení přiměřenosti rozsahu zveřejňovaných osobních údajů podle zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění.
Osobní údaje jsou v souladu s § 16, § 17 a § 95 zákona č. 128/2000 Sb., o obcích v platném znění.

I N F O R M A C E

pro jednání zastupitelstva města dne 26.04.2018

Ochrana osobních údajů dle nařízení EU č. 2016/679 ze dne 14. 4. 2016, účinné od 25. 5. 2018

Předkládá: **Batthyány Tibor - primátor statutárního města Liberec**

Zpracoval: Batthyány Tibor - primátor statutárního města Liberec

Důvodová zpráva

Důvodová zpráva

Pro ochranu osobních údajů je dosud platná Směrnice Evropského parlamentu 95/46/ES (ze dne 24. 10. 1995) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Postupně však vzniklo 28 různých národních právních předpisů, což s postupující globalizací přineslo stále větší problémy na úrovni ochrany osobních údajů fyzických osob.

Dne 14. 4. 2016 Evropský parlament schválil Obecné nařízení o ochraně osobních údajů, s účinností od 25. května 2018 – Nařízení EU číslo 2016/679 – General Data Protection Regulation (GDPR).

Obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru. Ode dne 25. května 2018 nahradí český zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

GDPR je vydán formou přímo účinného nařízení, které není nutné transponovat do právních řádů členských států EU.

Přílohy

Příloha č. 1 - Informace - podrobnější - GDPR od 05.2018

I. Hlavní změny plynoucí z GDPR:

1. **Posílení práv subjektů údajů** – GDPR klade hlavní důraz na práva subjektů údajů jejich dodržování ze strany správce/zpracovatele
2. **Širší informační povinnost** – správce je povinen subjekty údajů dostatečně informovat o účelu, právním základě, zpracování osobních údajů a o jejich právech apod.
3. **Nové požadavky na smlouvu o zpracování osobních údajů** – smlouva mezi správcem a zpracovatelem musí být písemná a musí obsahovat bezpečnostní prvky ochrany osobních údajů (audit, bezpečnostní opatření, apod.)
4. **Jednoznačný souhlas k jakémukoli zpracování osobních údajů** – v případě „souhlasu" se zpracováním osobních údajů musí být „souhlas" svobodný, konkrétní, informovaný, jednoznačný"
5. **Odvolání souhlasu, právo být zapomenut –** subjekt údajů má kdykoliv během zpracování svých osobních údajů právo odvolat dříve udělený souhlas. Správce pak musí ukončit zpracování takových údajů
6. **Přenositelnost údajů** – správce je povinen zajistit na základě žádosti subjektu údajů přenos jeho údajů k jinému správci
7. **Vlastní vyhodnocení dopadů zpracování osobních údajů** – správce je povinen provést hodnocení vlastních aktivit a jejich dopadů na ochranu osobních údajů a na zájmy subjektů údajů, pokud jejich zpracování může představovat vysoké riziko
8. **Vznik Evropského sboru pro ochranu osobních údajů** – vznikne nový celoevropský orgán (nahrazující dosavadní skupinu WP29), který bude mít pravomoci především v oblasti konzultací a sjednocování výkladů sporných otázek v oblasti ochrany osobních údajů
9. **Pověřenec pro ochranu osobních údajů (DPO – Data Protection Officer) –** je-li správce nebo zpracovatel subjektem veřejné správy, je povinen ustavit nezávislého pověřence, pokud nakládání s osobními údaji tvoří základ jejich podnikání či poskytování služeb
10. **Ohlašovací povinnost –** v případě bezpečnostního incidentu v oblasti ochrany osobních údajů je správce i zpracovatel povinen incident hlásit dozorovému úřadu
11. **Odpovědnost správce** – správce je povinen zajistit soulad s GDPR a být schopen jej prokázat
12. **Dozorový orgán** – u nás Úřad pro ochranu osobních údajů
13. **Výrazně vyšší pokuty za neplnění povinností** – správce či zpracovatel může za porušení svých povinností čelit vysokým pokutám

II. Dopady GDPR na organizaci

1. **Hlavní činnost –** úprava procesů, úprava smluvní dokumentace, splnit podmínky zajištění/vydávání souhlasu se zpracováním osobních údajů, školení zaměstnanců, apod.
2. **Procesy, interní směrnice –** změny v procesu řízení a reportingů, změny v procesu řízení rizik, změny v procesu řízení lidských zdrojů, aktualizace smluv, aktualizace interních směrnic (vytvoření nových), apod.
3. **Informační a komunikační technologie –** revize datové a bezpečnostní architektury, revize komunikačních rozhraní, aktualizace tiskových šablon, upgrade systémů, aplikace bezpečnostních opatření na všech vrstvách ICT infrastruktury

III. Z obecného nařízení EU

1. Základní principy

Obecné nařízení GDPR je založeno na dvou nových přístupech, a to na principu odpovědnosti správce a přístupu založeném na riziku v tomto rozsahu:

a) **princip odpovědnosti** znamená odpovědnost správce za dodržení zásad zpracování, které jsou v obecném nařízení GDPR uvedeny v článku 5 odst. 1 a zároveň musí správce být schopen tento soulad doložit. K dokládání souladu budou mimo jiné sloužit osvědčení, certifikace či kodexy nebo záznamy o činnostech zpracování osobních údajů.

b) **Princip přístupu založeném na riziku** v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. V užším slova smyslu jde u přístupu založeném na riziku jako o aplikaci některých povinností pouze v případě, kdy zpracování osobních údajů či porušení zabezpečení (bezpečnostní incident) představuje riziko či vysoké riziko pro práva a svobody fyzické osoby. V tomto rozsahu princip založený na riziku se uplatňuje zejména u nových povinností: ohlašování, resp. oznamování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, resp. subjektu údajů, posuzování vlivu zpracování na ochranu osobních údajů a povinné konzultace s Úřadem pro ochranu osobních údajů, jejichž aplikace je vázána na přítomnost rizika či vysokého rizika pro práva a svobody fyzických osob.

2. Hlavní definice a pojmy

V souvislosti s ochranou osobních údajů dle obecného nařízení GDPR se setkáváme s novými pojmy, ale také s řadou pojmů, které jsou definovány v české právní úpravě. V následujícím výčtu jsou tyto klíčové pojmy z ochrany osobních údajů uvedeny:

a) **Anonymní údaj –** takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k identifikované nebo identifikovatelné fyzické osobě.

b) **Automatizované zpracování –** je běžně rozšířenou formou zpracování osobních údajů za použití výpočetní techniky, bez lidského zásahu.

c) **Biometrický údaj –** osobní údaj technického charakteru zpracování fyzických či fyziologických znaků fyzické osoby, který umožňuje jedinečnou identifikaci. Typickým biometrickým údajem je např. snímek obličeje, otisk prstu, apod.

d) **Dozorový úřad –** Úřad pro ochranu osobních údajů (zkráceně ÚOOÚ) je v České republice nezávislým orgánem.

e) **Identifikovatelná fyzická osoba –** 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.

f) **NDA smlouva –** Non-disclosure agreement – Smlouva či dohoda o mlčenlivosti sjednaná v případě, že dvě strany si vzájemně (či jen jedna strana druhé) chtějí zpřístupnit nějaké informace, data či znalosti, u nichž je vhodné omezit jejich využití jen ke sjednanému účelu (např. v rámci pracovního poměru, obchodního jednání, ochrany osobních údajů, apod.).

g) **Omezení zpracování –** označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu. Způsoby, jak omezit zpracování osobních údajů, by mohly mimo jiné zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek. V systémech automatizovaného zpracování by omezení zpracování mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno, musí být v systému jasně vyznačena.

h) **Osobní údaj –** veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

i) **Osvědčení o ochraně údajů –** osvědčení (certifikát) vydávané subjektem pro vydávání osvědčení (certifikačním orgánem) pro účely prokázání souladu s obecným nařízením GDPR v případě operací zpracování prováděných správci a zpracovateli. V případě České republiky je vnitrostátním certifikačním orgánem Český institut pro akreditaci, o.p.s.

j) **Pověřenec pro ochranu osobních údajů –** neboli DPO (z anglického Data Protection Officer). Hlavním úkolem DPO je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z obecného nařízení GDPR, poradenství správcům a spolupráce s dozorovým úřadem.

k) **Právní důvody –** oprávnění správce osobní údaje zpracovávat. Právní důvody jsou nezbytným předpokladem, aby se vůbec dalo mluvit ze strany správce o legálním zpracování, neboť pokud by správce nedisponoval řádným právním důvodem ke zpracování osobních údajů, nebyl by schopen doložit plnění svých povinností při ochraně osobních údajů fyzických osob, jelikož by osobní údaje zpracovával nezákonně a musel by osobní údaje zlikvidovat. Výčet právních důvodů:
   - Subjekt údajů udělil souhlas pro jeden či více konkrétních účelů.
   - Zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů.
   - Zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje.
   - Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
   - Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.
   - Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.

l) **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.

m) **Příjemce –** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem ČR, se za příjemce nepovažují. Orgány veřejné moci, kterým jsou osobní údaje sdělovány na základě právní povinnosti pro účely výkonu jejich úředních povinností, jako jsou daňové a celní orgány, finanční vyšetřovací jednotky, nezávislé správní orgány nebo orgány finančního trhu příslušné pro regulaci trhů s

cennými papíry a dohled nad nimi, by neměly být považovány za příjemce, pokud obdrží osobní údaje, které jsou nezbytné pro provedení konkrétního šetření v obecném zájmu v souladu s právem EU či ČR. Žádost o sdělení osobních údajů zaslaná orgány veřejné moci by měla být vždy písemná a odůvodněná, měla by se týkat jednotlivého případu a neměla by se vztahovat na celou evidenci ani vést k propojení evidencí. Zpracování osobních údajů těmito orgány veřejné moci by mělo být v souladu s platnými pravidly pro ochranu osobních údajů podle účelů zpracování.

n) **Pseudonymizace –** je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejné fyzické osoby, aniž by bylo nutné znát její totožnost. Pseudonymizované osobní údaje nejsou anonymizovanými údaji, proto se na ně stále vztahuje regulace GDPR.
o) **Souhlas subjektu údajů –** jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.
p) **Správce –** fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů Jsou-li účely a prostředky zpracování určeny právními předpisy EU či České republiky, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.
q) **Správní pokuty –** za porušování zásad pro zpracování osobních údajů včetně podmínek týkajících se souhlasu dle článků 5, 6, 7 a 9 obecného nařízení GDPR jsou stanoveny nejvyšší správní pokuty až do výše 20 000 000 EUR nebo 4% celosvětového ročního obratu společnosti, podle toho, která částka je vyšší. Pro orgány veřejné moci je výše pokuty stanovena na 10 000 000 Kč.
r) **Subjekt údajů –** identifikovaná nebo identifikovatelná fyzická osoba. 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.
s) **Třetí strana –** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.
t) **Uchovávání osobních údajů –** udržování údajů v takové podobě, která je umožňuje dále zpracovávat.
u) **Zásady zpracování –** jednotlivé zásady jsou rozvinuty v článku 5 odst. 1 nařízení GDPR. K prokazování souladu se zásadami slouží záznamy o činnostech zpracování (u organizací též osvědčení, směrnice a kodexy). Výčet zásad zpracování:
   - Zákonnost, korektnost, transparentnost - správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně.
   - Omezení účelu - osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely.
   - Minimalizace údajů - osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány.
   - Přesnost - osobní údaje musí být přesné.
   - Omezení uložení - osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.
   - Integrita a důvěrnost - technické a organizační zabezpečení osobních údajů.
   - Odolnost – schopnost odolávat hrozbám

v) **Zpracovatel –** fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
w) **Zpracování –** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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. Zpracování ve smyslu obecného nařízení GDPR však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu např. zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením GDPR se tak jako správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu výše uvedené definice zpracování.
x) **Zvláštní kategorie osobních údajů –** osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zpracování genetických a biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
y) **Žadatel o vydání osvědčení –** subjekty/správci (klienti certifikace) využívající prostředky ke zpracování osobních údajů nebo dodavatelé nabízející prostředky, jejichž využitím dochází nebo může docházet ke zpracování osobních údajů.

3. Odpovědnost správce

a) Dle obecného nařízení GDPR je stanovena odpovědnost správce za jakékoliv zpracování osobních údajů prováděné správcem nebo pro něj. Správce je zejména povinen zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování jsou v souladu s tímto obecným nařízením GDPR, včetně účinnosti opatření. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob.
b) Správce odpovídá za identifikaci a analýzu různě pravděpodobných a závažných rizik pro práva a svobody fyzických osob, která mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů.
c) Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů se určují na základě povahy, rozsahu, kontextu a účelů zpracování. Riziko se hodnotí na základě

objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko.

d) V zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto obecným nařízením GDPR, odpovídá správce nebo zpracovatel za posouzení rizik spojených se zpracováním a přijetí opatření ke zmírnění těchto rizik, například šifrováním dat. Tato opatření by měla zajistit náležitou úroveň bezpečnosti, včetně důvěrnosti, s ohledem na stav techniky, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny. Při posuzování rizik pro zabezpečení osobních údajů by se měla vzít v úvahu rizika, která zpracování představuje, jako jsou náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě.
e) Správce odpovídá za jmenování Pověřence pro ochranu osobních údajů pokud:
   - Zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí.
   - Hlavní činnosti organizace spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů.
   - Hlavní činnosti organizace spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech.

4. Záznamy zpracování

a) Povinností správce a zpracovatele je uchovávání záznamů o činnostech zpracování pro doložení shody zpracování s obecným nařízením GDPR dle příslušných zásad.
b) Rozsah záznamů o činnostech zpracování je stanoven obecným nařízením GDPR minimálně v níže uvedené podobě, přičemž předepsaná forma je písemná včetně elektronické podoby.

Záznamy správce	**Záznamy zpracovatele**
Jméno a kontaktní údaje správce, společné správce a/nebo jmenovaného zástupce a pověřence	Jméno a kontaktní údaje zpracovatele a každého správce, jehož jménem zpracovává osobní údaje, jmenovaného zástupce správce nebo zpracovatele a pověřence
Účely zpracování	Kategorie zpracování vykonávaných jménem každého správce
Popis kategorií subjektů údajů a kategorií osobních údajů	Detaily všech přesunů osobních údajů do třetích zemí nebo mezinárodních organizací, včetně jejich jasné identifikace a dokumentace vhodných záruk
Kategorie příjemců, kteří mají k údajům přístup, včetně těch, kteří jsou mimo Evropskou unii	Obecný popis technických a organizačních opatření v oblasti bezpečnosti
Detaily všech přesunů osobních údajů do třetích zemí nebo mezinárodních organizací, včetně jejich jasné identifikace a dokumentace vhodných záruk	
Doba pro výmaz různých kategorií osobních údajů	
Obecný popis technických a organizačních opatření v oblasti bezpečnosti	

5. Zajištění souladu zpracování osobních údajů s obecným nařízením GDPR

a) Soulad nebo též shodu ochrany údajů při jejich zpracování prokazuje na základě principu odpovědnosti správce nebo zpracovatel v rozsahu stanoveném pro oblasti, které jsou definovány dozorovým úřadem a obecným nařízením GDPR.
b) Správce musí být schopen dodržení souladu dokumentovat.
c) Správce musí prověřovat soulad opakovaně s cílem optimalizovat činnosti a jejich zabezpečení s ohledem na všechna zpracování osobních údajů, která provádí nebo jimi pověřuje své smluvní zpracovatele.
d) Definované oblasti, které jsou posuzovány pro soulad s obecným nařízením GDPR:
   - Jsou dodrženy základní zásady zpracování v souladu s článkem 5 obecného nařízení GDPR.
   - Zpracování osobních údajů je prováděno zákonným způsobem v souladu s články 6 a 9 obecného nařízení GDPR.
   - Podmínky vyjádření souhlasu subjektu údajů jsou v souladu s článkem 7 obecného nařízení GDPR.
   - Osobní údaje ve věci rozsudků v trestných věcech a trestných činů a souvisejících bezpečnostních opatřeních jsou zpracovány za definovaných podmínek v souladu s článkem 10 obecného nařízení GDPR.
   - Je zajištěna požadovaná informovanost subjektu údajů v souladu s články 12 až 14 obecného nařízení GDPR.
   - Jsou zajištěna práva subjektu údajů v souladu s články 15 až 21 obecného nařízení GDPR.
   - Je zajištěno řízení bezpečnosti osobních údajů v souladu s články 24, 25 a 32 obecného nařízení GDPR.
   - Jsou zajištěny podmínky pro zpracování osobních údajů správcem nebo zpracovatelem se sídlem mimo EU v souladu s článkem 27 obecného nařízení GDPR.
   - Správce provádí zpracování prostřednictvím zpracovatele za požadovaných podmínek v souladu s články 28 a 29 obecného nařízení GDPR.
   - Správce nebo zpracovatel provádí v souladu s článkem 30 obecného nařízení GDPR záznamy o činnostech zpracování.
   - Správce nebo zpracovatel řeší porušení zabezpečení osobních údajů požadovaným způsobem v souladu s články 33 a 34 obecného nařízení GDPR.
   - Správce provedl v souladu s článkem 35 obecného nařízení GDPR posouzení vlivu na ochranu osobních údajů.
   - Správce zajistil předchozí konzultaci s dozorovým úřadem v souladu s článkem 36 nařízení GDPR.
   - Správce ustanovil v souladu s články 37 až 39 obecného nařízení GDPR pověřence pro ochranu osobních údajů.
   - Správce zpracovává osobní údaje v souladu s články 40 a 41 obecného nařízení GDPR dle kodexu chování.
   - Správce předává osobní údaje do třetích zemí nebo mezinárodním organizacím v souladu s články 44 až 50 obecného nařízení GDPR.

5. Zpracovatelé

a) Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva EU nebo ČR, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů

údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

- Zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo EU nebo ČR, které se na správce vztahuje. V takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.
- Zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.
- Přijme všechna opatření požadovaná podle článku 32 obecného nařízení GDPR.
- Dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v článku 28 odstavce 2 a 4 obecného nařízení GDPR.
- Zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených obecným nařízením GDPR.
- Je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici.
- V souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo EU nebo ČR nepožaduje uložení daných osobních údajů.
- Poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené mu správcem, a umožní audity, včetně inspekcí, prováděných správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

b) Smlouva nebo jiný právní akt mezi správcem a zpracovatelem / zpracovateli musí být vyhotoveny písemně, v to počítaje i elektronickou formu.

c) Smlouva musí minimálně stanovit následující parametry:

- Předmět zpracování.
- Dobu zpracování.
- Povahu zpracování.
- Účel zpracování.
- Typ osobních údajů.
- Kategorii subjektů údajů.
- Povinnosti a práva správce.
- Závazky zpracovatele, který:
    - Zpracovává osobní údaje pouze na základě pokynu správce.
    - Informuje správce o předávání do zahraničí, včetně povinnosti předávat na základě požadavků práva EU nebo ČR (pokud to právní předpis nezakazuje z důvodu veřejného zájmu).
    - Přijímá závazek mlčelivosti zaměstnanců zpracovatele.
    - Přijímá vhodná technická a organizační opatření na ochranu osobních údajů.
    - Zapojuje do zpracování další zpracovatele pouze s písemným svolením správce a informuje správce o všech zamýšlených změnách týkajících se zpracovatelů.
    - Zajišťuje, že při řetězení zpracovatelů musí každý další první zpracovatelem vybraný zpracovatel přijmout stejné povinnosti jako první zpracovatel.
    - Pokud předává osobní údaje, dochází k němu na základě rozhodnutí Komise nebo jiných nástrojů poskytujících vhodné záruky.

- Umožní audity prováděné správcem nebo jiným auditorem, kterého správce pověřil.
- Po ukončení zpracování osobní údaje vrátí správci, nebo je na základě pokynu správce vymaže (pokud právo EU nebo ČR nestanoví jinak).
- Je správci nápomocen při plnění jeho povinnosti reagovat na žádosti o výkon práv subjektů údajů.
- Je správci nápomocen při zajišťování zabezpečení zpracování, ohlašování případů porušení ochrany osobních údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace.

6. Práva subjektu údajů

Práva subjektu údajů jsou důležitým prvkem ochrany osobních údajů jako celku, jelikož subjekt údajů je často ve slabším postavení než správce a tudíž vybalancovávají vztah mezi ním a správcem.

Výčet práv subjektu údajů:

a) **Na přístup k informacím –** se rozumí oprávnění subjektu údajů na základě jeho aktivní žádosti získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:
   - Účely zpracování.
   - Kategorie dotčených osobních údajů.
   - Příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny.
   - Plánovaná doba, po kterou budou osobní údaje uloženy.
   - Existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku.
   - Právo podat stížnost u dozorového úřadu.
   - Veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.
   - Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

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

c) **Na výmaz údajů („být zapomenut“)** – představuje v obecném nařízení GDPR jinými slovy vyjádřenou povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:
   - Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány.
   - Subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování.
   - Subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování.
   - Osobní údaje byly zpracovány protiprávně.
   - Osobní údaje musí být vymazány ke splnění právní povinnosti.
   - Osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení GDPR.

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

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

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

d) **Na omezení zpracování –** je zcela nové právo subjektu údajů omezit zpracování osobních údajů správcem.
e) **Na přenositelnost zpracování –** je zcela nové právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému správci, je-li to technicky proveditelné.
   Společné podmínky k aplikaci práva na přenositelnost:
   - Musí jít o zpracování založené na právním důvodu souhlasu či smlouvě.
   - Zpracování se provádí automatizovaně.
f) **Na námitku proti zpracování –** subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:
   - Zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.
   - Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

   Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

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

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

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

7. Informační povinnost vůči subjektům údajů

a) Povinnosti správce v oblasti poskytování transparentních informací, sdělení a postupů pro výkon práv subjektů údajů jsou detailně upraveny v článcích 12, 13 a 14 obecného nařízení GDPR.
b) Výjimka z povinnosti poskytnout informaci je přípustná pouze v tom případě, že subjekt údajů již těmito informacemi disponuje. Správce však musí být v případě potřeby schopen prokázat, že subjekt údajů byl skutečně informován o všech požadovaných informacích, tj. že došlo ke splnění informační povinnosti dle obecného nařízení GDPR.
c) Do poskytovaných informací subjektu údajů patří:
   - Totožnost a kontaktní údaje správce a jeho případného zástupce.
   - Případně kontaktní údaje případného pověřence pro ochranu osobních údajů.
   - Účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování.
   - Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f).
   - Případné příjemce nebo kategorie příjemců osobních údajů.
   - Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci.
d) Vedle informací uvedených v předchozím odstavci 3 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:
   - Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby.
   - Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů.
   - Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním.
   - Existence práva podat stížnost u dozorového úřadu.
   - Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů.
   - Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4 obecného nařízení GDPR, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.
   - Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.
   - Odstavce 1, 2 a 3 se nepoužijí, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má.
   - Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 obecného nařízení GDPR a učinil veškerá sdělení podle článků 15 až 22 a 34 obecného nařízení GDPR o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve

vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

- Pokud se jedná o žádost podle článků 15 až 22 obecného nařízení GDPR, musí být informace o přijatých opatřeních poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.
- Zásadně platí, že informace podle článků 13 a 14 a veškerá sdělení a úkony podle článků 15 až 22 a 34 obecného nařízení GDPR se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce.

8. Ohlašování porušení zabezpečení osobních údajů

a) Správce nebo zpracovatel je povinen řešit porušení zabezpečení osobních údajů požadovaným způsobem v souladu s články 33 a 34 obecného nařízení GDPR.

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

c) Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

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

e) Pokud nastane porušení zabezpečení u zpracovatele, hlásí jej bez zbytečného odkladu správci, pro kterého dotčené osobní údaje zpracovává.

f) Obsah ohlášení dozorovému úřadu:
   - Popis povahy porušení zabezpečení osobních údajů.
   - Kategorie dotčených subjektů údajů.
   - Počet dotčených subjektů údajů.
   - Množství dotčených záznamů.
   - Identifikace osoby nebo kontaktního místa, které poskytuje bližší informace (jméno, příjmení, adresa, telefon, e-mail apod.).
   - Popis pravděpodobných důsledků porušení ochrany osobních údajů.
   - Popis opatření přijatých s cílem vyřešit porušení bezpečnosti osobních údajů:

g) Způsob ohlášení incidentu dozorovému úřadu je definován přímo dozorovým úřadem. K tomuto účelu je k dispozici elektronický formulář a instrukce pro jeho vyplnění na

webu dozorového úřadu: https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-uradu-pro-ochranu-osobnich-udaju/ds-1573/p1=1573.

h) Způsob oznámení incidentu subjektům údajů je definován přímo dozorovým úřadem. K tomuto účelu jsou instrukce na webu dozorového úřadu: https://www.uoou.cz/oznameni-o-naruseni-bezpecnosti-osobnich-udaju-subjektum-udaju/ds-1625/p1=1625.

9. Zabezpečení ochrany osobních údajů

a) Dle nařízení obecného GDPR jsou správce a zpracovatel povinni zavést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, a to případně včetně pseudonymizace a šifrování dat.

b) Mezi další způsoby opatření pro zabezpečení ochrany zpracování osobních údajů tak patří:

- Při manuálním i automatizovaném zpracování:
  - Zámky, mříže, čipy, karty, klíčový systém, trezory, apod.
  - Centrální pult ochrany.
  - Elektronické zabezpečení.
  - Kamerové systémy.
- Při automatizovaném zpracování:
  - Hesla, PIN, přístupová práva, role uživatelů, vícefaktorové ověřování, apod.
  - Bezpečnostní zálohy a ochrana datových nosičů.
  - Evidence přístupu k datům a nakládání s daty, provozní deník, logování apod.
  - Šifrování.
  - Antivirová ochrana.
  - Vedení předávacích protokolů vůči třetím stranám.
  - Zpracovatelská smlouva.
  - NDA smlouva.
- Obecně pro všechny kategorie zpracování:
  - Bezpečnostní směrnice.
  - Příručky a pokyny pro uživatele (provozní řád).
  - Školení uživatelů.
  - Dokumentace k přijatým technicko-organizačním opatřením.
  - Pravidelné kontroly funkčnosti technicko-organizačních opatření.

10. Pověřenec pro ochranu osobních údajů

Úkoly pověřence jsou stanoveny obecným nařízením GDPR v článku 39 v minimálním rozsahu:

a) Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto obecného nařízení GDPR a dalších předpisů EU nebo ČR v oblasti ochrany údajů.

b) Monitorování souladu s tímto obecným nařízením GDPR, dalšími předpisy EU nebo ČR v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů.

c) Poskytování poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 obecného nařízení GDPR.

d) Spolupráce s dozorovým úřadem.

e) Působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 obecného nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci

.

IV. Realizace nařízení v prostředí SML

Statutární město Liberec při plnění veřejných úkolů vystupuje při zpracování osobních údajů v pozici správce i zpracovatele.

1. Rada města dne 7. 11. 2017 svým usnesením č. 1117/2017 schválila „**Koncepci GDPR SML**“ na jejímž základě byly provedeny následující kroky:
   a) zadání realizace 1. etapy přijaté koncepce,
   b) ustanovení pracovní skupiny pro řešení implementace nařízení na ochranu osobních údajů,
   c) realizace analýzy činností MML (jednotlivých odborů) a MP jako základní podklad pro další kroky v oblasti GDPR a její implementace
      - inventura zpracovávání osobních údajů, jejich kategorizace a posouzení souladu s GDPR
      - inventura vnitřních předpisů a posouzení souladu s GDPR
      - Návrh organizačních opatření pro zajištění souladu
      - Návrh technických opatření
   d) návrh zajištění GDPR pro subjekty zřizované městem, tj. pro příspěvkové organizace (MŠ, ZŠ a další organizace),
2. Další připravovaná organizační, technologická, právní a technická, personální a ekonomická opatření, která budou reálně a prokazatelně směřovat k zajištění souladu ochrany osobních údajů organizace s principy GDPR:
   a) ustanovení pověřence pro SML
   b) příprava nové směrnice na ochranu osobních údajů pro MML a MP,
   c) příprava aktualizace směrnice IS SML (kybernetická bezpečnost),
   d) aktualizace směrnic MML, kterých se GDPR dotýká (organizační řád, spisový a skartační řád, zásady vyřizování petic, podnětů a stížností občanů, poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím a podle zákona č. 123/1998 Sb., o poskytování informací o životním prostředí, aj.)
   e) proškolení zaměstnanců SML k nařízení EU,
   f) návrh organizačních opatření pro zajištění souladu s GDPR,
   g) návrh technických opatření pro zajištění souladu s GDPR.

V. SML jako správce a zpracovatele osobních údajů

S ohledem na výše uvedené je nezbytně nutné ze strany zaměstnanců města a orgánů města nakládat s osobními údaji v souladu s nařízením EU o ochraně osobních údajů, u nichž je SML správcem či zpracovatelem. Tato povinnost se mimo jiné vztahuje i na výbory zastupitelstva a komise rady, pokud jejich členové nakládají s osobními údaji.

VI. Doporučení Úřadu pro ochranu osobních údajů

Pro nakládání s osobními údaji zveřejnil dozorový úřad na svých webových stránkách následující desatero:

1. Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, **musí být legitimní** a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování údajů musí být **založeno na některém ze základních důvodů** (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.
3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr - **účel zpracování údajů.**
4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být **vždy přiměřené účelu zpracování.**
5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít **jasný zákonný podklad**, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
6. Správce i zpracovatel osobních údajů musí osobní údaje **patřičně zabezpečit** a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně**. Informace o zpracování poskytované subjektu údajů musí být **zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci.**
8. Zpracování **nesmí nadměrně zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
9. Po naplnění účelu zpracování je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
10. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví obecné nařízení (GDPR). Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.

Poznámka:

Bližší informace k nařízení EU jsou přístupné např. na těchto webových stránkách:

Poř. číslo	Název dokumentu	Zdroj dokumentu
1.	Obecné nařízení GDPR Evropského parlamentu a rady (EU) 2016/679	http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN
2.	Úřad pro ochranu osobních údajů (dozorový úřad)	https://www.uoou.cz
3.	Pokyny pracovní skupiny WP29	https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/archiv=0&p1=3938
4.	Osvětový, vzdělávací a poradenský portál k problematice GDPR	https://www.gdpr.cz