**I N S T R U K C E**

**č. 8/2023**

**Ministerstva spravedlnosti**

**ze dne 15.08.2023, č. j. 145/2023-OI-SP**

**o technické spolupráci a zajištění bezpečnosti centrálních informačních systémů provozovaných Ministerstvem spravedlnosti**

Ministerstvo spravedlnosti (dále jen „**ministerstvo**“) stanoví:

**ČÁST PRVNÍ**

**ÚVODNÍ USTANOVENÍ**

§ 1

**Předmět úpravy**

1. Tato instrukce upravuje:
2. definice a evidence technických a kvalitativních parametrů se vztahem
k provozu, údržbě, bezpečnosti centrálních informačních systémů a služeb provozovaných ministerstvem (dále jen „**Informační systémy
a služby**“) v resortu ministerstva pro justiční složky, případně justičními složkami zajišťujícími centrální provoz aplikací pro jiné justiční složky nebo justiční složku, a vymezení rozsahu jeho užívání v rámci působnosti ministerstva nebo justiční složky, zejména:
	1. technické parametry (např. dostupnost, kapacita apod.) Informačních systémů a služeb,
	2. způsob řízení Informačních systémů a služeb, včetně plánování jeho zdrojů nutných pro kvalitní a bezproblémový provoz,
	3. bezpečnost Informačních systémů a služeb v oblasti personální, organizační, aplikační, technologické, datové a fyzické, resp. objektové,
3. práva a povinnosti interních a externích subjektů podílejících se na přípravě, realizaci, údržbě a užívání Informačních systémů a interní i externí vazby Informačních systémů a služeb.

§ 2

**Působnost instrukce**

1. Tato instrukce se vztahuje na Informační systémy dle zákona o informačních systémech veřejné správy[[1]](#footnote-1), zákona o kybernetické bezpečnosti[[2]](#footnote-2), případně klíčových, sdílených, aplikačních služeb a tzv. digitálních služeb dle zákona o právu na digitální služby[[3]](#footnote-3), včetně prováděcích vyhlášek.
2. Tato instrukce se nevztahuje na systémy obsahující nebo zpracovávající utajované informace podle zákona o ochraně utajovaných informací[[4]](#footnote-4).
3. Za plnění povinností vyplývajících z této instrukce odpovídají a právní jednání činí následující osoby:
* ministr spravedlnosti,
* předsedové:
* Nejvyššího správního soudu,
* Nejvyššího soudu,
* vrchních soudů,
* krajských soudů a Městského soudu v Praze,
* okresních (obvodních) soudů a Městského soudu v Brně,
* nejvyšší státní zástupce,
* vrchní státní zástupci,
* krajští státní zástupci a městský státní zástupce v Praze,
* okresní (obvodní) státní zástupci a městský státní zástupce v Brně,
* generální ředitel Vězeňské služby České republiky;
* ředitelé:
* Rejstříku trestů,
* Justiční akademie,
* Probační a mediační služby,
* Zotavovny Vězeňské služby České republiky,
* Institutu pro kriminologii a sociální prevenci,

(dále jen „**vedoucí justiční složky**“).

§ 3

**Vymezení pojmů**

Pro účely této instrukce se rozumí:

1. Active Directory – adresářové služby LDAP.
2. AISC – agendový informační systém cizinců.
3. Aktivum – obecně cokoliv, co má pro organizaci hodnotu, která se dělí na primární aktiva a podpůrná aktiva a dále na informační a technická. Blíže je problematika upřesněna v dokumentu „Metodika určování aktiv a stanovování garantů“, který je přílohou instrukce č. 5/2022[[5]](#footnote-5).
4. Auditor kybernetické bezpečnosti – osoba provádějící audit kybernetické bezpečnosti všech informačních aktiv zahrnutých do systému řízení bezpečnosti informací resortu spravedlnosti.
5. Dodavatel Informačního systému – subjekt, se kterým je uzavřen smluvní vztah
na provoz/vývoj/údržbu Informačního systému.
6. Garant podpůrného aktiva – fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti podpůrného aktiva.
7. Garant primárního aktiva – fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti primárního aktiva.
8. HW – hardware.
9. ICT – informační a komunikační technologie.
10. Informační systém – jedná se o informační systém dle zákona o informačních systémech veřejné správy1, zákona o kybernetické bezpečnosti2, případně klíčových, sdílených, aplikačních služeb a tzv. digitálních služeb dle zákona o právu na digitální služby, včetně prováděcích vyhlášek3.
11. Informační systémy – soubor samostatných informačních systémů zahrnujících několik vzájemně provázaných provozních informačních systémů resortu spravedlnosti, které byly vybudovány za účelem podpory ekonomických procesů, procesů řízení lidských zdrojů, řídicích procesů managementu a dalších souvisejících procesů naplňujících znaky nejen významného informačního systému nebo kritické informační infrastruktury podle zvláštního právního předpisu2.
12. ISVS – informační systém veřejné správy dle zákona o informačních systémech veřejné správy1.
13. KII – kritická informační infrastruktura dle zákona o kybernetické bezpečnosti2.
14. Klient – jedná se o typ klienta, jakožto webovou aplikaci, SW, Webová služba, ProID a RDP, script, případně mobilní zařízení.
15. LDAP – Lightweight Directory Access Protocol – definovaný protokol pro ukládání
a přístup k datům na adresářovém serveru.
16. OLA – Operational Level Agreement – dohoda o úrovni poskytovaných služeb mezi jednotlivými funkčními IT celky organizace, tzn. vztah mezi ministerstvem a justiční složkou, justiční složkou a dalšími justičními složkami nebo justiční složkou
a ministerstvem[[6]](#footnote-6).
17. Partner provozovatele – subdodavatel.
18. PIS – provozní informační systém dle zákona o informačních systémech veřejné správy1.
19. Podpůrné aktivum – jakékoliv aktivum zajišťující správnou funkčnost a podporu primárního aktiva (hardware, software, počítačová síť, pracovníci, lokalita, organizace apod.).
20. Primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje klíčový informační systém. Zároveň se jedná o aktivum vysoké důležitosti, jehož narušení ohrožuje výkon působnosti a správy justiční složky (v prostředí justice jsou to např. data agendových informačních systémů ISAS, ISYZ, ISVKS atd.).
21. ProID – serverové řešení pro automatické elektronické pečetění založené
na kvalifikovaném certifikátu.
22. Provozovatel – je orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém[[7]](#footnote-7); tuto roli vykonává zpravidla odbor informatiky ministerstva, případně i příslušná justiční složka, která zajišťuje centrální provoz aplikací pro jiné justiční složky nebo justiční složku.
23. Provozovatel ISVS – je provozovatelem informačního systému veřejné správy justiční složka nebo její součást, která zajišťuje funkčnost technických a programových prostředků tvořících informační systém veřejné správy. Provozováním informačního systému veřejné správy může správce pověřit jiné osoby nebo jejich součásti, pokud to jiný zákon nevylučuje[[8]](#footnote-8).
24. RDP – Remote Desktop Protocol je proprietární síťový protokol, který umožňuje uživateli využívat vzdálený počítač prostřednictvím počítačové sítě.
25. Seznam IS a služeb – jedná se o seznam, kde je vedena evidence informačních systémů dotčených touto instrukcí, tato evidence je vedena v rámci aplikace ShP na url adrese <https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx>. Seznam informačních systémů obsahuje základní informace (role, charakteristiky IS, parametry služeb, kontakty apod.) o informačních systémech a náležitosti vyplývající z právních předpisů upravujících kybernetickou bezpečnost a vytváření, správu, provoz, užívání
a rozvoj informačních systémů veřejné správy[[9]](#footnote-9).
26. ShP – SharePoint (softwarový nástroj pro týmovou spolupráci).
27. SLA – Service level Agreement – dohoda o úrovni poskytovaných služeb mezi IT organizací jako celkem a jejím zákazníkem, tzn. parametry služeb pro Systémy bude Provozovatel poskytovat v souladu s uzavřenými smlouvami s třetími stranami (partnery provozovatele) na zajištění podpor při provozu infrastruktury provozovatele v kombinaci s poskytováním služeb interních zaměstnanců ministerstva[[10]](#footnote-10).
28. Smluvní dokumentace – obecný pojem zahrnující jak vlastní smlouvu uzavřenou s externím subjektem, včetně Dohody o zachování mlčenlivosti, tak i dokumentaci
ke konkrétnímu informačnímu systému (provozní, uživatelská, administrátorská, bezpečnostní apod.) dle zákona o informačních systémech veřejné správy1, zákona
o kybernetické bezpečnosti2, případně klíčových, sdílených, aplikačních služeb a tzv. digitálních služeb dle zákona o právu na digitální služby3, včetně prováděcích vyhlášek.
29. Správce – je orgán nebo osoba definována podle § 3, písm. dd),ee), ff) a gg).
30. Správce aplikace – odborný útvar justiční složky nebo zaměstnanec odborného útvaru justiční složky, jemuž podle organizačního řádu justiční složky náleží odborné
a metodické řízení určité oblasti podporovaného informačního systému, a který je definován v interních aktech řízení jako odborný útvar spravující informační systém v souladu s právními předpisy upravujícími kybernetickou bezpečnost.
31. Správce informačního systému – je orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému[[11]](#footnote-11); tuto roli vykonává zpravidla odbor informatiky ministerstva, případně i příslušná justiční složka, která zajišťuje centrální provoz aplikací pro jiné justiční složky nebo justiční složku.
32. Správce komunikačního systému – je orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování[[12]](#footnote-12).
33. Správce ISVS – je správcem informačního systému veřejné správy justiční složka nebo její součást, která poskytuje služby informačního systému veřejné správy a za informační systém veřejné správy odpovídá, případně tuto roli může vykonávat i útvar ministerstva[[13]](#footnote-13).
34. Strana – justiční složka nebo Ministerstvo spravedlnosti.
35. SW – software.
36. Technický garant aktiva – osoba znalá ICT problematiky, která řeší technické aspekty provozovaného aktiva.
37. Technický garant podpůrného aktiva – technický pracovník, osoba znalá ICT problematiky, která řeší celkový ICT provoz v definované oblasti (organizace, resort).
38. Technický a kvalitativní parametr – soubor technických a programových prostředků, např. dostupnost, kapacita apod.).
39. URL - Uniform Resource Locator je soubor znaků, který slouží k identifikaci přesného umístění informací na internetu.
40. Uživatel – fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá primární aktiva; ve většině případů zahrnuje pracovníka justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený běžný (uživatelský) rozsah oprávnění přístupu.
41. VIS – Významný informační systém dle zákona o kybernetické bezpečnosti2.
42. VPN – virtual private network je virtuální soukromá síť, jedná se o zabezpečené šifrované připojení mezi dvěma sítěmi nebo mezi konkrétním uživatelem a sítí.
43. WAF – web application firewall je specifická forma aplikačního firewallu, která filtruje, monitoruje a blokuje HTTP provoz až do webové služby.
44. Další pojmy a zkratky jsou součástí instrukce č. 5/20225 a jejich příloh, zejména dílčích politik.

**ČÁST DRUHÁ**

§ 4

**Interní a externí subjekty Informačních systémů nebo služeb**

1. Interní subjekty jsou justiční složky a jejich uživatelé, kteří využívají nebo spravují informační systém / informační systémy / službu / služby.
2. Externí subjekt / externí smluvní partner je dodavatel nebo právnická či fyzická osoba, které jsou zpřístupňovány nebo předávány informační aktiva justiční složky.
3. Dodavatel je právnická nebo fyzická osoba, která se podílí na dodávce služeb nebo komponent souvisejících s informacemi nebo informačními systémy resortu spravedlnosti.

§ 5

**Přístup k datům**

Přístup k datům Informačního systému pro subjekty uvedené v § 4 odst. (1) až (3) lze realizovat na základě smluvní dokumentace k Informačnímu systému a na základě práv a povinností vyplývajících nejen z platných právních a resortních předpisů.

§ 6

**Dostupnost a kapacita Informačních systémů**

1. Dostupnost Informačních systémů je určována a řízena na podkladě zpracovaného hodnocení rizik Systému (analýza rizik) dle Metodiky určování aktiv a stanovování garantů a Metodiky hodnocení a řízení rizik vyplývajících z Instrukce č. 5/20225.
2. Kvalitativní a technické parametry služeb pro Informační systémy bude Provozovatel poskytovat v souladu s aktuálně uzavřenými smlouvami s třetími stranami (partnery provozovatele) na zajištění podpor při provozu infrastruktury provozovatele a jejich údaje budou publikovány odborem informatiky Ministerstva spravedlnosti na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx).

§ 7

**Práva a povinnosti subjektů podílejících se na provozu, rozvoji, údržbě a užívání Informačních systémů**

1. Provozovatel zajišťuje poskytování a kvalitu služeb, včetně technických
a programových prostředků a vykonává pro Správce v rámci provozu Informačních systémů a služeb z hlediska technické a komunikační infrastruktury zejména:
2. poskytování výpočetního výkonu (servery);
3. poskytování datového uložiště;
4. poskytování LAN a SAN infrastruktury;
5. poskytování komunikační infrastruktury, včetně MAN a WAN;
6. poskytování kryptografické ochrany síťové komunikace;
7. poskytování služeb ochrany perimetru a dalších příslušných služeb např. VPN, WAF apod.;
8. poskytování nástroje pro monitoring a zajištění přístupu justiční složky k tomuto nástroji;
9. poskytování nástroje pro logování a zajištění přístupu justiční složky k tomuto nástroji;
10. provádění penetračních testů, minimálně v součinnosti dodavatele informačního
a komunikačního systému se zaměřením na důležitá aktiva podle vyhlášky
o kybernetické bezpečnosti[[14]](#footnote-14);
11. poskytování a správa certifikátů;
12. zajišťování licencí a licenční podpory pro použité programové vybavení Informačního systému;
13. poskytování zálohovacího řešení a plánů záloh včetně provádění záloh
a ověřování funkčnosti zálohovacích médií formou plánovaných, pravidelných testů obnov, min. 1 x ročně;
14. vypracování a údržba plánu obnovy, včetně provádění případné obnovy
a pravidelných testů obnovy od „stolu“ (simulace havárie prováděná formou revize) min. 1 x za 3 roky;
15. poskytování souhrnného měsíčního reportingu justiční složce o:
	* 1. provozních problémech a incidentech,
		2. dodržování kvalitativních parametrů ze strany poskytovatele (dodržování SLA);
16. poskytování a průběžná aktualizace seznamu oprávněných osob Provozovatele s přístupem k Informačním systémům Provozovatele;
17. poskytování a průběžná aktualizace seznamu oprávněných osob Provozovatele s přístupem k infrastruktuře, na které je Informační systém provozován;
18. zajištění odděleného vývojového, testovacího a provozního prostředí.
19. Provozovatel zajišťuje pro Správce v rámci provozu Informačních systémů z hlediska poskytovaných služeb zejména:
20. součinnost se Správcem při provádění bezpečnostních auditů, ať již ze strany ministerstva (např. Auditora kybernetické bezpečnosti nebo garanta příslušného aktiva), nebo dalších orgánů (např. Národní úřad pro kybernetickou a informační bezpečnost);
21. součinnost se Správcem a dodavatelem informačního systému při zavádění úprav a změn v Informačním systému;
22. bezpečný provoz technické a komunikační infrastruktury
v souladu se zákonem o kybernetické bezpečnosti2, včetně zajištění fyzické bezpečnosti;
23. provoz nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
24. provoz nástroje pro detekci kybernetických bezpečnostních události
a provozních a aplikačních událostí;
25. poskytování přístupu k nástroji pro sběr a vyhodnocení kybernetických bezpečnostních událostí;
26. poskytování přístupu k nástroji pro detekci kybernetických bezpečnostních událostí, včetně reportovacích nástrojů a rozhraní;
27. spolupráci při zvládání kybernetických bezpečnostních incidentů.
28. V této souvislosti zajišťuje Provozovatel důvěrnost, dostupnost a integritu dat shromažďovaných v Systému, a to zejména tím, že zabezpečuje:
29. v součinnosti se Správcem kybernetickou bezpečnost Informačního systému;
30. v součinnosti se Správcem prostřednictvím třetí osoby (dodavatele) servis, podporu a rozvoj Informačního systému, včetně odstraňování technických problémů spojených s používáním Informačního systému;
31. v součinnosti se Správcem řízení přístupu do Informačního systému;
32. provoz a údržbu serverů a další infrastruktury spojené s Informačním systémem, včetně jeho proaktivního monitoringu;
33. bezpečnost serverů a další infrastruktury Informačního systému, zejména kontrolovaný přístup k nim;
34. zálohování Informačního systému;
35. provozuje a udržuje systém pro sběr požadavků a incidentů v režimu dle kvalitativních parametrů KII.
36. Správce je povinen:
37. provozovateli písemně či elektronicky oznámit bez zbytečného odkladu jakékoliv změny údajů uvedených na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx);
38. dodržovat požadavky právních norem a dalších předpisů, se zvláštním zřetelem na zákon o kybernetické bezpečnosti2, platné právní předpisy týkající se zpracování
 a ochrany osobních údajů[[15]](#footnote-15), zákon o informačních systémech veřejné správy1;
39. dodržovat platnou Instrukci o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti5 a požadavky vyplývající z navazujících bezpečnostních politik a metodik Ministerstva spravedlnosti;
40. po výzvě Provozovatele poskytnout součinnost při zajištění provozu nebo bezpečnosti Systému, a to včetně zajištění součinnosti dodavatele Systému;
41. informovat Provozovatele s dostatečným časovým předstihem (minimálně 14 kalendářních dnů předem) o nasazení nových verzí (distribucí) Systému a případně si vyžádat součinnost Provozovatele při těchto činnostech.

§ 8

**Bezpečnost Informačních systémů**

Cílem činností v oblasti bezpečnosti informací v prostředí ICT resortu spravedlnosti je podporovat plnění úkolů justičních složek, zajistit jejich kontinuitu a dodržování právních předpisů v oblasti ochrany a zabezpečení informací a osobních údajů tím, že omezují možná narušení jejich činností, následky bezpečnostních incidentů a zajišťují potřebnou důvěrnost, integritu a dostupnost informací v prostředí ICT.

§ 9

**Ochrana osobních údajů**

1. Správce a Provozovatel uchovává a zpracovává informace a údaje vzniklé v rámci provozu Informačních systémů dle této instrukce automatizovaně i manuálně v rámci vlastní smluvní dokumentace či v Informačním systému, a to sami či prostřednictvím pověřených zpracovatelů.
2. Správce a Provozovatel učiní v souladu s platnými právními předpisy dostatečná organizační a technická opatření zabraňující přístupu neoprávněných osob k osobním údajům.
3. Správce a Provozovatel jsou povinni se navzájem informovat o každém případu ztráty či úniku osobních údajů, neoprávněné manipulaci s osobními údaji nebo jiném porušení zabezpečení osobních údajů (dále jen „Porušení zabezpečení Osobních údajů“). Informace bude předána přes kontakty uvedené na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx), a to bez zbytečného odkladu, nejpozději do 24 hodin od vzniku Porušení zabezpečení Osobních údajů nebo i pouhé hrozby, jestliže Strana mohla o tomto Porušení zabezpečení Osobních údajů či i o hrozbě vzniku Porušení zabezpečení Osobních údajů vědět při vynaložení veškeré odborné péče. Nemohla-li Strana zjistit případ skutečného či hrozícího Porušení zabezpečení Osobních údajů před uplynutím lhůty dle předchozí věty tohoto článku, informuje druhou Stranu nejpozději do 24 hodin od okamžiku, kdy se o vzniku Porušení zabezpečení Osobních údajů nebo jeho hrozbě dozví. Strana je
i po poskytnutí informace druhé Straně povinna být maximálně nápomocna při řešení Porušení zabezpečení Osobních údajů, resp. při přijímání opatření ke zmírnění možných nepříznivých dopadů a zabránění vzniku obdobných situací v budoucnu. V ostatním se další postupy řídí přílohou č. 15 Instrukce č. 5/20225.
4. V případě, že jsou Správce a Provozovatel vůči Informačnímu systému v postavení společných správců podle Obecného nařízení Evropské Unie o ochraně osobních údajů15 (GDPR) nebo společně spravujících orgánů dle zákona o zpracování osobních údajů15 (ZZOÚ), definice jejich vztahu a odpovědnost za plnění povinností stanovených uvedenými právními předpisy je uvedena na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx).

**ČÁST TŘETÍ**

**ZÁVĚREČNÁ A ZMOCŇOVACÍ USTANOVENÍ**

§ 10

1. Tato instrukce nenahrazuje pravidla a postupy vyplývající z resortních předpisů, zejména z instrukce č. 5/20225, včetně platných bezpečnostních politik a dalších bezpečnostních dokumentací.
2. Ředitel odboru informatiky ministerstva se zmocňuje k vydávání aktualizací informací na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx).
3. Seznam atributů v rámci Seznamu IS a služeb v příloze č. 1 vydá ředitel odboru informatiky MSp formou řízené dokumentace.
4. Informace související s provozem, údržbou a rozvojem Informačních systémů publikuje odbor informatiky ministerstva na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx).

§ 11

**Účinnost**

Tato instrukce nabývá účinnosti dnem 1. 9. 2023.

**JUDr. Pavel Blažek, Ph.D.**

ministr spravedlnosti

**Příloha č. 1 k instrukci č. 8/2023**

SEZNAM IS A SLUŽEB

Tato příloha obsahuje Seznam atributů použitých na stránkách [Seznam IS a služeb](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx).

I. Seznam atributů v rámci Seznamu IS a služeb.

1. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. [↑](#footnote-ref-1)
2. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. [↑](#footnote-ref-2)
3. Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů. [↑](#footnote-ref-3)
4. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. [↑](#footnote-ref-4)
5. Instrukce č. 5/2022 Ministerstva spravedlnosti ze dne 30. června 2022, č. j. 115/2022-OI-SP/1 o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti. [↑](#footnote-ref-5)
6. Sjednané OLA parametry jsou uvedeny na stránkách [Seznam IS a služeb.](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx) [↑](#footnote-ref-6)
7. podle § 2 písm. g) zákona o kybernetické bezpečnosti [↑](#footnote-ref-7)
8. podle § 2 písmene d) zákona o informačních systémech veřejné správy [↑](#footnote-ref-8)
9. Zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů; zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů; vyhláška č. 360/2020 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, upravují vzájemná práva a povinnosti týkající se pravidel kybernetické bezpečnosti; vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů. [↑](#footnote-ref-9)
10. Sjednané SLA parametry jsou uvedeny na stránkách [Seznam IS a služeb.](https://itmsp.servis.justice.cz/Lists/Seznam%20IS%20a%20slueb/AllItems.aspx) [↑](#footnote-ref-10)
11. podle § 2 písm. e) zákona o kybernetické bezpečnosti [↑](#footnote-ref-11)
12. podle § 2 písm. f) zákona o kybernetické bezpečnosti [↑](#footnote-ref-12)
13. podle § 2 písmene c) zákona o informačních systémech veřejné správy [↑](#footnote-ref-13)
14. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) [↑](#footnote-ref-14)
15. 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., o zpracování osobních údajů, zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů [↑](#footnote-ref-15)