

SMĚRNICE

ORGANIZACE:	Nezávislý odborový svaz Policie České republiky
NÁZEV DOKUMENTU:	Směrnice o zpracovávání a ochraně osobních údajů, č. 7/2023
OZNAČENÍ SMĚRNICE:	IS-GDPR-180501
VERZE SMĚRNICE:	23.6
ZPRACOVATEL:	ARION spol. s r.o.
PLATNOST OD:	01.07.2023
ÚČINNOST OD:	01.07.2023
SCHVÁLENO:	17. Sjezdem NOS PČR, 19.06.2023

OBSAH

1	ÚVODNÍ USTANOVENÍ.....	3
2	DEFINICE A ZKRATKY	3
3	ODPOVĚDNOSTI, POVINNOSTI A PRÁVOMOCI.....	5
4	OCHRANA OSOBNÍCH ÚDAJŮ	7
5	ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	9
6	SEZNAM PRÁVNÍCH NOREM.....	17

1 ÚVODNÍ USTANOVENÍ

1.1 Účel

Účelem tohoto dokumentu je stanovit všeobecně platnou metodiku pro nakládání a zpracování osobních údajů v organizaci Nezávislý odborový svaz Policie České republiky, se sídlem Praha 1, ul. Bartolomějská 7, PSČ 110 00, IČ: 49629034 (dále jen „Organizace“ nebo „NOS PČR“) tak, aby byly zajištěny podmínky ochrany stanovené NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „Nařízení“), zákonem č. 110/2019 Sb., o zpracování osobních údajů, zákona č. 127/2005Sb., o elektronických komunikacích, Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a podmínky, za kterých se osobní údaje zpracovávají v Organizaci, a to za účelem zajištění jejich řádné ochrany a zabránění jejich úniku, vyžrazení, zneužití, zničení a zamezení jejich ztrát.

Cílem je stanovit hlavní a jednoznačné zásady odpovědnosti, povinnosti a pravomoci při zpracování a zabezpečování ochrany osobních údajů v organizaci Nezávislý odborový svaz Policie České republiky. Tato směrnice stanovuje, aby subjekty zpracovávající osobní údaje zpracovávaly pouze údaje, které skutečně potřebují k výkonu pracovní činnosti a smluvních povinností, a to po nezbytně nutnou dobu, a aby vynaložily veškerou péči na eliminaci rizik spojených se zneužitím, nesprávným nakládáním, nesprávným stanovením účelu zpracování nebo neoprávněným shromažďováním a zpracováním osobních údajů.

Tento dokument je vydáván jako řídicí dokument pro organizaci Nezávislý odborový svaz Policie České republiky.

1.2 Rozsah závaznosti

Dokument je závazný pro zaměstnance Organizace a její smluvní dodavatele, pokud je součástí jejich díla jakékoliv zpracování osobních údajů, a to v níže stanoveném rozsahu.

2 DEFINICE A ZKRATKY

2.1 Definice

„**Bezpečnostní incident**“ je jedna nebo více událostí, v důsledku kterých nastala nebo existuje vysoká pravděpodobnost, že nastane, kompromitace činností Organizace nebo narušení bezpečnosti informací a souvisejících informačních aktiv.

„**Blokování osobních údajů**“ je operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů s výjimkou nezbytných zásahů.

„**Člen**“ je osoba splňující podmínky dle stanov Organizace.

„**Důvěrnost**“ je vlastnost vyjadřující omezení v oprávnění autorizované entity k přístupu a sdílení informačních aktiv a ochranu osobních a proprietárních dat.

„**Neoprávněné nakládání s osobními údaji**“ je jejich únik, vyžrazení, zneužití, poškození, znehodnocení, neoprávněný přístup a likvidace, porušení jejich ochrany nebo ztráta.

„**Nosič osobního údaje**“ je prostředek, který umožňuje udržování osobních údajů v podobě, která je umožňuje dále zpracovávat. Může mít listinnou podobu nebo jinou hmotnou podobu nebo to může být elektronické médium, které je pevnou nebo oddělitelnou, přenosnou nebo neprenosnou součástí počítačového systému.

„**Nositel rodného čísla**“ je fyzická osoba, které bylo rodné číslo přiděleno.

„**Ochrana osobních údajů**“ je soubor opatření v oblasti personální, administrativní, fyzické ochrany a informační bezpečnosti potřebných pro zajištění ochrany osobních údajů.

„**Osobní údaj**“ jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě

(dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

„**Manažer bezpečnosti osobních údajů**“ je osoba jmenovaná Organizací jako odpovědné osoby za ochranu osobních údajů (dále jen “MBOU”).

„**Příjemce**“ je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují. Zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

„**Rodné číslo**“ je identifikátor fyzické osoby přidělovaný v souladu se zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech.

„**Sjezd NOS PČR**“ je definován ve stanovách Organizace.

„**Shromažďování osobních údajů**“ je systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.

„**Souhlas subjektu údajů**“ je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

„**Správce**“ je organizace Nezávislý odborový svaz Policie České republiky, se sídlem Praha 1, ul. Bartolomějská 7, PSČ 110 00, IČ: 49629034, která prostřednictvím svého statutárního zástupce určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Správce může zmocnit nebo pověřit zpracováním osobních údajů Zpracovatele.

„**Subjekt údajů**“ je fyzická osoba, k níž se osobní údaje vztahují. Subjekt údajů se považuje za identifikovaný, nebo identifikovatelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu.

„**Uchovávání osobních údajů**“ je udržování údajů v takové podobě, která je umožňuje dále zpracovávat.

„**Úřad pro ochranu osobních údajů**“ je zřízen zákonem o ochraně osobních údajů. Jsou mu svěřeny kompetence ústředního správního úřadu pro oblast ochrany OÚ v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem.

„**Zachování mlčenlivosti**“ je povinnost nesdělovat osobní údaje a informace o opatřeních k jejich zabezpečení osobě, která není oprávněna se s těmito seznamovat.

„**Zničení (likvidace) osobních údajů**“ je fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.

„**Zpracování osobních údajů**“ je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, kterými jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

„**Zpracovatel**“ je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro Správce;

„**Zveřejněný osobní údaj**“ je údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného Katalogu.

„**Zvláštní kategorie údajů (citlivé údaje)**“ jsou osobní údaje, které vypovídají o rasovém

či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2.2 Zkratky

ČR	Česká republika
DPO	Data Protection Officer
EU	Evropská Unie
ICT	Hardware a software – prostředky informačních technologií – Information and Communication Technologies
MBOU	Manažer bezpečnosti osobních údajů
NDA	Non – Disclosure Agreement – Dohoda o mlčenlivosti
NOS PČR	Nezávislý odborový svaz Policie České republiky, se sídlem Praha 1, ul. Bartolomějská 7, PSČ 110 00, IČ: 49629034
PIA	Privacy Impact Assessments – dopadová analýza - posouzení vlivu zamýšlených operací zpracování na ochranu OÚ
ÚOOÚ	Úřad pro ochranu osobních údajů
ZZOÚ	Zákon č. 110/2019 Sb., o zpracování osobních údajů a Zákon č. 111/2019 Sb. o změně některých zákonů, ve znění pozdějších předpisů

3 ODPOVĚDNOSTI, POVINNOSTI A PRAVOMOCI

3.1 Vedení Organizace

Vedení Organizace je odpovědné za nastavení ochrany a zpracovávání osobních údajů v Organizaci. Vedení Organizace odpovídá za:

- rozpracování, udržování a řízení ochrany osobních údajů v souladu s touto směrnicí v rozsahu své působnosti,
- plánování a vyhodnocení ochrany a bezpečnosti osobních údajů,
- řešení a vyšetřování bezpečnostních incidentů vzniklých na úseku ochrany osobních údajů, analýzu jejich příčin a vyžadování nápravných opatření v rámci své působnosti,
- plnění povinností Organizace jako Správce vůči ÚOOÚ,
- zajištění ochrany a bezpečnosti osobních údajů, a to od zahájení jejich zpracovávání až do chvíle, kdy jsou likvidovány, a to jak prostředky administrativní ochrany, tak technickými prostředky,
- dodržování personálních, administrativních opatření a opatření fyzické ochrany a informační bezpečnosti stanovených obecně závaznými předpisy,
- zpracovávání pouze přesných osobních údajů pouze v souladu s účelem, k němuž byly shromážděny, a to v rozsahu nezbytném pro naplnění stanoveného účelu,
- informování subjektu údajů, popř. získání jeho souhlasu se zpracováním,
- stanovení způsobů, prostředků a míst zpracování osobních údajů, včetně povinností a odpovědnosti jednotlivých oprávněných osob,
- poskytnutí podkladů pro plnění povinností vůči ÚOOÚ,
- vedení záznamů o činnostech zpracování osobních údajů v souladu s Nařízením

- a minimálně v rozsahu tam uvedeném,
- l) předání kopií záznamů o činnostech zpracování osobních údajů MBOU,
 - m) stanovení účelu a doby zpracování osobních údajů,
 - n) zabezpečení plnění povinností Správce a Zpracovatele v souladu s Nařízením a ZZOÚ,
 - o) zajištění, aby názoru MBOU na situaci, která se dotýká oblasti ochrany osobních údajů, byla vždy přikládána váha,
 - p) zabezpečení uzavření smluv o zpracování osobních údajů se Zpracovatelem či Správcem,
 - q) zajištění účasti a stanoviska MBOU v situacích, kdy jsou přijímána rozhodnutí, která se mohou dotknout ochrany osobních údajů,
 - r) obsahovou náplň vzdělávání a výchovy v oblasti ochrany osobních údajů,
 - s) provádění kontroly dodržování Nařízení a ZZOÚ a řídicí dokumentace v Organizaci,
 - t) včasné informování MBOU o porušení Nařízení nebo ZZOÚ a o následných nápravných opatřeních,
 - u) zajištění vhodných technických a organizačních opatření v souladu s obecně závaznými předpisy a touto směrnicí,
 - v) zákonnost provozovaných služeb využívajících osobních údajů.

Vedení Organizace má pravomoc:

- a) vyžadovat pomoc a stanoviska MBOU při řešení situací souvisejících s ochranou osobních údajů a zákonností jejich shromažďování,
- b) být kontaktní osobou při komunikaci mezi Správcem a MBOU,
- c) řídit zajištění ochrany a bezpečnosti osobních údajů v Organizaci,
- d) provádět kontrolu dodržování Nařízení a ZZOÚ dokumentů systémů řízení a další dokumentace v Organizaci, a to ve spolupráci s MBOU.

3.2 Manažer bezpečnosti osobních údajů

Organizace určuje MBOU v souladu s Nařízením, které stanovuje na základě uzavřené smlouvy a podporuje MBOU při plnění úkolů uvedených ve článku 39 Nařízení s tím, že mu poskytuje zdroje nezbytné k plnění těchto úkolů, přístup k osobním údajům a k operacím zpracování osobních údajů v Organizaci.

3.2.1 MBOU plní zejména tyto úkoly:

- i. poskytování informací, poradenství a školení zaměstnanců Organizace,
- ii. poskytování informací subjektům údajů a plnění povinností podle Nařízení a dalších předpisů EU a ZZOÚ a monitorování souladu s těmito právními předpisy,
- iii. monitorování souladu zpracování osobních údajů v Organizaci s Nařízením, dalšími právními předpisy EU a ZZOÚ a s koncepcemi Správce nebo Zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do zpracování osobních údajů a souvisejících auditů,
- iv. poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle čl. 35 Nařízení,
- v. spolupráce s dozorovým úřadem – působit jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování OÚ.

3.3 Všichni zaměstnanci a/nebo smluvní dodavatelé

Všichni zaměstnanci a/nebo smluvní dodavatelé jsou povinni zejména:

- a) zajistit přiměřenou úroveň ochrany osobních údajů, k jejichž zpracování jsou oprávněni, zejména sdílením dat z prostředí Microsoft 365 nebo používáním šifrované ochrany proti ztrátě a zneužití dat:

- předávaných elektronickou poštou nebo přenášených nechráněnými telekomunikačními sítěmi,
 - v souborech a sdílených datových úložištích,
 - v pevných a přenosných počítačích, tabletech, mobilních telefonech a externích paměťových médiích,
- b) zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny a v rozsahu nezbytném pro naplnění stanoveného účelu a nesdružovat osobní údaje, které byly získány k rozdílným účelům,
- c) zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních k jejich ochraně; povinnost mlčenlivosti trvá i po skončení pracovního poměru, práce konané mimo pracovní poměr nebo příslušných prací,
- d) v případě zjištění neoprávněného nakládání s osobními údaji, v případech porušení zabezpečení osobních údajů, informovat přímého nadřízeného nebo vedení Organizace na email: gdpr@nosp.cz,
- e) poskytnout vedení Organizace a MBOU potřebnou součinnost.

4 OCHRANA OSOBNÍCH ÚDAJŮ

4.1 Subjekty údajů

Typickými subjekty údajů v podmínkách Organizace jsou:

- a) Členové Organizace
- b) fyzické osoby v zaměstnaneckém nebo obdobném vztahu,
- c) uchazeči o zaměstnání,
- d) obchodní partneři – fyzické osoby nebo zástupci právnických osob,
- e) další osoby (zákazníci, účastníci marketingových akcí apod.).

V souvislosti s identifikací subjektu údajů je třeba posoudit, jaký je účel zpracovávání a zda je ke zpracovávání nutný souhlas subjektu údajů nebo zda je zpracování osobních údajů možné na základě jiného právního titulu.

Dále je nutné stanovit způsob získávání osobních údajů od subjektů údajů, zejména s ohledem na to, aby nedocházelo k využívání údajů získaných k jinému účelu, případně ke slučování údajů získaných k jiným účelům, a způsob plnění informační povinnosti Organizace vůči subjektu údajů.

4.2 Systém opatření k ochraně osobních údajů

Opatření k ochraně zahrnují organizační, personální, administrativní, ICT opatření a opatření fyzické ochrany realizovaná na straně Správce nebo Zpracovatele osobních údajů.

4.2.1 Personální opatření

Zaměstnanci a/nebo smluvnímu partnerovi Organizace je umožněn přístup k osobním údajům při správě nebo zpracování, na základě splnění všech následujících podmínek:

- i. oprávněného požadavku,
- ii. prokazatelného seznámení se způsobem, jakým mohou fyzické osoby s oprávněním s osobními údaji nakládat,
- iii. prokazatelného závazkem mlčenlivosti (NDA),
- iv. schválením přístupu odpovědným členem vedení Organizace,
- v. smluvnímu partnerovi Organizace na základě uzavřené smlouvy o zpracování osobních údajů.

4.2.2 Administrativní opatření

Administrativní ochrana osobních údajů zahrnuje zejména:

- i. vedení záznamů o činnostech zpracování,
- ii. vedení katalogů účelů a právních titulů zpracování,

- iii. označování a evidenci nosičů, v souladu se Spisovým a skartačním řádem, který tvoří přílohu č. 1 této směrnice,
- iv. vedení záznamů o předávání a příjmu nosičů,
- v. ukládání, archivaci a skartaci nosičů,
- vi. řízenou likvidaci nosičů informací (listinných, elektronických), v souladu se Spisovým a skartačním řádem
- vii. oprávnění k manipulaci s osobními údaji v rámci správy nebo zpracování je možné pouze na základě souhlasu příslušného Správce nebo Zpracovatele (vlastníka) informace,
- viii. přeprava je zajišťována důvěryhodným kurýrem.

4.2.3 Fyzická ochrana osobních údajů

Fyzická ochrana osobních údajů zahrnuje zejména:

- i. příslušná režimová opatření kdy informace musí být udržovány v zabezpečených monitorovaných prostorech s kontrolou přístupu,
- ii. technické prostředky řízení přístupů,
- iii. mechanické zábranné prostředky,
- iv. PZTS – požární zabezpečovací a tísňové systémy.

4.2.4 Ochrana osobních údajů v systémech a prostředcích ICT

Systémy a prostředky ICT určené pro správu a zpracování osobních údajů jsou zejména:

- i. šifrování přenositelných paměťových médií a discích a při přenosu v nechráněných telekomunikačních sítích,
- ii. zákaz ukládání dat a informací na vedením Organizace neschválená paměťová média,
- iii. řízení přístupů k osobním údajům striktně dle schválených autorizačních konceptů,
- iv. auditování autorizovaných i neautorizovaných přístupů,
- v. napojení a vyhodnocování bezpečnostních událostí v bezpečnostním dohledu,
- vi. zpracování a pravidelné ověřování plánů pro případ mimořádných situací, operativní postupy pro zajištění bezpečné činnosti systémů a prostředků ICT,
- vii. zajištění logování, zálohování a obnovy dat,
- viii. řízení verzí, archivace a skartace.

4.2.5 Ohlašování případů porušení zabezpečení osobních údajů

Jakékoli porušení zabezpečení osobních údajů, včetně informace o provedených nápravných opatřeních, ohlásí Organizace prostřednictvím MBOU dozorovému úřadu bez zbytečného odkladu do 24 hodin, nejpozději však do 72 hodin od okamžiku, kdy se o něm dozvěděla, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Toto rozhodnutí náleží výhradně vedení Organizace, stejně jako rozhodnutí o dalším postupu, týká-li se porušení zabezpečení osobních údajů, u kterých je Organizace pouze Zpracovatelem a pravidla postupu nahlášení obsahuje konkrétní smlouva o zpracování OÚ s konkrétním Správcem. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Ohlášení dozorovému úřadu musí obsahovat:

- i. popis případu, včetně přibližného rozsahu úniku (množství dotčených subjektů, množství uniklých dat, kategorie dat),
- ii. jméno kontaktní osoby (MBOU), která může poskytnout detailnější informace dozorovému úřadu,

- iii. popis pravděpodobných důsledků porušení zabezpečení,
- iv. popis opatření, které mělo za cíl vyřešit porušení zabezpečení osobních údajů, včetně případných kroků vedoucích ke zmírnění dopadu úniku.

4.2.6 Ohlašovací povinnost

Každý zaměstnanec nebo člen Organizace či její smluvní dodavatel je v případě zjištění neoprávněného nakládání s osobními údaji či případu porušení zabezpečení osobních údajů povinen neprodleně informovat přímého nadřízeného a/nebo vedení Organizace [na e-mail: gdpr@nosp.cz](mailto:gdpr@nosp.cz).

5 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Zpracování osobních údajů, které není v souladu s Nařízením a ZZOU se v Organizaci zakazuje.

5.1 Podmínky zpracovávání osobních údajů

Vedení Organizace odpovídá za záměr zpracovávat osobní údaje MBOU. Oznámení o záměru zpracovávat osobních údajů obsahuje:

- a) zákonné zdůvodnění zpracování osobních údajů, účel, rozsah, místo, prostředky a zdroje zpracovávání osobních údajů.
- b) seznam všech zpracovatelů a příjemců osobních údajů,
- c) seznam personálních, administrativních a režimových opatření sloužících k zajištění ochrany zpracovávaných osobních údajů.
- d) bez posouzení záměru zpracovávat osobní údaje vedením Organizace a MBOU je zakázáno zahájit zpracování osobních údajů.

5.1.1 Účel zpracování

Vedení Organizace odpovídá za stanovení účelu zpracovávání osobních údajů, rozsah využívaných údajů a předkládá zdůvodnění zpracování osobních údajů. Stanovený účel zpracovávání musí být pravdivý a jednoznačný.

Osobní údaje lze zpracovávat pouze s ohledem na platné právní předpisy ČR a Nařízení, v souladu s účelem, k němuž byly shromážděny. Zpracovávat je k jinému účelu je možné jen tehdy, pokud o této změně zpracování byl subjekt údajů informován, a nelze-li takové zpracování provádět na základě právního titulu nevyžadujícího předchozí souhlas, pokud k tomu dal subjekt údajů souhlas.

5.1.2 Rozsah zpracovávaných údajů

Rozsah zpracovávaných údajů musí být stanoven tak, aby splnil stanovený účel, a přitom nebyly shromažďovány a zpracovávány nadbytečné osobní údaje.

5.1.3 Zdroje osobních údajů

Zdrojem pro zpracovávání osobních údajů jsou údaje poskytnuté subjektem údajů, nebo shromážděné internetovou stránkou případně jiné zdroje, přičemž jiné zdroje osobních údajů lze využít pouze při splnění všech povinností stanovených ZZOU a Nařízením.

5.1.4 Místo a způsob zpracování, opatření k ochraně osobních údajů

Vedení Organizace stanoví v řídicí dokumentaci (metodice) místo/a, na kterých jsou osobní údaje zpracovávány, prostředky a způsob (technologie), který je ke zpracovávání využíván a stanoví personální, administrativní a režimová opatření sloužící k zajištění ochrany osobních údajů, které zpracovává.

Oprávnění pracovníci mohou zahájit zpracování osobních údajů jen za předpokladu, že jsou splněny veškeré podmínky stanovené Nařízením a ZZOU, tj. je zejména splněna zákonnost zpracování a informační povinnost.

5.1.5 Pravidla pro internetové aktivity a pravidla pro používání sociálních sítí

Organizace je v rámci svých internetových aktivit nebo aktivit na sociálních sítích, ať už pro marketingové nebo pro jiné účely, povinná dodržovat povinnosti a zásady podle Nařízení.

5.2 Posouzení vlivu na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, provede vedení Organizace v součinnosti s MBOU před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu OÚ (dále jen "PIA"), a to v souladu s článkem 35 Nařízení.

5.2.1 Předchozí konzultace

Pokud z PIA vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by Organizace nepřijala opatření ke zmírnění tohoto rizika, konzultuje prostřednictvím MBOU toto zpracování před jeho započítím s dozorovým úřadem. Při konzultaci se postupuje v souladu s článkem 36 Nařízení.

5.3 Vedení záznamů zpracování

Organizace vede v souladu s čl. 30 Nařízení záznamy o činnostech zpracování, za něž zodpovídá, tyto záznamy obsahují všechny tyto informace:

- i. jméno a kontaktní údaje Správce a případného společného správce, zástupce Správce,
- ii. účely zpracování,
- iii. popis kategorií subjektů údajů a kategorií osobních údajů,
- iv. kategorie Příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně Příjemců ve třetích zemích nebo mezinárodních organizacích,
- v. informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce Nařízení, doložení vhodných záruk,
- vi. je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
- vii. je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 Nařízení.

Organizace v pozici Zpracovatele a každý smluvní Zpracovatel vede záznamy o činnostech zpracování, za něž zodpovídá, jež minimálně obsahují:

- i. jméno a kontaktní údaje Zpracovatele nebo zpracovatelů a každého Správce, pro něhož Zpracovatel jedná, a případného zástupce správce nebo Zpracovatele,
- ii. kategorie zpracování prováděného pro každého ze Správců,
- iii. informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce Nařízení, doložení vhodných záruk,
- iv. je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 Nařízení.

Záznamy se vyhotovují písemně, v to počítaje i elektronickou formu.

5.4 Zpřístupnění údajů, zpracování pomocí Zpracovatele

Ke zpracovávání osobních údajů je možno využít externí dodavatele, Zpracovatele. Podmínkou je uzavření písemné smlouvy o zpracovávání osobních údajů mezi Správcem a Zpracovatelem a závazek Zpracovatele dodržovat při nakládání s osobními údaji tuto směrnici.

Organizace také může působit jakožto Zpracovatel osobních údajů jiných Správců.

5.4.1 Posouzení nutnosti řešení ochrany osobních údajů ve smluvním vztahu

Vedení Organizace provede posouzení nutnosti řešení otázky ochrany a zpracování osobních údajů ve smluvním vztahu, je-li takovýto dotčen užitím osobních údajů subjektů, při posuzování záměru uzavřít smluvní vztah mezi Organizací a jiným subjektem.

5.4.2 Uzavření smlouvy o zpracování osobních údajů a zveřejnění zpracovatelů osobních údajů

- i. Za uzavření smlouvy o zpracování osobních údajů odpovídá vedení Organizace, které jakožto garant uzavírá smluvní vztah, jehož součástí je i zpracovávání osobních údajů, a které odpovídá za obsahové náležitosti takto uzavírané smlouvy,
- ii. Po uzavření smlouvy o zpracování osobních údajů se Zpracovatelem je skutečnost nového Zpracovatele osobních údajů ve vztahu k Organizaci, jakožto Správci, zapsána do „Katalogu zpracovatelů osobních údajů“ vedeného Organizací, který Organizace publikuje na svých webových stránkách, a to v rozsahu názvu (obchodní firmy) a identifikačního čísla Zpracovatele.

5.5 Souhlas se zpracováváním, informace o zpracovávání, ochrana a výkon práv subjektu údajů

5.5.1 Souhlas subjektu údajů

Pokud Organizace zpracovává osobní údaje na základě článku 6, odst. 1, písm. b), c), d), e), f) Nařízení, není nutný souhlas subjektu údajů, ale je potřeba splnit informační povinnost vůči subjektu údajů.

V ostatních případech může Organizace zpracovávat osobní údaje pouze s předchozím souhlasem subjektu údajů. Tento souhlas je nutný i v případě, že Organizace zpracovává osobní údaje k jinému účelu, než k jakému byly shromážděny. Organizace musí být schopna udělení souhlasu prokázat, a to po celou dobu zpracování, k jemuž byl dán souhlas. Součástí získání souhlasu je i informování subjektu údajů o účelu zpracovávání.

5.5.2 Informování subjektu údajů

Organizace je povinna včas a řádně v souladu s článkem 13 a 14 Nařízení ve stanoveném rozsahu informovat subjekt údajů o tom, že Správce zpracovává jeho osobní údaje. Kromě výše uvedených informací poskytne subjektu údajů další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů v rozsahu stanoveném Nařízením. Organizace musí subjekt údajů informovat o jeho právech vyplývajících z Nařízení.

5.5.3 Právo na přístup k informacím

Správce je povinen, na základě žádosti subjektu údajů, bezplatně jej informovat o tom, jaké údaje o něm zpracovává. Správce vydá subjektu údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud jsou zpracovávány, pak Správce umožní subjektu údajů přístup k těmto osobním údajům. Náležitosti sdělení jsou uvedeny v Nařízení.

Organizace plní ve vztahu k subjektu údajů Informační povinnost.

Příslušní pracovníci jsou povinni poskytnout bez zbytečného odkladu potřebné informace a požadovanou součinnost vedení Organizace a MBOU. Veškeré záznamy o poskytnutí informací se vedou v písemné formě (to zahrnuje i elektronickou formu).

5.5.4 Právo na opravu

Oprávněný pracovník bez zbytečného odkladu opraví či doplní nepřesné, resp. neúplné osobní údaje, které se týkají subjektu údajů, a to na základě žádosti subjektu údajů.

5.5.5 Omezení zpracování

Organizace omezí zpracování pokud:

- i. subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby Správce mohl ověřit přesnost osobních údajů,
- ii. zpracování je protiprávní a subjekt údajů odmítá výmaz osobního údaje a žádá místo toho o omezení jeho použití,
- iii. Správce již osobní údaj nepotřebuje pro účely zpracování, ale subjekt údajů jej požaduje pro určení, výkon nebo obhajobu právních nároků,
- iv. subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 Nařízení, dokud nebude ověřeno, zda oprávněné důvody Správce převažují nad oprávněnými důvody subjektu údajů.

5.5.6 Likvidace osobních údajů, právo na výmaz (právo být zapomenut)

Organizace, nebo na základě jejího pokynu Zpracovatel, je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány.

Organizace bez zbytečného odkladu vymaže osobní údaje, které se týkají subjektu údajů, který uplatnil právo na výmaz, nebo který využil práva být zapomenut, a to za předpokladu, že je dán jeden z těchto důvodů:

- i. osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- ii. subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) Nařízení zpracovány, a neexistuje žádný další právní důvod pro zpracování,
- iii. subjekt údajů vznesl námitky proti zpracování podle čl. 21 odst. 1 Nařízení a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznesl námitky proti zpracování podle čl. 21 odst. 2 Nařízení,
- iv. osobní údaje byly zpracovány protiprávně,
- v. osobní údaje musí být vymazány ke splnění zákonné povinnosti,
- vi. osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační Organizace podle čl. 8 odst. 1. 2 Nařízení.

Výše uvedené právo subjektu údajů se neuplatní, pokud je zpracování nezbytné:

- i. pro výkon práva na svobodu projevu a informace,
- ii. pro splnění zákonné povinnosti, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen,
- iii. z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení,
- iv. pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 Nařízení, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování,
- v. pro určení, výkon nebo obhajobu právních nároků.

5.5.7 Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Správce oznamuje jednotlivým Příjemcům, jimž byly osobní údaje zpřístupněny,

veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18 Nařízení, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto Příjemcích, pokud to subjekt údajů požaduje.

5.5.8 Právo na přenositelnost údajů

Organizace umožní subjektu údajů získat osobní údaje, které se ho týkají a které poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a umožní subjektu údajů předání těchto údajů jinému Správci, a to na základě žádosti subjektu údajů a v případě, že:

- i. zpracování je založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1 písm. b); Nařízení,
- ii. zpracování se provádí automatizovaně.

Při výkonu práva na přenositelnost údajů má subjekt údajů právo na to, aby osobní údaje byly předány přímo Správcem druhému Správci, je-li to technicky proveditelné.

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

5.6 Zpracování zvláštních kategorií údajů

Zpracovávání zvláštních kategorií údajů (citlivých údajů) je možné jen při splnění všech podmínek stanovených Nařízením a pouze v následujících případech:

- a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo EU nebo členského státu stanoví, že zákaz nemůže být subjektem údajů zrušen,
- b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv Správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem EU nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů,
- c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské, nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
- e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí,
- g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu osobních údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,
- h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva EU nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v Nařízení,
- i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo

- zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva EU nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství,
- j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 Nařízení na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

5.7 Využívání rodného čísla

Rodná čísla lze v evidencích, databázích a jiných zpracováních v Organizaci využívat pouze:

- a) při zpracovávání dle zvláštního právního předpisu,
- b) s písemným souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

5.8 Pořizování kopií průkazu zdravotního pojištění (kartičky pojištěnce)

Pořizování kopií zdravotního průkazu je možné jen s výslovným souhlasem subjektu údajů podle zákon č. 111/2019 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů a navazujícího zákona č. 133/2000 Sb. Zákon o evidenci obyvatel a rodných číslech, a to vzhledem k tomu, že číslo pojištěnce je současně rodné číslo fyzické osoby.

5.9 Pořizování kopií občanských průkazů

Pořizování kopií občanských průkazů je možné jen s výslovným souhlasem subjektu údajů podle zákona č. 328/1999 Sb. Zákon o občanských průkazech.

5.10 Biometrické údaje

Organizace nezpracovává biometrické údaje. Zaměstnanci mají možnost se pomocí biometrických údajů ověřovat pro přihlášení na klientské zařízení (např. notebook, mobilní telefon). Tento způsob ověřování není Organizací vynucen a jeho využívání Organizace nedoporučuje využívat. Pokud Zaměstnanec využívá své biometrické údaje k ověřování na klientském zařízení Organizace, je si vědom, že Organizace nemá určeny žádné organizační a technická opatření, která předpokládají zpracování biometrických údajů. V případě využívání biometrických údajů pro ověřování na klientských zařízeních Organizace, jsou tyto biometrické údaje převedeny na hash a uloženy v konkrétním zařízení. Pokud zaměstnanec klientské zařízení ztratí nebo jej předává do servisního střediska, zůstává hash vytvořený z biometrických údajů uložen na klientském zařízení.

5.11 Zpracování osobních údajů při krizových stavech

Z důvodu veřejného zájmu např. v oblasti veřejného zdraví může mít Organizace na základě mimořádného opatření povinnost provádět úkony, při kterých může docházet ke zpracování osobních údajů zaměstnanců. Příkladem této situace bylo např. povinné testování zaměstnanců na přítomnost nákazy COVID-19. Konkrétní zpracování osobních údajů se řídí příslušnými pokyny konkrétního nařízení a informace o zpracování osobních údajů musí být náležitě zabezpečena před možným narušením dostupnosti, důvěrnosti nebo integrity dat. Přístup k osobním údajům v případě krizového stavu je řízen, tj. povolen jen pro určené osoby stanovené vedením Organizace.

Organizace má povinnost poskytnout zaměstnancům konkrétní informace o zpracování osobních údajů, minimálně pak:

- i. totožnost a kontaktní údaje Organizace a MBOU
- ii. účely zpracování osobních údajů
- iii. právní základ tohoto zpracování a případný oprávněný zájem
- iv. informace o případném předání osobních údajů jiným příjemcům nebo

- v. kategorie příjemců osobních údajů
- vi. dobu zpracování osobních údajů
- vii. právech Subjektu údajů
- viii. případný úmysl Organizace předat osobní údaje do třetí země
- ix. skutečnost, zda dochází k automatizovanému rozhodování, včetně profilování
- ix. existence práva podat stížnost u dozorového úřadu nebo MBOU.

Součástí evidence zpracovávaných osobních údajů může být vytvoření záznamu o činnostech zpracování podle čl. 30 Obecného nařízení.

5.12 Zpracování Osobních údajů při sjezdu NOS PČR a online jednání

V případě online jednání nebo sjezdu NOS PČR může být využívána cloudová služba Microsoft Teams, pomocí které je možné pořizovat videozáznamy v souladu se stanovami Organizace. V případě pořizování záznamu s jeho uložením jsou účastníci informováni upozorněním v aplikaci Microsoft Teams. Účely pořizování videozáznamu jsou uvedeny ve Stanovách Organizace, např. pro potřeby zapisovatele a pro ověření zápisu. Délka uchovávání videozáznamů je definována ve stanovách Organizace.

5.13 Výběrová řízení pro přijetí nových zaměstnanců

Pro přijímání nových zaměstnanců je prováděno výběrové řízení, při kterém jsou zpracovávány životopisy uchazečů. Po skončení výběrového řízení jsou životopisy přijatých i nepřijatých uchazečů skartovány do 14 dnů, a to jak v písemné, tak v elektronické podobě. Skartaci elektronických a písemných dat je povinen zajistit každý zaměstnanec, kterému byly životopisy uchazečů zpřístupněny.

5.14 Proces přijetí členů Organizace a zpracování osobní údajů členů Organizace

Správce zpracovává osobní údaje členů Organizace uvedených na přihlášce. V případě přijetí člena, mu je přidělen jedinečný identifikátor – identifikační číslo člena. Aktuální vzory přihlášek jsou dostupné na webové prezentaci Organizace: <https://www.nospcr.cz/formulare/#prihlasky>. Členové Organizace mají možnost čerpat výhody a bonusy, při kterých jsou zpracovávány jejich osobní údaje. Pro poskytnutí konkrétní výhody nebo bonusu mohou být osobní údaje člena předávány jiné společnosti, která se podílí na zajištění plnění výhod nebo bonusů. Přehled výhod a bonusů je uveden na webové prezentaci Organizace <https://www.nospcr.cz/souhrn-vyhod/>.

5.15 Proces odchodu zaměstnance

Před ukončením pracovního poměru se zaměstnancem je zaměstnanec povinen předat firemní dokumenty a e-mailovou komunikaci svému nástupci nebo přímému nadřízenému. Zaměstnanec je povinen ověřit, že v e-mailové schránce nemá žádné doručené a odeslané e-maily s osobním obsahem.

Po odchodu zaměstnance je na e-mailovou adresu nastavena NDR zpráva upozorňující adresáty na ukončení pracovního poměru se zaměstnancem a e-mailová schránka je ponechána maximálně po dobu 3 měsíců od ukončení pracovního poměru pro možnost dohledání předchozí firemní e-mailové komunikace. Následně je zadán požadavek na Správce počítačové sítě, aby byl provedeno vymazání e-mailové schránky.

5.16 Předávání osobních údajů smluvním partnerům

Smluvním partnerům Organizace mohou být předávány osobní údaje členů a zaměstnanců pro zajištění poskytování služby, výhody nebo benefitu. Zejména jsou předávány následující osobní údaje: jméno, příjmení, telefon, e-mail. Smluvní partner může předané osobní údaje využít na základě oprávněného zájmu ke kontaktování člena nebo zaměstnance Organizace pro zaslání obchodního sdělení. Smluvní partneři dále využívají osobní údaje člena pro ověření platného členství v NOS PČR.

5.17 Obchodní sdělení

Subjektům údajů mohou být zasílány obchodní sdělení na základě uděleného souhlasu Subjektu údajů nebo na základě oprávněného zájmu. V obou případech má Subjekt údajů možnost kdykoli odvolat souhlas se zasíláním Obchodních sdělení.

5.18 Předávání osobních údajů do jiných států

Oprávněný pracovník, který hodlá předávat osobní údaje do zahraničí nebo určité mezinárodní organizaci (vyjma členských zemí EU), sdělí tuto skutečnost písemně vedení Organizace, ve svém sdělení uvede důvod předání, zdroj osobních údajů, jejich kategorii, konečné určení (stát, příjemce), popř. dobu předávání při opakované činnosti, které jsou potřebné k podání žádosti o povolení k předání ze strany ÚOOÚ.

5.18.1 Vedení Organizace:

- i. posoudí, zda je k předání potřebný souhlas ÚOOÚ,
- ii. předá svoje stanovisko MBOU, který v případě nutnosti dále posoudí nutnost souhlasu.

5.18.2 MBOU

MBOU v případě potřeby požádá neprodleně ÚOOÚ o povolení k předání nebo předávání OÚ do jiných států.

MBOU informuje neprodleně Organizaci:

- i. o tom, zda je možné osobní údaje předat do zahraničí bez souhlasu ÚOOÚ,
- ii. o podmínkách, které musí být případně splněny, aby mohlo k předání dojít,
- iii. o vydání nebo zamítnutí povolení ze strany ÚOOÚ.

5.19 Kontrolní činnost

5.19.1 Vnější kontrola

Vnější kontrolu dodržování Nařízení a ZZOÚ je oprávněn provádět výhradně příslušný dozorový úřad. Podmínky pro činnost dozorového úřadu a jeho spolupracovníků zajišťuje vedení Organizace v součinnosti s MBOU.

5.19.2 Interní kontrola

Kontrolu dodržování vnitřních předpisů a opatření ochrany osobních údajů v rámci Organizace provádí její vedení a MBOU a z této činnosti jsou pořizovány písemné kontrolní protokoly.

5.19.3 Externí kontrola

Organizace má právo kontrolovat dodržování sjednaných podmínek ochrany osobních údajů u smluvních partnerů. Ve smlouvě se smluvním partnerem musí být uvedena povinnost, že bude Organizaci za účelem kontroly umožněn:

- i. přístup k systémům a prostředkům ICT určeným pro nakládání s osobními údaji, včetně prostředků fyzické ochrany údajů v systémech a prostředcích ICT,
- ii. přístup k prostředkům fyzické ochrany osobních údajů,
- iii. přístup ke všem administrativním / technickým opatřením týkajících se nakládání s osobními údaji,
- iv. z kontrol jsou vyloučeny komunikační systémy, které zajišťují funkčnost technických a programových prostředků kritické informační infrastruktury.

6 SEZNAM PRÁVNÍCH NOREM

Nařízení EU 2016/679	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Zákon č. 110/2019 Sb.	zákon ze dne 12. března 2019 o zpracování osobních údajů, v platném znění
Zákon č. 111/2019 Sb.	zákon ze dne 12. března 2019, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, v platném znění
Zákon č. 133/2000 Sb.	zákon o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)
Zákon č. 40/2009 Sb.	Trestní zákoník, v platném znění
Zákon č. 418/2011 Sb.	zákon ze dne 27. října o trestní odpovědnosti právnických osob a řízení proti nim, v platném znění
Zákon č. 480/2004 Sb.	zákon o některých službách informační organizace a o změně některých zákonů (zákon o některých službách informační organizace) , v platném znění
Zákon č. 89/2012 Sb.	Občanský zákoník, v platném znění
Zákon č. 127/2005 Sb.	zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) , v platném znění
Zákon č. 181/2014 Sb.	zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění
Vyhláška č. 82/2018 Sb.	vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat (vyhláška o kybernetické bezpečnosti), v platném znění