Kritéria pro vydávání osvědčení a kritéria pro akreditaci (KVO)

k ochraně osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679

Verze 0.7
ze dne 27.10 2017

(Poznámka: V rámci českého překladu nařízení 2016/679 byla použita poněkud odlišná terminologie, která není v souladu se stávající terminologií používanou v oblasti akreditací. Proto v rámci textů je v závorce uváděn k pojmu z nařízení i ekvivalent dle současné terminologie v oblasti akreditací).

1. Úvod

Přijetím nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zrušení směrnice 95/46/ES (dále též jen nařízení) je do právního řádu z hlediska ochrany osobních údajů zaváděn nový institut, a to vydávání osvědčení o ochraně osobních údajů (certifikát) (čl. 42 nařízení odst. 1).

Dle výše uvedeného nařízení (čl. 42, odst. 1) se vydávání osvědčení uplatní v případě operací zpracování prováděných správcem nebo zpracovatelem a má osvědčit soulad s nařízením. Toto pojetí podporuje i text dalšího ustanovení (čl. 42. odst. 2), který uvádí, že při předávání osobních údajů do třetích zemí je vydání osvědčení (certifikátu) jednou z možností, jak prokáže správce nebo zpracovatel (a to zejména ze zemí mimo EU), že poskytuje vhodné záruky odpovídající úrovně ochrany osobních údajů. Z toho plyne, že by se vydávání osvědčení (certifikátu) mělo primárně týkat zpracování osobních údajů (která zahrnuje jednu nebo více operací) nebo systému řízení ochrany osobních údajů u správce nebo zpracovatele. V recitálu (důvodové zprávě) v bodě 100 je však též uvedeno, že vydávání osvědčení (certifikátu) má subjektům údajů zajistit, aby rychle mohly u příslušných produktů a služeb posoudit úroveň ochrany osobních údajů. Z toho plyne, že by se vydávání osvědčení (certifikátů) mělo týkat i produktů (sw a hw) a služeb.

V nařízení jsou definovány tři možnosti (čl. 43 odst. 1), jak vybrat subjekt pro vydávání osvědčení (certifikační orgán), jedná se jednak o postup, kdy za stanovených podmínek akredituje subjekty pro vydávání osvědčení (certifikační orgány) přímo příslušný dozorový úřad (v případě České republiky je to Úřad pro ochranu osobních údajů) nebo subjekty pro vydávání osvědčení (certifikační orgány) akredituje vnitrostátní akreditační orgán, kterým je Český institut pro akreditaci (v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008 a v souladu s normou ČSN EN ISO/IEC 17065 a požadavky stanovenými příslušným dozorovým úřadem) a konečně i kombinací obou postupů. Úřad pro ochranu osobních údajů vybral jako nejvhodnější variantu akreditaci subjektů pro vydávání osvědčení (certifikačních orgánů) prováděné Českým institutem pro akreditaci, o.p.s. (dále též ČIA), a to z důvodů jeho dlouholeté praxe s procesy akreditace, zárukou nezávislosti a možnosti celoevropského uznávání takto vydaných osvědčení. Pro uplatnění postupů akreditace je nutno vydat kritéria (viz čl. 42 odst. 5) schválená příslušným dozorovým úřadem. Obsah tohoto dokumentu představuje taková kritéria vycházející z požadavků stanovených nařízením.

2. Definice a pojmy

Žadatelem o vydání osvědčení (klientem certifikace) – subjekty/správci využívající hodnocené produkty ke zpracování osobních údajů nebo dodavatelé nabízející

hodnocené produkty, jejichž využitím dochází nebo může docházet ke zpracování osobních údajů.

Subjektem pro vydávání osvědčení (subjektem pro posuzování shody, certifikačním orgánem) – subjekt akreditovaný ČIA nebo vnitrostátním akreditačním orgánem jiného státu Evropské unie určeným v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008, který provádí hodnocení dle těchto kritérií a na jeho základě vydává osvědčení o ochraně údajů (certifikát).

Hodnocením – činnost subjektu pro vydávání osvědčení (certifikačního orgánu) spočívající v posouzení, zda je v daném případě zajištěna shoda hodnoceného produktu s požadavky stanovenými Obecným nařízením o ochraně osobních údajů Evropského parlamentu a Rady (EU) 2016/679. Součástí hodnocení je posouzení, zda žadatel (klient) s přihlédnutím ke stavu techniky, nákladům na provedení, povaze rozsahu, kontextu a účelům u hodnoceného produktu analyzoval rizika hrozící právům a svobodám fyzických osob v souvislosti se zpracováním jejich osobních údajů a zavedl přiměřená technická opatření k jejich omezení.

Produktem – programy (software), výpočetní technika (hardware) a služby u výrobce nebo dodavatele, jednotlivá zpracování údajů nebo systémy řízení ochrany osobních údajů u správce nebo zpracovatele.

Kritérii hodnocení (certifikačními požadavky) – požadavky a kritéria obsažené v části 4. tohoto dokumentu, který představuje souhrn požadavků/kritérií pro zajištění ochrany osobních údajů tak, aby byl prokázán soulad s nařízením Evropského parlamentu a Rady (EU) 2016/679.

Osvědčením o ochraně údajů (certifikátem) – osvědčení (certifikát) vydávané subjekty pro vydávání osvědčení (certifikačními orgány) pro účely prokázání souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) v případě operací zpracování prováděných správci a zpracovateli.

Certifikačním schématem – certifikační systém vztahující se ke specifikovaným produktům, pro které platí stejné specifikované požadavky, specifická pravidla a postupy.
Poznámka: Certifikační schéma vychází z ČSN EN ISO/IEC 17067 - schéma 2 (programy, výrobky) nebo schématu 6 (zpracování osobních údajů, řízení ochrany osobních údajů u správce nebo zpracovatele a služby).

Subjektem údajů – fyzická osoba identifikovaná (pomocí identifikačních) nebo identifikovatelná (pomocí souboru jiných osobních údajů o ní vedených).

Identifikovatelnou fyzickou osobou – 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.

Osobním údajem – veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

Zpracováním – 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.

Správcem – 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.

Zpracovatelem – fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Zvláštní kategorií 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.

Souhlasem 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.

3. organizační řešení vydávání osvědčení (certifikátů)

3.1 vymezení rozsahu vydávání osvědčení (certifikátu)

3.1.1 hmotné produkty:

Název produktu/skupiny produktů	Certifikační schéma	Specifikace norem (normativních dokumentů)
Programové produkty /software (pro účely zpracování osobních údajů)	ČSN EN ISO 17067:2014, systém 2 Ve spojení s Kritéria KVO, verze 1.0	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, kapitola I. až V. Kritéria KVO, část 4.7.2, 4.6.5, 4.7.3.2 až 4.7.3.10, 4.7.4.3, 4.7.4.4
Výpočetní technika/ hardware (pro účely zpracování osobních údajů)	ČSN EN ISO 17067:2014, systém 2 Ve spojení s Kritéria KVO, verze 1.0	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, kapitola I. až V. Kritéria KVO, část 4.7.2, 4.7.3.2, 4.7.3.4, 4.7.3.5, 4.7.3.6, 4.7.3.8. 4.7.4.3, 4.7.4.4.

3.1.2 procesy a služby:

Název produktu/skupiny produktů	Certifikační schéma	Specifikace norem (normativních

		dokumentů)
Jednotlivá zpracování osobních údajů (proces) správce nebo zpracovatele	ČSN EN ISO 17067:2014, systém 6 Ve spojení s Kritéria KVO, verze 1.0	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, kapitola I. až V. Kritéria KVO, část 4
Systém řízení ochrany osobních údajů u správce nebo zpracovatele (zahrnuje více zpracování osobních údajů)	ČSN EN ISO 17067:2014, systém 6 Ve spojení s Kritéria KVO, verze 1.0	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, kapitola I. až V. Kritéria KVO, část 4
Služby	ČSN EN ISO 17067:2014, systém 6 Ve spojení s Kritéria KVO, verze 1.0	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, kapitola I. až V. Kritéria KVO, část 4.7

Poznámka: V případě, kdy správce a zpracovatel využívá programů (sw), výpočetní techniky (hw) a služeb s dříve vydaným osvědčením (certifikátem) to neznamená, že je u správce zajištěna/zaručena shoda s nařízením 2016/679, protože důležitou náležitostí je i nastavení parametrů příslušeného programu, výpočetní techniky nebo služby a dalších náležitostí přímo nesouvisejících s programy, výpočetní technikou a službami (například organizační opatření uplatněná u správce nebo zpracovatele, způsob předávání osobních údajů do zahraniční apod.).

3.2 Kritéria pro akreditaci orgánů vydávajících osvědčení (certifikačních orgánů)

3.2.2 Požadavky na orgány vydávající osvědčení (certifikační orgány) se řídí normou ČSN EN ISO/IEC 17065 Posuzování shody – požadavky na orgány certifikující produkty, procesy a služby.

3.2.3 Doplňující požadavky WP29
(budou převzaty z podkladů poskytnutých WP29)

3.2.4 Doplňující požadavky Úřadu pro ochranu osobních údajů:

a) orgán vydávající osvědčení (certifikační orgán) není v konkursním řízení,

b) orgány vydávající osvědčení (certifikační orgán) nemá splatné nedoplatky na pojistném na veřejné zdravotní pojištění, na pojistném na sociální zabezpečení, na příspěvku na státní politiku zaměstnanosti, nemá v evidenci daní zachyceny daňové nedoplatky,

c) orgán vydávající osvědčení (certifikační orgán) nebyl pravomocně odsouzen pro úmyslný trestný čin nebo nedbalostní trestný čin spáchaný v souvislosti s předmětem podnikání,

d) statutární zástupce orgánu vydávajícího osvědčení (certifikačního orgánu) nebyl pravomocně odsouzen pro úmyslný trestný čin nebo nedbalostní trestný čin spáchaný v souvislosti s předmětem podnikání,

e) kvalifikace pracovníků orgánu vydávajícího osvědčení (certifikačního orgánu):

- znalost právních předpisů v oblasti ochranu osobních údajů (nařízení 2016/679, zákon č 101/2000 Sb. o ochraně osobních údajů, vybrané normy, jejichž požadavky se správci mohou řídit při zpracování osobních údajů zejména ČSN ISO/IEC 27001 apod.),
- znalost problematiky zajištění bezpečnosti a ochrany osobních údajů (praxe v roli auditora nebo manažera informační bezpečnosti minimálně 5 let a doloženým provedením alespoň 10 plných auditů apod.).

f) pokud bude subjekt pro vydávání osvědčení akreditován vnitrostátním akreditačním orgánem jiného státu Evropské unie, budou jím vydávaná osvědčení platná v rozsahu kritérii hodnocení (certifikačních požadavků) vydaných dozorovým orgánem příslušného státu.

Poznámka:

1. *Ke zpracovávaným osobním údajům akreditačním orgánem v průběhu procesu akreditace, včetně případné kontroly (zda subjekt stále splňuje podmínky akreditace) lze konstatovat, že proces provádění akreditace je upraven nařízením Evropského parlamentu a Rady (ES) č. 765/2008 a Nařízení Evropského parlamentu a rady (EU) č. 2016/679, zákonem č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů apod. Pokud je tedy pro výkon činnosti (v předpisech uvedené) třeba zpracovávat nezbytné osobní údaje, potom se údaje zpracovávají bez souhlasu subjektů a akreditační orgán je v pozici správce. Zároveň subjekt údajů musí být o zpracování osobních údajů informován.*
2. *Ke zpracovávaným osobním údajům subjektem pro vydávání osvědčení (certifikačním orgánem) v průběhu vydávání osvědčení (certifikace) a případného dohledu (zda provádí certifikaci v souladu předpisy a závaznými postupy) nad certifikacemi prováděným akreditačním orgánem, lze konstatovat, že proces provádění vydávání osvědčení (certifikace) je upraven nařízením Evropského parlamentu a Rady (ES) č. 765/2008 a Nařízení Evropského parlamentu a rady (EU) č. 2016/679, zákonem č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů apod. Pokud je tedy pro výkon činnosti (v nařízení uvedeném) třeba zpracovávat nezbytné osobní údaje, potom se údaje zpracovávají bez souhlasu subjektů a subjekt pro vydávání osvědčení (certifikační orgán) je v pozici správce a akreditační orgán v pozici zpracovatele (pracuje s údaji získanými certifikačním orgánem pro ověření správnosti jím provedeného hodnocení). Zároveň subjekt údajů musí být o zpracování osobních údajů informován.*

3.3 **vydávání osvědčení (certifikátu)**

V průběhu hodnocení se provádí porovnání dokumentace hodnoceného produktu ve vztahu ke skutečným parametrům produktu, a to vše v porovnání s kritérii hodnocení (certifikačními požadavky) stanovenými tímto dokumentem. Hodnocení může být prováděno porovnáním dokumentace a testováním produktu na plnění kritérií hodnocení (certifikačními požadavky).

Dokument potvrzující shodu s nařízením 2016/679 se vydává formou osvědčení (certifikátu), obsahujícího výrok subjektů pro vydávání osvědčení (certifikačního orgánu). Vzhledem k tomu, že hodnoceným produktem mohou být programy (software), výrobky (hardware), služby, zpracování osobních údajů nebo řízení ochrany osobních údajů, nemusí být možné/relevantní u všech produktů (zejména hw, sw a služby) hodnotit splnění všech kritérií hodnocení (certifikačních požadavků).

Na osvědčení (certifikátu) bude uvedena identifikace subjektu, jehož se hodnocení týká, identifikace skupiny produktů, které se hodnocení týká (sw, hw, služba, zpracování osobních údajů nebo systém řízení ochrany osobních údajů), uvedení oboru platnosti certifikátu (ochrana osobních údajů dle nařízení 2016/679), identifikace (slovní popis) hodnoceného předmětu (včetně případné verze), vyjádření

k plnění kritérií hodnocení (certifikačních požadavků). Pokud všechny kritéria hodnocení (certifikační požadavky) hodnoceny nejsou, potom je uveden jejich seznam se zdůvodněním, proč nebylo jejich plnění hodnoceno. Dále je na osvědčení (certifikátu) uvedena doba platnosti osvědčení, datum vydání osvědčení a identifikace subjektu, který osvědčení vydal. Přílohou osvědčení je protokol hodnocení produktu.

Vydané osvědčení (certifikát) má platnost tři roky a v případě, že dojde ke změnám produktu, které znamenají odchylky od hodnoceného stavu, certifikát pozbývá platnosti, pokud není změna ohlášena orgánu pro vydávání osvědčení (certifikačními orgánu). Žadatelé (klienti certifikace) oznámí proběhlé změny produktů, na které mají vydáno osvědčení (certifikát), a to do 15 dní od provedení změny. Na základě oznámení provádí subjekt pro vydávání osvědčení (certifikační orgán) dozor. Dozor může spočívat v získání vzorku hodnoceného předmětu (sw nebo hw) a kontroly dodržování deklarovaných vlastností /parametrů, případně kontroly u správce nebo zpracovatele, zda jsou dodržovány popsané parametry (služby, zpracování osobních údajů, nastavení systému ochrany osobních údajů).

4. Kritéria hodnocení (certifikační požadavky)

Subjekt pro vydávání osvědčení (certifikační orgán) vydá osvědčení (certifikát) o ochraně údajů správci nebo zpracovateli, který prokáže soulad s následujícími kritérii hodnocení (certifikačními požadavky).
Správce musí být schopen dodržení kritérií dokumentovat (části, na které se vztahuje požadavek doložitelnosti v dokumentaci, jsou v textu označeny “*“).

4.1 Jsou dodrženy základní zásady zpracování v souladu s článkem 5 nařízení.

4.1.1 **Zpracování, kterých se zásady týkají:**
- všechna posuzovaná zpracování osobních údajů,

4.1.2 **Základní zásady:**

4.1.2.1 údaje jsou zpracovávány k definovaným a dokumentovaným účelům, které (*platí všechny odrážky*):
- jsou definovány a srozumitelné popsány,
- jsou zákonné (*nesmí se jednat o zpracování v rozporu s právními předpisy ČR nebo EU*),
- data jsou zpracovávána způsobem, který je slučitelný s definovanými účely,
- zpracování pro účely statistické, archivace ve veřejném zájmu a vědeckého či historického výzkumu se nepovažují za neslučitelné s původními účely,

4.1.2.2 údaje jsou zpracovávány jen v rozsahu nezbytném pro zajištění účelu (*platí všechny odrážky*)
- jsou shromažďovány pouze nezbytné údaje,
- údaje, u kterých pominul účel zpracování, jsou vymazány,

4.1.2.3 údaje jsou přesné a aktualizované (*platí všechny odrážky*)**,**
- jsou shromažďovány přesné údaje,
- údaje jsou udržovány v aktualizovaném stavu,
- nepřesné údaje jsou vymazány nebo opraveny,

4.1.2.4 údaje jsou uloženy pouze po dobu nezbytně nutnou pro zajištění účelu (*platí všechny odrážky*)
- údaje jsou uloženy po dobu nezbytnou,
- po uplynutí doby uchování jsou údaje vymazány,

- při zpracování výhradně pro účely statistické, archivace ve veřejném zájmu a vědeckého či historického výzkumu lze údaje uložit i po delší dobu.

4.1.2.5 údaje jsou zpracovávány způsobem, který zajistí jejich bezpečnost (podrobně viz část 4.7)

4.1.3 **odpovědnost - správce musí být schopen dodržení zásad doložit/dokumentovat**

4.2 Zpracování osobních údajů je v souladu s články 6 a 9 nařízení prováděno zákonným způsobem (*)

4.2.1 **Zpracování osobních údajů** (*platí alespoň jedna z následujících odrážek*)

- zpracování je nezbytné pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů,
- zpracování je nezbytné pro plnění smluvních vztahů, jejichž stranou je subjekt údajů,
- zpracování je nezbytné pro plnění právní povinnosti správce
  - stanovené právními předpisy EU nebo
  - stanovené právními předpisy České republiky,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
  - stanoveného právními předpisy EU nebo
  - stanoveného právními předpisy České republiky,
- zpracování je nezbytné pro zajištění oprávněných zájmů správce či třetí strany s vyloučením případů, kdy mají přednost zájmy nebo ochrana základních práv a svobod subjektů údajů, zejména pokud jde o dítě,
- subjekt údajů udělil souhlas se zpracováním osobních údajů pro jeden nebo více účelů,

4.2.2 **zpracování zvláštních kategorií osobních údajů** (*platí alespoň jedna z následujících odrážek v případě zpracování této kategorie osobních údajů*)

- zpracování je nezbytné pro plnění povinností a výkon zvláštních práv v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany
  - stanovených právními předpisy EU,
  - stanovených právními předpisy České republiky nebo
  - kolektivní dohodou podle práva České republiky (které stanoví se vhodné záruky týkající se základních práv a zájmů subjektů údajů),
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
  - v případě, kdy subjekt údajů není schopen (fyzicky nebo právně) udělit souhlas,
- zpracování je prováděno v rámci oprávněných činností nadace, sdružení nebo jiného neziskového subjektu, který sleduje politické, filozofické, náboženské nebo odborové cíle a
  - vztahuje se na současné nebo bývalé členy takového subjektu,
  - vztahuje se osoby, které s takovým subjektem udržují pravidelné styky související s jeho cíli nebo

    - údaje jsou zpřístupňovány mimo takový subjekt pouze se souhlasem subjektů údajů,
- zpracovávány jsou údaje zjevně zveřejněné subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo v rámci soudních pravomocí,
- zpracování je nezbytné z důvodu významného veřejného zájmu
    - stanoveného právními předpisy EU,
    - stanoveného právními předpisy České republiky,

  a které:
    - dodržuje podstatu práva na ochranu údajů,
    - poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,
- zpracování je nezbytné pro účely preventivního a pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní a sociální péče či léčby, řízení systémů a služeb zdravotní nebo sociální péče
    - stanovené právními předpisy EU,
    - stanovené právními předpisy České republiky,
    - podle smlouvy se zdravotnickým pracovníkem,
    - údaje jsou zpracovávány osobou
        - vázanou služebním tajemstvím,
        - s odpovědností podle právních předpisů EU nebo ČR,
        - podle pravidel stanovenými orgány ČR,
        - na níž se vztahuje povinnost mlčenlivosti,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví (*například ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění norem kvality a bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků*)
    - stanovené právními předpisy EU,
    - stanovené právními předpisy České republiky,

  a které:
    - poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu, statistické účely
    - stanovené právními předpisy EU,
    - stanovené právními předpisy České republiky,

  a které:
    - je přiměřené sledovanému cíli,
    - dodržuje podstatu práva na ochranu údajů,
    - poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.
- subjekt údajů udělil výslovný souhlas se zpracováním pro jeden nebo více účelů
    - s vyloučením případů, kdy právo Unie stanoví, že zákaz zpracování osobních údajů zvláštních kategorií nemůže být subjektem údajů zrušen,
    - s vyloučením případů, kdy právo ČR stanoví, že zákaz zpracování osobních údajů zvláštních kategorií nemůže být subjektem údajů zrušen,

4.3 Podmínky vyjádření souhlasu subjektu údajů v souladu s článkem 7 nařízení (*platí všechny následující náležitosti***)**

4.3.1 Zpracování, kterých se posouzení týkají:

- všechna posuzovaná zpracování osobních údajů,

4.3.2 souhlas je doložitelný
- po celou dobu zpracování osobních údajů,
- obsahuje vyjádření zákonného zástupce (*fakultativně u dětí do 16 let*),
  - vyjádření zákonného zástupce je přiměřeným způsobem ověřováno,
- souhlas subjektu údajů je výslovný (*fakultativně u zvláštních kategorií osobních údajů*),

4.3.3 souhlas je srozumitelný
- přehledný (*použití jasných a jednoduchých jazykových prostředků*),
- přístupný,
- informovaný (*minimální obsah informace*):
  - identifikace správce,
  - účel
  - popsán rozsah zpracování, na který je souhlas udělován,
  - poučení o možnosti souhlas odvolat,
  - informace o tom, že není dotčena zákonnost zpracování osobních údajů před odvoláním souhlasu,

4.3.4 souhlas je svobodný (*jiná plnění správce či zpracovatele či činnosti subjektu údajů nesmí být podmiňovány udělením souhlasu),*

4.3.5 souhlas je oddělený (*odlišitelný a oddělený od jiných dokumentů*),

4.3.6 souhlas je odvolatelný
- je zajištěna snadnost odvolání souhlasu.

4.4 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 nařízení

4.4.1 podmínky zpracování (*platí alespoň jedna z následujících odrážek v případě zpracování takových údajů*)
- zpracování je prováděno pod dozorem orgánu veřejné moci,
  - v případě souhrnného rejstříku trestů platí výlučně,
- zpracování je oprávněné podle právních předpisů EU, které poskytují vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektů údajů,
- zpracování je oprávněné podle právních předpisů ČR, které poskytují vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektů údajů.

4.5 Je zajištěna požadovaná informovanost subjektu údajů v souladu s články 12 až 14 nařízení (*):

4.5.1 Informace o zpracování osobních údajů získaných přímo od subjektu údajů je poskytována za definovaných podmínek

4.5.1.1 způsob podání informace (*platí všechny možnosti*)
- srozumitelný, transparentní a snadno přístupný způsob,
- přehledný způsob (za použití jasných a jednoduchých jazykových prostředků),
- forma (*u formy platí alespoň jedna z možností*)
  - písemně,
  - elektronicky,
  - jinými prokazatelnými prostředky,
  - ústně:
    - na požádání subjektu údajů
    - identita subjektu je prokázána jinými prostředky,

4.5.1.2 lhůty pro podání informace:
- nejpozději v okamžiku získání osobních údajů od subjektů údajů,

4.5.1.3 obsah podané informace:

- informace podávané vždy (*platí všechny možnosti*)
  - o správci
    - totožnost a kontaktní údaj správce,
    - totožnost a kontaktní údaj zástupce správce,
    - kontaktní údaj pověřence pro ochranu osobních údajů (*pokud existuje*),
  - o účelech zpracování,
  - o jiných účelech zpracování, než pro které byly osobní údaje shromážděny (*jen pokud správce hodlá osobní údaje pro jiné účely zpracovávat*),
  - o právním základu pro zpracování,
  - o oprávněných zájmech správce nebo třetí strany (*pokud je zpracování nezbytné pro zajištění oprávněných zájmů správce nebo třetí strany*),
  - o příjemcích nebo kategoriích příjemců,
  - předání do třetí země nebo mezinárodní organizaci
    - existenci či neexistenci rozhodnutí komise o odpovídající ochraně osobních údajů,
    - odkaz na vhodné záruky a prostředky získání kopie těchto údajů nebo o informace tom, kde byly údaje zpřístupněny v případech předávání
      - založeného na vhodných zárukách,
      - pomocí právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty;
      - pomocí standardních doložek přijatých Komisí;
      - pomocí standardních doložek přijatých dozorovým úřadem a schválených Komisí,
      - pomocí schváleného kodexu chování,
      - pomocí vydaného osvědčení.
      - pomocí závazných podnikových pravidel,
      - jiné předání, za podmínek:
        - jde o jednorázové předání,
        - jde o omezený počet subjektů,
        - předání je nezbytné pro účely závažných oprávněných zájmů správce (které nejsou převáženy zájmy, právy a svobodami subjektů údajů).

- Další podávané informace (*vždy pokud jsou informace nezbytné pro zajištění spravedlivého a transparentního zpracování*)
  - doba uchování nebo kritéria použitá pro určení doby uchování,
  - oprávněné zájmy správce nebo třetí strany v případě, že je zpracování nezbytné pro zajištění těchto zájmů,
  - informace o právech subjektu údajů
    - na přístup k informacím,
    - na opravu nebo výmaz údajů,
    - na omezení zpracování,
    - na námitku proti zpracování,
    - na přenositelnost zpracování,
    - na možnost podání stížnosti u dozorového úřadu,
    - na odvolání souhlasu (*pokud je zpracování založeno na udělení souhlasu subjektů údajů*)
  - požadavek k poskytnutí osobních údajů

- na základě právních předpisů,
- smluvní požadavek,
- požadavek je nutné uvést do smlouvy

a který je doplněn informací

- o povinnost poskytnout osobní údaje
- o důsledcích neposkytnutí údajů pro subjekt údajů.

▪ informace, že dochází k automatizovanému rozhodování nebo profilování při zpracování osobních údajů
- skutečnost, že dochází automatizovanému rozhodování nebo profilování,
- použitý postup automatizovanému rozhodování nebo profilování,
- význam zpracování pro subjekt údajů,
- důsledky zpracování pro subjekt údajů.

▪ informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
- může odmítnout žádosti vyhovět,
- uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
- dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.5.1.4 V případě společných správců jsou jednoznačným a srozumitelným způsobem vymezeny podíly na zajištění informovanosti subjektu údajů.

4.5.2 **Informace o zpracování osobních údajů, které nebyly získány přímo od subjektu údajů, je poskytována za definovaných podmínek:**

4.5.2.1 Nejsou použity výjimky z informační povinnosti v případech, kdy

- poskytnutí informací o zpracování vyžaduje nepřeměřené úsilí nebo není možné:
  ▪ jde o zpracování, kde by podání informace znemožnilo nebo výrazně ztížilo dosažení cílů zpracování,
  - správce přijímá vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů,
  ▪ pro účely archivace ve veřejném zájmu,
  - správce přijímá vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně záruk
    - že vhodná opatření jsou zajištěna,
    - že zpracování nelze provést způsobem neobsahujícím identifikaci subjektů údajů (anonymizace),
  ▪ pro vědecký a historický výzkum,
  - správce přijímá vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně záruk
    - že vhodná opatření jsou zajištěna,
    - že zpracování nelze provést způsobem neobsahujícím identifikaci subjektů údajů (anonymizace),
  ▪ pro statistické účely,
  - správce přijímá vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektů údajů, včetně záruk
    - že vhodná opatření jsou zajištěna,

        - že zpracování nelze provést způsobem neobsahujícím identifikaci subjektu údajů (anonymizace),
- je získávání a zpřístupnění údajů je upraveno právními předpisy EU nebo České republiky,
- osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovat služební tajemství upravenou právem EU nebo ČR, včetně zákonné povinnosti mlčenlivosti,
- subjekt údajů již informace o zpracování má,

4.5.2.2 Je dodržen způsob podání informace (*platí všechny možnosti*)

- srozumitelný, transparentní a snadno přístupný způsob,
- přehledný způsob (*za použití jasných a jednoduchých jazykových prostředků*),
- závazná forma (*u formy platí alespoň jedna z možností*)
    - písemně,
    - elektronicky,
    - jinými prokazatelnými prostředky,
    - ústně
        - na požádání subjektu údajů
        - identita subjektu prokázána jinými prostředky,

4.5.2.3 Jsou dodrženy lhůty pro podání informace:

- v přiměřené lhůtě (nejpozději do 1 měsíce) po získání osobních údajů,
- nejpozději při první komunikaci se subjektem údajů,
- nejpozději při první zpřístupnění osobních údajů jinému příjemci (pokud existuje)

4.5.2.4 Je dodržen obsah podané informace

- informace podávané vždy (*platí všechny možnosti*)
    - o správci
        - totožnost a kontaktní údaj správce,
        - totožnost a kontaktní údaj zástupce správce,
        - kontaktní údaj pověřence pro ochranu osobních údajů (*pokud existuje*),
    - o účelech zpracování,
    - o jiných účelech zpracování, než pro které byly osobní údaje shromážděny (*jen pokud správce hodlá osobní údaje pro jiné účely zpracovávat*),
    - o právním základu pro zpracování,
    - kategorii dotčených osobních údajů,
    - příjemce nebo kategorie příjemců osobních údajů,
        - předání třetí země nebo mezinárodní organizaci existenci či neexistenci rozhodnutí Komise o odpovídající ochraně osobních údajů,
        - odkaz na vhodné záruky a prostředky získání kopie těchto údajů nebo informace o tom, kde byly údaje zpřístupněny v případech předávání
            - založeného na vhodných zárukách,
            - pomocí právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty,
            - pomocí standardních doložek přijatých Komisí,
            - pomocí standardních doložek přijatých dozorovým úřadem a schválených Komisí,
            - pomocí schváleného kodexu chování,

- pomocí vydaného osvědčení,
- pomocí závazných podnikových pravidel,
- jiné předání, za podmínek:
  - jde o jednorázové předání,
  - jde o omezený počet subjektů,
  - předání je nezbytné pro účely závažných oprávněných zájmů správce (nejsou převáženy zájmy, právy a svobodami subjektů údajů).

- informace podávané v některých případech (*vždy pokud jsou informace nezbytné pro zajištění spravedlivého a transparentního zpracování*)
  - doba uchování nebo kritéria použitá pro určení doby uchování,
  - oprávněné zájmy třetí strany, pokud je zpracování nezbytné pro zajištění oprávněných zájmů správce nebo třetí strany,
  - informace o právech subjektů údajů
    - na přístup k informacím,
    - na opravu nebo výmaz údajů,
    - na omezení zpracování,
    - na námitku proti zpracování,
    - na přenositelnost zpracování,
    - na možnost podání stížnosti u dozorového orgánu,
    - na odvolání souhlasu (*pokud je zpracování založeno na udělení souhlasu subjektů údajů*),
  - zdroj osobních údajů, včetně informace o původu z veřejně dostupných zdrojů,
  - informace, že dochází k automatizovanému rozhodování nebo profilování při zpracování osobních údajů
    - skutečnost, že dochází automatizovanému rozhodování nebo profilování,
    - použitý postup automatizovanému rozhodování nebo profilování,
    - význam zpracování pro subjekt údajů,
    - důsledky zpracování pro subjekt údajů.
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.5.2.5 V případě společných správců jsou jednoznačným a srozumitelným způsobem vymezeny podíly na zajištění informovanosti,

4.6 Jsou zajištěna práva subjektu údajů v souladu s články 15 až 21 nařízení:

4.6.1 Právo subjektu údajů na přístup k osobním údajům (*)

4.6.1.1 Definice zpracování, kterých se právo na přístup týká
- všechna zpracování osobních údajů,

4.6.1.2 Požadavky (*platí všechny možnosti*)
- je zajištěn přístup subjektu údajů k informacím o zpracování osobních údajů a k osobním údajům:
  - o účelech zpracování,
  - o kategoriích osobních údajů,
  - o příjemcích nebo kategoriích příjemců i ve třetích zemích,

- o době uchování, nebo kritériích, podle nichž bude doba stanovena,
- o právech subjektů údajů:
  - na opravu údajů
  - na výmaz údajů,
  - na omezení zpracování,
  - na námitku proti zpracování,
  - na podání stížnosti u dozorového úřadu,
- veškeré dostupné informace o zdroji údajů, pokud jím není přímo subjekt údajů,
- že dochází k automatizovanému rozhodování, včetně profilování při zpracování osobních údajů:
  - postup zpracování,
  - význam zpracování,
  - důsledky zpracování,
- v případě předání do třetích zemí nebo mezinárodní organizaci o vhodných zárukách, které se vztahují k předání,

- správce vydává potvrzení subjektu údajů, že osobní údaje o něm jsou/nejsou zpracovávány,
- je zajištěn přístup subjektu údajů k jeho osobním údajům,
- údaje jsou poskytovány subjektu údajů:
  - tak, že nedochází k dotčení práva svobod jiných osob,
  - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
      - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
  - pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,
  - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě.
  - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového orgánu a žádat soudní ochranu,
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - může požadaovat přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.2 **Právo subjektu údajů na opravu osobních údajů a doplnění neúplných osobních údajů (*):**

4.6.2.1 Definice zpracování, kterých se právo týká

- všechna hodnocená zpracování osobních údajů,

4.6.2.2 Požadavky

- správce přijímá žádosti subjektu údaje o opravu nepřesných údajů,

- správce opravuje bez zbytečného odkladu nepřesné osobní údaje,
- správce přijímá žádosti subjektu údaje o doplnění neúplných údajů (i dodatečným prohlášením),
- správce doplňuje bez zbytečného odkladu neúplné údaje,
- správce oznamuje jednotlivým příjemcům údajů veškeré opravy osobních údajů s výjimkou případů,
    - kdy se to ukáže jako nemožné,
    - kdy to vyžaduje nepřeměřené úsilí,
- v případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemců zaslal oznámení o opravách osobních údajů,
- údaje jsou poskytovány subjektu údajů:
    - pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,
    - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
        - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
        - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
    - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě.
    - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
        - o důvodech nepřijetí žádosti,
        - o možnosti podat stížnost u dozorového úřadu a žádat soudní ochranu,
    - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
        - může odmítnout žádosti vyhovět,
        - uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
        - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.3 Právo subjektu údajů na výmaz osobních údajů (právo být zapomenut) (*):

4.6.3.1 Definice případů, kterých se právo týká

- zpracování, u kterých pominul účel zpracování osobních údajů,
- zpracování, kde subjekt údajů odvolal souhlas se zpracováním osobních údajů,
- zpracování (včetně profilování), kde subjekt údajů vznesl námitky proti zpracování osobních údajů a oprávněné důvody zpracování nepřevažují nad právy a svobodami subjektů údajů, pro:
    - plnění úkolů ve veřejném zájmu,
    - plnění úkolů při výkonu veřejné moci,
    - pro účely oprávněných zájmů příslušného správce či třetí strany,
- subjekt údajů vznesl námitky proti zpracování osobních údajů
    - pro účely přímého marketingu (včetně profilování),
- osobní údaje jsou zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění povinnosti na základě požadavků práva (EU nebo ČR),

- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti,

4.6.3.2 Výjimky, kdy se právo na výmez osobních údajů neuplatní:

- zpracování je nezbytné pro výkon práva na svobodu projevu a informace,
- zpracování je nezbytné pro splnění právní povinnosti (vyžadované právem EU nebo ČR),
- zpracování je nezbytné pro plnění úkolů ve veřejném zájmu
- zpracování je nezbytné pro plnění úkolů při výkonu veřejné moci,
- zpracování je nezbytné pro určení, výkon a obhajobu právních nároků.
- zpracování je nezbytné ve veřejném zájmu v oblasti veřejného zdraví:
  - pro účely preventivního a pracovního lékařství,
  - pro posouzení pracovní schopnosti zaměstnance,
  - pro účely lékařské diagnostiky,

  a na základě práva EU nebo ČR nebo podle smlouvy se zdravotnickým pracovníkem, též
  - pro poskytování zdravotní péče,
  - pro poskytování sociální péče,
  - pro řízení systémů a služeb zdravotní péče,
  - pro řízení systémů a služeb sociální péče,
- že zpracování je nezbytné na základě práva EU nebo ČR a z důvodů veřejného zájmu v oblasti veřejného zdraví:
  - při ochraně před vážnými přeshraničními zdravotními hrozbami,
  - při zajištění norem kvality a bezpečnosti zdravotní péče, při zajištění norem kvality a bezpečnosti léčivých přípravků
  - při zajištění norem kvality a bezpečnosti zdravotnických prostředků,
  - údaje mohou být zpracovávány také
    - pracovníkem, na něhož se vztahuje povinnost mlčelivosti:
      - na základě služebního tajemství podle práva EU nebo ČR,
      - na vlastní odpovědnost podle práva EU nebo ČR,
      - na základě pravidel stanovaných vnitrostátními orgány,
      - na základě pravidel stanovených jinou osobou,
    - jinou osobou, na niž se vztahuje povinnost mlčelivosti:
      - podle práva EU nebo ČR
      - podle pravidel stanovených příslušnými vnitrostátními orgány,
- zpracování je nezbytné pro účely vědeckého a historického výzkumu, pro statistické účely, pokud:
  - není možné, aby účely byly splněny zpracováním, které neumožňuje identifikovat subjekty údajů,
  - je pravděpodobné, že by výmaz osobních údajů znemožnil nebo vážně ohrozil splnění cílů uvedeného zpracování,
  - jsou zavedena technická a organizační opatření
    - k zajištění vhodných záruk za práva svobod subjektů údajů,
    - k zajištění minimalizace zpracovávaných údajů.

4.6.3.3 Požadavky:

- správce přijímá žádosti o výmaz osobních údajů od subjektu údajů,
- správce vymaže osobní údaje, pokud zpracování nepodléhá výjimce dle bodu 4.6.3.2,
- pokud údaje byly zveřejněny, přijímá správce (s ohledem na dostupnou technologii a náklady) přiměřené kroky, aby informoval správce, kteří údaje také zpracovávají, že je subjekt údajů žádá, aby vymazaly
  - veškeré kopie,
  - replikace,
  - odkazy na tyto údaje,
  - došlo k informování správců, které osobní údaje zpracovávají, že subjekt údajů žádá výmaz údajů (odkazy, kopie, replikace),
- správce příjemcům údajů oznamuje výmaz osobních údajů, s výjimkou případů
  - kdy se to ukáže jako nemožné,
  - kdy to vyžaduje nepřeměřené úsilí,
- v případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemců zaslal oznámení o výmazu osobních údajů,

- údaje jsou poskytovány subjektu údajů:
  - pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,
  - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
    - o každém prodloužení lhůty je subjekt údajů informován včetně důvodů prodloužení,
  - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě,
  - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového orgánu a žádat soudní ochranu,
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.4 **Právo subjektu údajů na omezení zpracování osobních údajů (*):**

4.6.4.1 Definice případů, kterých se právo týká:
- subjekt popírá přesnost osobních údajů,
- zpracování je protiprávní, ale subjekt údajů žádá pouze omezení jejich použití (na místo výmazu údajů),
- pominul-li účel zpracování, ale subjekt (údajů) osobní údaje požaduje pro určení, výkon nebo obhajobu právních nároků,
- subjekt údajů vznesl námitku proti zpracování osobních údajů.

4.6.4.2 Výjimky

- pokud subjekt údajů požádá o omezení zpracování osobních údajů, jeho údaje mohou být zpracovávány bez jeho souhlasu pouze z důvodu:
  - určení, výkonu a obhajoby právních nároků,
  - ochrany práv jiné fyzické nebo právnické osoby,
  - veřejného zájmu EU nebo jejího členského státu,

4.6.4.3 Požadavky:

- správce přijímá žádost subjektu údajů o omezení zpracování jeho osobních údajů,
- správce omezí zpracování osobních údajů, pokud zpracování nepodléhá výjimce dle bodu 4.6.4.2,
- pokud došlo k omezení zpracování údajů, osobní údaje mohou být zpracovávány pouze se souhlasem subjektu údajů, s výjimkou
  - uložení osobních údajů,
- správce oznamuje jednotlivým příjemcům osobních údajů omezení zpracování osobních údajů s výjimkou případů:
  - kdy se to ukáže jako nemožné,
  - kdy to vyžaduje nepřeměřené úsilí,
- v případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemcům zaslal oznámení o omezení zpracování osobních údajů,
- správce musí ověřit přesnost osobních údajů v případě, že ji subjekt popírá,
- pokud dochází ke zrušení omezení zpracování, musí na to být upozorněn subjekt údajů (který dosáhl omezení),
- údaje jsou poskytovány subjektu údajů:
  - v případě pochybností o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,
  - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
    - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
  - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě,
  - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového úřadu a žádat soudní ochranu,
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - může požadovat přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.5 Právo na přenositelnost údajů (*):

4.6.5.1 Definice zpracování, kterých se povinnost týká:

- automatizovaně prováděná zpracování,
- zpracování osobních údajů, která jsou založena na souhlasu subjektu údajů,
- zpracování zvláštních kategorií osobních údajů, která jsou založena na výslovném souhlasu subjektu údajů,
- zpracování je nezbytné pro plnění smlouvy se subjektem údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů,

4.6.5.2 Výjimky z uplatnění práva:
- zpracování, kterými je správce pověřen a která jsou nezbytná pro plnění úkolů ve veřejném zájmu,
- zpracování, kterými je správce pověřen a která jsou nezbytná při výkonu veřejné moci,
- zpracování zvláštních kategorií osobních údajů, kde se právo na přenositelnost osobních údajů neuplatní, protože právo EU nebo ČR stanoví, že výslovný souhlas subjektů údajů nelze uplatnit.

4.6.5.3 Požadavky na zajištění práva na přenositelnost údajů:
- správce přijímá žádost subjektu údajů o zajištění o přenositelnosti jeho údajů,
- správce zajistí přenositelnost osobních údajů, pokud zpracování nepodléhá výjimce dle bodu 4.6.5.2,
- osobní údaje poskytuje jeden správce přímo druhému správci
  - pokud to je technicky proveditelné,
- správce osobní údaje subjektů údajů poskytuje a/nebo přijímá v požadovaném formátu, který je:
  - strukturovaný,
  - strojově čitelný,
  - běžný,
- uplatněním práva není dotčeno právo na výmaz údajů,
- uplatněním práva nejsou nepříznivě dotčena práva a svobody jiných subjektů.
- údaje jsou poskytovány subjektu údajů:
  - pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,
  - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
    - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
  - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě.
  - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového úřadu a žádat soudní ochranu,
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,

- uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
- dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.6 Právo subjektů údajů vznést námitku proti zpracování osobních údajů, které se jej týkají (*):

4.6.6.1 Definice zpracování, kterých se povinnost týká:
- zpracování nezbytné pro plnění úkolů ve veřejném zájmu (včetně profilování) (*Poznámka - definováno právním předpisem*),
- zpracování nezbytné při výkonu veřejné moci (včetně profilování) (*Poznámka - definováno právním předpisem*),
- zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany (včetně profilování)
- zpracování pro účely přímého marketingu (včetně profilování),
- zpracovávání pro účely vědeckého či historického výzkumu nebo pro statistické účely,

4.6.6.2 Výjimky z uplatnění práva:
- zpracování pro účely oprávněných zájmů příslušného správce či třetí strany (včetně profilování), kdy mají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů (zejména pokud je subjektem údajů dítě),
- zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely, kdy je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.

4.6.6.3 Požadavky na zajištění práva na vznesení námitky proti zpracování osobních údajů, které se ho týkají:
- je zajištěno, že subjekt údajů je na právo vznést námitku upozorněn:
  - výslovně a zřetelně,
  - odděleně od jakýchkoli jiných informací,
  - nejpozději v okamžiku první komunikace se správcem,
- správce přijímá dokumenty o vznesení námitky subjektu údajů proti zpracování jeho osobních údajů,
- správce vyřizuje námitky a o způsobu vyřízení informuje subjekt údajů,
- správce informuje subjekt údajů o tom, že zpracování podléhá výjimce dle bodu 5.6.6.2,
- je zajištěno, v případě využívání služeb informační společnosti, že subjekt údajů může uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací,
- správce může ve zpracování osobních údajů pokračovat, a to přes podání námitky, pokud má závažné oprávněné důvody, které prokazují, že:
  - důvody zpracování převažují nad zájmy nebo právy a svobodami subjektu údajů,
  - zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků,
- V případě vznesení námitky proti zpracování osobních údajů pro účely přímého marketingu správce údaje již dále nezpracovává,
- údaje jsou poskytovány subjektu údajů:
  - pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů,

- bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
    - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
- pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě.
- pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového úřadu a žádat soudní ochranu,
- informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.6.7 Právo subjektu údajů nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování (*):

4.6.7.1 Definice zpracování, kterých se toto právo týká:
- všechna zpracování, kde je rozhodnutí založeno výhradně na automatizovaném zpracování osobních údajů, které má právní účinky nebo se subjektu údajů obdobným způsobem dotýká.

4.6.7.2 Výjimky z uplatnění práva:
- případy, kde je rozhodnutí nezbytné k uzavření nebo plnění smlouvy se subjektem údajů,
- případy, kde je rozhodnutí povoleno právem EU nebo ČR (včetně právem stanovených opatření zajišťujících ochranu práv a svobod),
- případy, kdy je rozhodnutí založeno na výslovném souhlasu subjektu údajů.

4.6.7.3 Požadavky na zajištění práva:
- subjekt údajů má právo nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování (včetně profilování), které má právní účinky nebo se subjektu údajů obdobným způsobem dotýká,
- správce přijímá žádosti subjektu údajů nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování,
- správce na žádost subjektu údajů ukončí provádění rozhodování založeného výhradně na automatizovaném zpracování, pokud rozhodování nepodléhá výjimce dle bodu 4.6.7.2,
- v případech, kdy:
    - je rozhodnutí nezbytné k uzavření nebo plnění smlouvy se subjektem údajů,
    - je rozhodnutí založeno na výslovném souhlasu subjektu údajů.

  správce musí provést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektů údajů minimálně v rozsahu:
    - práva na lidský zásah ze strany správce,
    - práva vyjádřit svůj názor,

- práva napadnout rozhodnutí.

- v případech, kdy jsou zpracovávány zvláštní kategorie osobních údajů, a zároveň
  - je rozhodnutí nezbytné k uzavření nebo plnění smlouvy se subjektem údajů,
  - nebo je rozhodnutí povoleno právem EU nebo ČR (včetně právem stanovených opatření zajišťujících ochranu práv a svobod),
  - nebo je rozhodnutí založeno na výslovném souhlasu subjektu údajů,

  musí jít o zpracování,
  - kde jsou zavedena vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů a zároveň je zpracování:
    - nezbytné z důvodu veřejného zájmu na základě práva EU nebo ČR, který je:
      - přiměřený sledovanému cíli,
      - dodržuje podstatu práva na ochranu osobních údajů,
      - poskytuje vhodné a konkrétní záruky pro ochranu lidských práv a zájmů subjektu údajů,
    - nebo založené na výslovném souhlasu subjektu údajů,
      - netýká se případů, kdy právo EU nebo ČR stanoví, že výslovný souhlas nelze uplatnit.

- údaje jsou poskytovány subjektu údajů:
  - bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti,
    - s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce,
    - o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení,
  - pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě,
  - pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů:
    - o důvodech nepřijetí žádosti,
    - o možnosti podat stížnost u dozorového úřadu a žádat soudní ochranu,
  - informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce:
    - může odmítnout žádosti vyhovět,
    - uložit přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace,
    - dokládá nedůvodnost nebo nepřiměřenost žádosti.

4.7 Je zajištěno řízení bezpečnosti osobních údajů v souladu s články 24, 25 a 32 nařízení (*)

4.7.1 **Údaje jsou zpracovávány způsobem, který zajistí jejich náležité zabezpečení před**:
- neoprávněným a protiprávním zpracováním
- náhodnou ztrátou,

- zničením,
- poškozením.

Varianta 1

– požadavky jsou dány normou ČSN ISO/IEC 27001 Informační technologie – bezpečnostní techniky-Systém řízení bezpečnosti informací – Požadavky. Jejich splnění je možno prokázat certifikátem vydaným akreditovaným certifikačním orgánem na tuto technickou normu.
Akreditovaným orgán, který akreditoval certifikační orgán musí být signatářem EA MLA a IAF MLA.
Týká se zpracování osobních údajů nebo systému ochrany informací u správce.

Varianta 2

4.7.2 Posouzení bezpečnosti provedené správce nebo zpracovatelem nebo dodavatelem:
- byla provedena analýza a posouzení působení hrozeb na zpracování osobních údajů
- byl navržen soubor (technických a organizačních) opatření uplatněný,
  - při vyvíjení produktu,
  - při využívání produktu,
- účinnost přijatých je opatření pravidelně testována a vyhodnocována.

4.7.3 Soubor technických a organizačních opatření:

4.7.3.1 k řízení fyzického přístupu do prostor, kde probíhá zpracování osobních údajů, kde jsou umístěna aktivní zařízení, včetně paměťových nebo přenosných zařízení:
- opatření jsou zdokumentována a odpovídají skutečnému stavu,
- jsou definovány nezbytné zóny/perimetry/prostory přístupu,
- přístup do různých zón/perimetrů/prostor je řízen (zabezpečení – zámky, mříže, poplachové zabezpečovací systémy, čipové karty, hw klíče apod.),
- jsou zpracovány postupy nebo instrukce pro osoby vstupující do různých zón/perimetrů/prostor,
- přístup do různých zón/perimetrů/prostor je sledován a zaznamenáván (kamery, logy),
- funkčnost opatření pro řízení přístupu do různých zón/perimetrů/prostor je pravidelně kontrolována.

4.7.3.2 k řízení logického přístupu k osobním údajům (včetně datových nosičů),
- je implementován dostatečně škálovatelný přístup k údajům/ souborům/adresářům/aplikacím na základě rolí, přístupových práv, typu údajů a hesel,
- existuje proces správy přístupu k datům:
  - přidělování a odebírání přístupových práv,
  - přezkoumávání přidělených přístupových práv,
  - je zajištěna neslučitelnost souběžného přidělení některých rolí jediné osobě,
  - omezení a používání privilegovaných rolí,
  - jsou k dispozici informace o osobě a čase udělení, změně nebo odnětí přístupových práv a rolí (včetně historie) a tento záznam je tvořen automaticky,
  - soupis vydaných přístupových práv je snadno přístupný oprávněným zaměstnancům,
  - tvorba přístupových práv je popsána, zdokumentována a jasně vysvětlena pro každého oprávněného uživatele,

- pravidla pro správu přístupových práv jsou definována, nastavena a dokumentována,
- přístup k údajům je sledován a zaznamenáván,
- funkčnost opatření pro řízení přístupu je pravidelně kontrolována.

4.7.3.3 k zajištění čitelnosti osobních údajů oprávněnými osobami:

- jsou zpracovány postupy nebo instrukce k zajištění čitelnosti osobních údajů jen oprávněnými osobami,
  - zajištění nečitelnosti
    - použití přiměřeného šifrování, hashování,
    - správa klíčů,
    - existence mechanizmů vynucujících/ověřujících použití šifrování, hashování,
  - zajištění neidentifikovatelnosti
    - pseudonymizace,
    - oddělná správa pseudonymů,
  - dodržování pravidla čistého stolu,
  - existence a dodržování pravidel pro práci s výpočetní technikou (počítače, tiskárny, skenery, mobily apod.).

4.7.3.4 logování a monitorování

- existují opatření, které brání uživatelům manipulovat s daty, která jsou testována,
  - existují opatření pro ověření přístupu uživatele a jsou testována,
  - přístup je monitorován a protokolován,
    - je uplatněno on-line monitorování a sledování,
    - je uplatňováno protokolování činnosti všech uživatelů,
    - protokolování je škálovatelné (dle činnosti, obsahu a doby uchování logu),
    - log je zabezpečen (včetně přístupu),
    - vytváření logů nemůže být blokováno,
    - jsou nasazeny nástroje pro snadnou analýzu logů,
    - zavedení a konfigurace přístupových práv k logování je prováděno oprávněnou osobou (mimo uživatele logu),
    - údaje protokolu jsou bezpečně zničeny po uplynutí doby uchování.

4.7.3.5 použití identifikace a autentizace:

- jsou vytvořena přiměřená opatření pro identifikaci a ověřování identity uživatelů,
- je zabráněno opakovaným pokusům o identifikaci a autentizaci po vykonání definovaného počtu neúspěšných pokusů,
- jsou aplikována opatření pro předcházení případnému útoku (např. dočasná deaktivace uživatelských účtů),
- nástroje používané pro autentizaci (například klíče, čipové karty, bezpečnostní tokeny apod.) jsou v zásobě pro vydávání novým uživatelům,
- prostředky určené pro identifikaci a autentizaci jsou zabezpečeny (např. proti klonování a neoprávněnému přístupu),
- jsou zpracovány postupy nebo instrukce pro identifikaci a autentizaci.

4.7.3.6 použití hesel

- existují postupy zajišťující správnost přiřazení hesel uživatelům, jejich důvěrnost (ochrana před kompromitováním/prozrazením) a integritu,
- uživatelé mohou snadno změnit hesla,
- existuje periodické vynucení změny hesla a tvorbu odpovídajících hesel (délka, složitost)

- jsou zpracovány postupy nebo instrukce pro správu a použití hesel (např. zapomenutí hesla uživatelem),

4.7.3.7 komunikační prostředí

- jsou implementovány opatření na řízení, správu, kontrolu a zabezpečení provozu sítě,
  - při odběru síťových služeb jsou definovány bezpečnostní opatření, úroveň a další parametry poskytovaných služeb,
  - zabezpečení vzdáleného přístupu je srovnatelné s interním přístupem (např. šifrování, VPN, obousměrný ověřování, dvoufaktorová autentizace),
    - přenosy veřejnými sítěmi jsou vhodným způsobem chráněny (např. šifrovány),
    - při přenosu dat mezi vnitřní sítí a vnější sítí, je vnitřní síť chráněna a oddělena (firewally, DMZ apod.).
  - je zabezpečen přenos údajů o přihlášení (jméno/ heslo),
  - přenos obsahu webovými službami je zajišťován pouze v nezbytných případech (zejména pro online bankovnictví, webových e-mailových rozhraní atd.),

4.7.3.8 zajištění funkčnosti

- zařízení musí být umístěna tak, aby byla chráněna a udržována ve stavu dostupnosti a integrity,
- existují opatření na zajištění napájení před výpadkem energetických sítí,
- existují opatření na zajištění datových přenosů před výpadkem, rušením nebo poškozením,
- existují opatření na zajištění ochrany údajů proti ohni, vodě, silným elektromagnetickým polím apod.,
- existují opatření na ochranu proti škodlivým kódům,
- je prováděna synchronizace hodin všech systémů,
- existují pravidla pro práci s mobilními zařízeními.

4.7.3.9 zálohování

- existuje zálohovací mechanizmus (automatizovaný),
- parametry zálohování možno konfigurovat dle potřeb/požadavků (rozsah, termíny),
- záložní kopie dat je zabezpečena proti neoprávněnému přístupu a čtení (řízení přístupu, šifrování, pseudonymizace),
- záložní kopie dat jsou testovány (úplnost, správnost, čitelnost),
- záložní kopie lze bezpečně vymazat,
- jsou zpracovány postupy nebo instrukce pro zálohování dat,

4.7.3.10 archivace

- je oddělena archivace a zálohování dat,
- archivní data jsou popsána a katalogizována,
- jsou zpracovány postupy nebo instrukce pro archivaci dat,
- je možno provádět archivaci na různá místa (záložní infrastruktura, cloud, externí média),
- archivní data jsou zabezpečena proti neoprávněnému přístupu a čtení,
- archivní data jsou zabezpečena pro případ mimořádných událostí (protipožárních trezory, v různých budovách nebo místech),
- je prováděno testování čitelnosti archivovaných dat v pravidelných intervalech,

4.7.3.11 kontinuita činnosti /obnova po mimořádné situaci

- jsou definovány požadavky/koncepce na zjištění kontinuity činnosti /obnově po mimořádné situaci,

- jsou popsány a zdokumentovány procesy a postupy (plán) zajišťující kontinuitu činnosti /obnovu po mimořádné situaci,
  - automatizované přepnutí na záložní infrastrukturu,
  - obnova dat ze zálohy,
- procesy a postupy zajišťující kontinuitu činnosti/obnovu po mimořádné situaci jsou pravidelně testovány,

4.7.3.12 likvidace dat a datových nosičů

- všechna data jsou po pominutí účelu zpracování osobních údajů bezpečně vymazána (včetně záloh a archivu, pokud to nevylučuje právní předpis),
- všechna zařízení obsahující paměťová média musí být před likvidací nebo dalším použitím zkontrolována, zda byla data a programy bezpečně odstraněny nebo přepsány,
- všechna údaje vytištěné a zapsané na papírových kopiích musí být bezpečně zlikvidovány,

4.7.3.13 personální opatření

- pravidla prověřování zaměstnance,
- pravidla proškolování zaměstnance,
- pravidla pro zajištění odpovědnost zaměstnance v době zaměstnání i po jeho ukončení,
- pravidla pro vedení disciplinárního řízení,

4.7.4 pro doložitelnost činnosti správce se zpracovává následující dokumentace

4.7.4.1 bezpečnostní politika

- je zpracována bezpečnostní politika,
- bezpečnostní politika je prosazována a pravidelně kontrolována vedením,
- bezpečnostní politika je přezkoumávána v pravidelných intervalech nebo v případě změn produktu upravována,

4.7.4.2 analýza rizik:

- byla provedena analýza a posouzení působení hrozeb na zpracování osobních údajů,
- byl navržen soubor (technických a organizačních) opatření, který zabraňuje působení hrozeb nebo alespoň zajišťuje omezení působení (na přijatelnou úroveň) hrozeb na zpracování osobních údajů, a to s ohledem na:
  - povahu zpracování,
  - rozsah zpracování,
  - účely zpracování,
  - souvislostem (kontextu) zpracování,
  - hrozícím rizikům pro práva a svobody fyzických osob,
  - stavu techniky,
  - nákladům na provedení,
- přijatá opatření zajišťují integritu, důvěrnost a dostupnosti osobních údajů na přiměřené úrovni,
- účinnost přijatých je opatření pravidelně testována, vyhodnocována a upravována,

4.7.4.3 dokumentace opatření na ochranu dat:

- dokumentace produktů (i pořizovaných) poskytuje informace o zabezpečení a přehled o opatřeních na ochranu údajů (včetně jejich možné škálovatelnosti),
- evidence historie produktu (verze, autoři, přejímání atd.),
- dokumentace a zpřístupnění návodů a pokynů pro uživatele,
- evidence zajištění informovanosti uživatelů,

4.7.4.4 dokumentace vývoje produktu:

- pravidla pro vývoj,
- dokumentace produktů,
- dokumentace změn,
- dokumentace testování a přejímání/akceptace produktu,

4.7.4.5 inventarizace hardware, software, služeb, data a média:
- vytvoření evidence,
- evidence dokumentace a popisů,
- zajištění ochrany duševního vlastnictví,

4.7.4.6 media (CD, DVD, kazety, diskety a USB paměti apod.).
- identifikace druhu média,
- identifikaci druhu informací obsažených na médiích,
- katalogizace medií,
- skladování v místě s řízeným přístupem,
- přístup má pověřená osoba,
- je evidován přístup a zaslání,

4.7.5 ověření přijatých technických a organizačních opatření:
- podpisem schváleného kodexu činnosti,
- vydaným osvědčením,
- jinak,

4.8 Jsou zajištěny podmínky pro zpracování osobních údajů správcem nebo zpracovatelem se sídlem mimo EU v souladu s článkem 27 nařízení (*)

4.8.1 Definice zpracování, kterých se povinnost týká:
- nabídky služeb nebo zboží subjektu údajů v EU,
- monitorování chováním subjektu údajů v rámci EU.

4.8.1.1 Výjimky:
- zpracování je příležitostné,
- zpracování nezahrnuje ve velkém měřítku zpracování osobních údajů zvláštních kategorií,
- zpracování nezahrnuje ve velkém měřítku zpracování osobních údajů týkajících se rozsudků ve věcech trestních a trestných činů,
- je nepravděpodobné, že zpracování představuje riziko pro práva a svobody fyzických osob.

4.8.2 Povinnosti:

4.8.2.1 správce sídlící mimo EU jmenoval písemně svého zástupce v ČR (nebo členském státě EU).

4.9 Správce provádí zpracování prostřednictvím zpracovatele za požadovaných podmínek v souladu s články 28 a 29 nařízení (*):

4.9.1 Povinnosti správce, pokud zpracování provádí zpracovatel

4.9.1.1 Správce uzavírá se zpracovatelem smlouvu nebo se zpracování řídí jiným právním aktem podle práva EU nebo ČR, který stanoví:
- předmět zpracování,
- dobu zpracování,
- povahu zpracování,
- účel zpracování,
- typ osobních údajů,
- kategorii subjektů údajů,
- povinnosti a práva správce,
- závazky zpracovatele, které zpracovává osobní údaje
  - zpracovává osobní údaje pouze na základě pokynu správce,
  - informuje správce o předávání do zahraničí, včetně povinnosti předávat na základě požadavků práva EU nebo členského státu (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 členských států 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.

4.10 Správce nebo zpracovatel provádí v souladu s článkem 30 nařízení záznamy o činnostech zpracování (*):

4.10.1 Definice správců nebo zpracovatelů, kterých se povinnost týká

- zaměstnává více jak 250 osob,
- zpracování představuje riziko pro práva a svobody subjektů údajů,
- zpracování není příležitostné,
- zpracování zahrnuje zvláštní kategorie osobních údajů,
- zpracování zahrnuje údaje týkající se rozsudků ve věcech trestních a trestných činů.

4.10.2 Povinnost subjektů

4.10.2.1 správce

- záznamy o činnostech zpracování vede v písemné podobě (i elektronicky)
- záznamy o činnostech obsahují
  - jméno a kontaktní údaje správce, společného správce, zástupce správce a pověřence pro ochranu osobních údajů
  - účel zpracování,
  - popis kategorií subjektů údajů a kategorií osobních údajů,
  - kategorie příjemců, včetně příjemců ve třetích zemích,
  - informace o případném předání osobních údajů do třetích zemí nebo mezinárodním organizacím (četně identifikace třetí země nebo mezinárodní organizace)
    - doložení vhodných záruk při předání do třetích zemí nebo mezinárodním organizacím v případech, kdy nelze uplatnit jiná ustanovení nařízení 2016/679, tedy pokud:
      - tento převod není opakovaný,
      - týká se pouze omezeného počtu subjektů údajů,
      - je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů,

- pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů,
- správce o předání informuje dozorový úřad (UOOÚ),
- správce subjekt údajů informoval o předání a o závažných legitimních zájmech, které sledoval.

▪ plánované lhůty pro vymazání jednotlivých kategorií údajů (jeli to možné),
▪ obecný popis technických a organizačních opatření (je-li to možné),

4.10.2.2 zpracovatel

- záznamy o činnostech zpracování vede v písemné podobě (i elektronicky)
- záznamy o činnostech obsahují:
  - ▪ jméno a kontaktní údaje zpracovatele nebo zpracovatelů, jméno a kontaktní údaje správců, pro něhož zpracovatel jedná, případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů,
  - ▪ kategorii zpracování prováděného pro každého správce,
  - ▪ informace o případném předání osobních údajů do třetích zemí nebo mezinárodním organizacím (četně identifikace třetí země nebo mezinárodní organizace)
    - doložení vhodných záruk při předání do třetích zemí nebo mezinárodním organizacím v případech, kdy nelze uplatnit jiná ustanovení nařízení 2016/679, tedy pokud:
      - tento převod není opakovaný,
      - týká se pouze omezeného počtu subjektů údajů,
      - je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů,
      - pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů,
      - správce o předání informuje dozorový úřad (UOOÚ),
      - správce subjekt údajů informoval o předání a o závažných legitimních zájmech, které sledoval.
  - ▪ obecný popis technických a organizačních opatření (je-li to možné).

4.11 Správce nebo zpracovatel řeší porušení zabezpečení osobních údajů požadovaným způsobem v souladu s články 33 a 34 nařízení (*):

4.11.1 správce

4.11.1.1 zdokumentuje veškeré případy porušení zabezpečení osobních údajů (nastavení procesů a obsahu),

- ▪ 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:
    - uplatněné před porušením zabezpečení osobních údajů,
    - uplatněné po porušení zabezpečení osobních údajů (zejména ke zmírnění možných nepříznivých důsledků),
- procesy a termíny.
- zpracovatele.

4.11.1.2 Oznámí porušení zabezpečení osobních údajů dozorovému úřadu (ÚOOÚ):

- v případech, které pravděpodobně způsobí rizika pro práva a svobody fyzických osob
- oznámí do 72 hodin od okamžiku, kdy se o porušení dozvěděl,
    - pokud lhůty dodrženy nejsou, doplní zdůvodnění zpoždění,
    - pokud není možné poskytnout úplné informace najednou, mohou být poskytnuty bez zbytečného odkladu postupně,
- Obsah oznámení:
    - 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:
        - uplatněné před porušením zabezpečení osobních údajů,
        - uplatněné po porušení zabezpečení osobních údajů (zejména ke zmírnění možných nepříznivých důsledků),

4.11.1.3 Oznámí porušení zabezpečení osobních údajů subjektu údajů

- v případech porušení zabezpečení osobních údajů, které pravděpodobně způsobí vysoká rizika pro práva a svobody fyzických osob,
- v případech, že správce nezavedl náležitá technická a organizační opatření uplatněná na zasažené údaje, která činí údaje nesrozumitelnými pro osoby, které nemají oprávněný přístup,
- v případech, že správce nezavedl následná opatření, která zajistí, že se vysoké riziko pro práva a svobody fyzických osob neprojeví
- k oznámení:
    - oznámení se zasílá přímo subjektům údajů,
        - pokud by oznámení přímo subjektům údajů vyžadovalo nepřiměřené úsilí, potom je zvolen

jiný, stejně účinný, způsob (veřejné oznámení apod.),

- využití jasných a jednoduchých jazykových prostředků,
- oznámit bez zbytečného odkladu,
- obsah:
  - 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
    - uplatněné před porušením zabezpečení osobních údajů,
    - uplatněné po porušení zabezpečení osobních údajů (zejména ke zmírnění možných nepříznivých důsledků),

4.11.2 Zpracovatel

4.11.2.1 zjištěná porušení zabezpečení osobních údajů oznámení to bez zbytečného odkladu správci

4.12 Správce provedl v souladu s článkem 35 nařízení posouzení vlivu na ochranu osobních údajů (*):

4.12.1 Definice zpracování, kterých se povinnost týká:

4.12.1.1 zpracování osobních údajů, které budou mít vysoké riziko pro práva a svobody fyzických osob:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- rozsáhlé zpracování osobních údajů, které vypovídají:
  - o rasovém či etnickém původu,
  - o politických názorech,
  - o náboženském vyznání,
  - o filozofickém přesvědčení,
  - o zdravotním stavu,
  - o sexuálním životě nebo sexuální orientaci fyzické osoby,
  - členství v odborech,
  - genetických údajů,
  - biometrických údajů,
  - o trestných činech nebo se týkajících rozsudků ve věcech trestních, či souvisejících bezpečnostních opatřeních.
- rozsáhlé systematické monitorování veřejně přístupných prostorů,
- zpracování dle seznamu zveřejněného dozorovým úřadem (ÚOOÚ),
- jiná zpracování, kde vysoká riziko vyplývá z použitých technologií, z povahy, z rozsahu z kontextu a z účelů zpracování osobních údajů.

4.12.1.2 Výjimky

- zpracování dle seznamu výjimek zveřejněného dozorovým úřadem (ÚOOÚ), pokud seznam existuje,
- soubor operací nebo soubor zpracování, kdy:
  - zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
    - pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím právního základu,
    - ČR (dozorový úřad ÚOOÚ) nepovažuje provedení posouzení za nezbytné,
  - zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.
    - pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím právního základu,
    - ČR (dozorový úřad ÚOOÚ) nepovažuje provedení posouzení za nezbytné.

4.12.2 Termíny
- posouzení se provádí před zahájením zpracování,
- přezkum posouzení se provádí alespoň při změně rizika.

4.12.3 Obsah posouzení vlivu na ochranu osobních údajů
- alespoň:
  - systematický popis zamýšlených operací zpracování,
  - účely zpracování (včetně případných oprávněných zájmů správce),
  - posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska zajištění účelů,
  - posouzení rizik pro práva a svobody subjektů údajů,
  - plánovaná opatření k řešení těchto rizik:
    - záruky,
    - bezpečnostní opatření
    - mechanizmy k zajištění ochrany osobních údajů
    - přihlédnutí k oprávněným zájmům subjektů údajů.
  - doložení souladu s nařízení Evropského parlamentu a Rady (EU) 2016/679 (kodex, osvědčení nebo jinak).

4.13 Správce zajistil předchozí konzultaci s dozorovým úřadem v souladu s článkem 36 nařízení (*):

4.13.1 Definice zpracování, kterých se povinnost týká:

4.13.1.1 Zpracování osobních údajů, které budou mít vysoké riziko pro práva a svobody fyzických osob,
- u kterých správce nepřijal opatření ke zmírnění rizika pro práva a svobody fyzických osob.

4.13.2 Termíny:
- konzultace se provádí před zahájením zpracování,

4.13.3 Informace, které musí mít správce k dispozici a poskytuje je ČR dozorovému úřadu (ÚOOÚ):
- rozdělení odpovědnosti správce, společných správců a zpracovatelů zapojených do zpracování (pokud existuje – zejména v případě zpracování v rámci skupiny podniků),

- účely zpracování,
- způsoby zpracování,
- opatření a záruky poskytnuté za účelem ochrany práv a svobod subjektů údajů,
- kontaktní údaje případného pověřence pro ochranu osobních údajů,
- posouzení vlivu na ochranu osobních údajů,

4.13.4 Správce postupuje v rámci konzultace na základě dokumentů vydaných dozorovým úřadem (ÚOOÚ) v rámci jím uplatněných pravomocí.

4.14 Správce ustanovil v souladu s články 37 až 39 nařízení pověřence pro ochranu osobních údajů (*)

4.14.1 definice správců nebo zpracovatelů, kterých se povinnost týká

- orgány veřejné moci či veřejný subjekt (s výjimkou soudů jednajících v rámci svých soudních pravomocí),
- správce nebo zpracovatel, jehož hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
- správce nebo zpracovatel, jehož hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených,
- jiné subjekty, pokud to stanoví právní předpisy.

4.14.2 společný pověřenec pro ochranu osobních údajů

- skupina podniků muže jmenovat jediného pověřence,
  - pokud je snadno dostupný z každého podniku,
- pro několik orgánů veřejné moci nebo veřejné subjekty s přihlédnutím:
  - k jejich organizační struktuře
  - k jejich velikosti,

4.14.3 požadavky na odbornost pověřence pro ochranu osobních údajů,

- znalosti práva v oblasti ochrany osobních údajů,
- praxe v oblasti ochrany osobních údajů,
- schopnosti plnit úkoly:
  - poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle nařízení 2016/679 a dalších předpisů Unie nebo členských států v oblasti ochrany údajů,
  - monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států 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; monitorování souladu s koncepcemi správce (včetně rozdělení odpovědností, zvyšování povědomí o ochraně osobních údajů, odborná příprava pracovníků),
  - poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování při posouzení vlivu na ochranu osobních údajů,

- spolupráce s dozorovým úřadem (ÚOOÚ),
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle, a případně vedení konzultací v jakékoli jiné věci

4.14.4 další požadavky na správce

- zveřejnit kontaktní údaje pověřence pro ochranu osobních údajů,
- sdělit kontaktní údaje pověřence pro ochranu osobních údajů dozorovému úřadu (ÚOOÚ),
- podporovat pověřence pro ochranu osobních údajů při plnění úkolů tím, že mu poskytují zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí,
- zajistit, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů,
- v souvislosti s plněním svých úkolů není pověřenec správcem nebo zpracovatelem propuštěn ani sankcionován.
- pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.
- pověřenec je k dispozici subjektům údajů ve všech záležitostech spojených se zpracováním jejich osobních údajů,
- pověřenec je při plnění úkolů vázán tajemstvím a důvěrností (v souladu s právem EU nebo ČR).

4.15 Správce zpracovává osobní údaje v souladu s články 40 a 41 nařízení dle kodexu chování (*):

4.15.1 Pokud správce podepsal kodex chování:

- dodržuje ustanovení kodexu chování,
- je prováděno pravidelné monitorování dodržování kodexu.

4.16 Správce předává osobní údaje do třetích zemí nebo mezinárodním organizacím v souladu s články 44 až 50 nařízení (*):

4.16.1 Předávání založené na rozhodnutí o odpovídající ochraně

4.16.1.1 Případy, na které není třeba povolení dozorového úřadu (ÚOOÚ):

- Existuje platné rozhodnutí Komise umožňující
  - předání do určité země,
  - předání do určitého území v určité zemi,
  - předání do odvětví nebo více odvětví v určité zemi země,
  - předání určité mezinárodní organizaci,
  - platné rozhodnutí komise dle směrnice 95/46/ES.

4.16.2 Předávání založené na vhodných zárukách

4.16.2.1 Případy, na které není třeba povolení dozorového úřadu (ÚOOÚ):

- pomocí právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty,
- pomocí standardních doložek o ochraně osobních údajů přijatých Komisí,
- pomocí standardních doložek o ochraně údajů přijatých dozorovým úřadem a schválených Komisí,

- pomocí schváleného kodexu chování se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů,
- pomocí vydaného osvědčení se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů,
- pomocí závazných podnikových pravidel, která:
    - jsou právně závazná a platná pro všechny a prosazovaná všemi dotčenými členy skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, včetně jejich zaměstnanců;
    - subjektům údajů výslovně přiznávají vymahatelná práva v souvislosti se zpracováním jejich osobních údajů;
    - vymezují:
        - strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků a každého z jejích členů;
        - předání údajů nebo soubor předání,
            - kategorie osobních údajů,
            - typ zpracování,
            - účely zpracování,
            - typu dotčených subjektů údajů,
            - určení třetích zemí pro předání,
        - svoji právně závaznou povahu
            - interně,
            - externě,
        - použití obecných zásad pro ochranu údajů obsahuje zejména
            - účelové omezení,
            - minimalizaci údajů,
            - omezenou dobu uložení,
            - kvalitu údajů,
            - záměrnou a standardní ochranu osobních údajů,
            - právní základ pro zpracování,
            - zpracování zvláštních kategorií osobních údajů,
            - opatření k zajištění zabezpečení údajů,
            - požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány,
        - práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu:
            - právo na přístup k osobním údajům,
            - právo na opravu,
            - právo na výmaz,
            - právo na omezení zpracování,
            - právo na přenositelnost údajů,
            - právo nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování,
            - právo podat stížnost u příslušného dozorového úřadu a příslušných soudů členských států,
            - právní ochrana a případně i práva na odškodnění v případě porušení závazných podnikových pravidel,

- přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii,
- způsob poskytování informací o závazných podnikových pravidlech subjektům údajů,
- úkoly pověřenců pro ochranu osobních údajů, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků a sledování školení a vyřizování stížností,
- postupy pro vyřizování stížností,
- mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly:
  - audity ochrany údajů,
  - metody zajištění opravných opatření pro ochranu práv subjektu údajů,
  - výsledky takového ověření jsou oznámeny pověřenci pro ochranu osobních údajů, nebo jakékoli jiné osobě či subjektu pověřenému monitorováním a vedení řídícího podniku,
- mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu,
- mechanismus spolupráce s dozorovým orgánem, zejména zpřístupňování výsledků ověřování dodržování opatření dozorovému úřadu,
- mechanismy pro podávání zpráv příslušnému dozorovému úřadu,
- právní požadavky, které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly, kterým je člen skupiny podniků nebo uskupení podniků podřízen ve třetí zemi,
- odbornou přípravu v oblasti ochrany údajů zaměstnanců.

4.16.2.2 Případy, na které je třeba povolení dozorového úřadu (ÚOOÚ) Úřadu pro ochranu osobních údajů:

- pomocí ad hoc smluvních doložek mezi správcem nebo zpracovatelem a správcem, zpracovatelem nebo příjemcem osobních údajů ve třetí zemi nebo v mezinárodní organizaci;
- pomocí správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektu údajů,
- platí i rozhodnutí vydané dozorovým úřadem (ÚOOÚ) nebo rozhodnutí vydané Komisí dle směrnice 95/46/ES.

4.16.3 Rozhodnutí soudního orgánu a rozhodnutí správního orgánu třetí země, jež po správci nebo zpracovateli požadují předání nebo zpřístupnění osobních údajů, lze jakýmkoli způsobem uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem, aniž jsou dotčeny jiné důvody pro převod podle této kapitoly.

4.16.4 Výjimky pro specifické situace

4.16.4.1 Případy, na které není třeba povolení dozorového úřadu (ÚOOÚ)

4.16.4.2 Uplatní se:

- pokud neexistuje rozhodnutí o odpovídající ochraně dle 14.6.1,
- pokud neexistují vhodné záruky pro předávání osobních údajů dle 14.6.2,

4.16.4.3 Podmínky:

- subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a následně k navrhovanému předání vydal svůj výslovný souhlas
    - nevztahuje se na činnosti prováděné orgány veřejné moci při výkonu jejich úředních pravomocí,
- předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů
    - nevztahuje se na činnosti prováděné orgány veřejné moci při výkonu jejich úředních pravomocí,
- předání je nezbytné pro uzavření nebo splnění smlouvy, která byla uzavřena v zájmu subjektu údajů mezi správcem a jinou fyzickou nebo právnickou osobou
    - nevztahuje se na činnosti prováděné orgány veřejné moci při výkonu jejich úředních pravomocí,
- je předání nezbytné z důležitých důvodů veřejného zájmu, který je uznán právem Unie nebo právem členského státu, které se na správce vztahuje,
- je předání nezbytné pro určení, výkon nebo obhajobu právních nároků,
- je předání nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiných osob v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas,
- k předání dochází z rejstříku, který je na základě práva Unie nebo členského státu určen pro informování veřejnosti a je přístupný k nahlížení veřejnosti obecně nebo jakékoli osobě, která může prokázat oprávněný zájem, avšak pouze pokud jsou v daném případě splněny podmínky pro nahlížení stanovené právem Unie nebo členského státu.

4.16.4.4 Pokud nelze uplatnit podmínky v článku 4.16.4.2, může předání do třetí země nebo mezinárodní organizaci dojít pouze tehdy, pokud:

- tento převod není opakovaný,
- týká se pouze omezeného počtu subjektů údajů,
- je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů,
- pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů
- informuje dozorový úřad,

- správce subjekt údajů informuje o předání a o závažných legitimních zájmech, které sledoval.

5 Použité zkratky:

EA MLA – European Accreditation Mulilateral Agreement

IAF MLA - International Accreditation Forum Multilateral Recognition Arrangements

KVO – kritéria pro vydávání osvědčení a kritéria pro akreditaci

ČSN – Česká technická norma

EN – Evropská norma

ISO - International Organization for Standardization

EU – Evropská unie

ES – Evropské společenství

ČR – Česká republika

6 Platnost dokumentu:

Kritéria pro vydávání osvědčení nabývají platnost dnem uveřejnění ve věstníku Úřadu pro ochranu osobních údajů.