Směrnice
předsedy Vrchního soudu v Olomouci S 277/2022,
o ochraně osobních údajů

Na základě nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „nařízení"), směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (dále jen „trestněprávní směrnice"), zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon o zpracování osobních údajů"), a zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, vydává předseda Vrchního soudu v Olomouci tuto směrnici (dále jen „směrnice").

ČÁST PRVNÍ

OBECNÁ ČÁST
Čl. 1
Základní pojmy

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

(1) **Příklady informací, které samy o sobě nebo v kombinaci představují osobní údaje:**

- jméno a příjmení,
- adresa bydliště,
- e-mailová adresa, jako je například jméno.příjmení@firma.com,
- telefonní číslo — soukromé i pracovní,
- číslo identifikační karty zaměstnance, číslo občanského průkazu, číslo řidičského průkazu a číslo cestovního pasu,
- datum narození a rodné číslo,
- místo narození,
- pohlaví,
- věk,
- vzdělání,
- osobní stav,
- příjem ze zaměstnání, příjem z důchodu,
- IČ, DIČ,
- obchodní firma,

- akademický titul,
- číslo účtu, klientské číslo účtu, IBAN,
- IP adresa,
- identifikátor datové schránky.

(2) **Zvláštními kategoriemi osobních údajů** jsou osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofické přesvědčení nebo členství v odborech, 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.

(3) **Subjektem osobních údajů** je fyzická osoba, k níž se osobní údaje vztahují.

(4) **Zpracováním osobních údajů** je 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.

(5) **Správcem** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Za správce se považuje Vrchní soud v Olomouci (dále jen „VSOL“).

(6) **Bezpečnostním incidentem** je jakákoliv událost, která může vést k porušení zabezpečení osobních údajů.

(7) **Porušením zabezpečení osobních údajů** je každá událost, která vede k náhodnému nebo protiprávnímu stavu spočívajícím v:

a) **zničení** osobních údajů — osobní údaje už neexistují, případně nejsou použitelné (např.: zničení spisů v důsledku mimořádné události),

b) **ztrátě** osobních údajů — osobní údaje existují, ale došlo ke ztrátě kontroly nad těmito údaji, přístupu nebo ztrátě nosiče (např.: ztráta nebo krádež spisu, notebooku či USB),

c) **pozměnění nebo změně** osobních údajů - došlo k poškození integrity již zaznamenaných osobních údajů takovým způsobem, že jsou nesprávné nebo neúplné (např.: náhodná změna či smazání osobních údajů v seznamu jmen),

d) **poskytnutí** osobních údajů třetím osobám, které nejsou oprávněny k přístupu k osobním údajům (např.: osobní údaje byly zaslány omylem na jiné e-mailové adresy), nebo **přístupu** k osobním údajům při přenosu, uložení nebo jiném zpracování, v jejímž důsledku osobní údaje získaly neoprávněné osoby a došlo k porušení důvěrnosti (např.: osobní údaje jsou zpřístupněny jiným osobám v důsledku kybernetického útoku).

(8) **Vedoucím úseku** se pro účely této směrnice rozumí místopředsedové soudu a ředitel správy soudu.

(9) **Vedoucím oddělení** se pro účely této směrnice rozumí systémový inženýr, vedoucí kanceláře trestního, občanskoprávního a konkursního a insolvenčního úseku, vedoucí soudní podatelny a archivu, dozorčí úřednice, personalista, správce aplikací a bezpečnostní ředitel.

(10) **Příjemcem** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiné subjekty, kterým jsou osobní údaje poskytnuty, s výjimkou orgánů veřejné moci, které mohou získávat osobní údaje v rámci svých vyšetřovacích pravomocí podle zvláštních právních předpisů. Za příjemce se nepovažuje zaměstnanec VSOL.

(11) **Zaměstnancem** se přiměřeně pro účely této směrnice rozumí též soudce.

Čl. 2
Předmět úpravy

(1) Směrnice upravuje základní zásady a pravidla ve vztahu ke zpracování osobních údajů a zabezpečení jejich ochrany a v této souvislosti vymezuje odpovědnost a povinnosti zaměstnanců a soudců či stážistů (dále jen „zaměstnanci“). Směrnice dále vymezuje pravidla pro porušení zabezpečení ochrany osobních údajů, působnost a úkoly metodika pro ochranu osobních údajů (dále jen „metodik GDPR“) a působnost a úkoly konzultanta pro ochranu osobních údajů (dále jen „konzultant GDPR“), jakož i postup při vyřizování žádostí nebo podnětů subjektů údajů. Tato úprava navazuje na nařízení, trestněprávní směrnici, zákon o zpracování osobních údajů a zákon o soudech a soudcích.
(2) Tato směrnice rovněž zapracovává úpravu instrukce č. 5/2022 Ministerstva spravedlnosti ze dne 30. 6. 2022, č. j. 115/2022-OI-SP/1 o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti (dále jen „instrukce č. 5/2022“). Neupravuje-li tato směrnice blíže určitou oblast, aplikují se ustanovení právní úpravy instrukce č. 5/2022 a jejich jednotlivých politik.

Čl. 3
Obecné zásady

(1) Osobní údaje musí být:
a) zpracovávány korektně, zákonným a transparentním způsobem (zásada zákonnosti, korektnosti a transparentnosti),
b) shromažďovány jen pro určité, výslovně vyjádřené a legitimní účely a nesmí být dále zpracovány způsobem s těmito účely neslučitelnými, pokud právní předpis nestanoví jinak (zásada účelového omezení),
c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (zásada minimalizace),
d) v rámci možností přesné a v případě potřeby aktualizované (zásada přesnosti),
e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (zásada omezení uložení),
f) zpracovávány tak, aby bylo zajištěno náležité zabezpečení osobních údajů (zásada integrity a důvěrnosti).

(2) Při zpracování osobních údajů je postupováno v souladu s platnými právními předpisy upravujícími zpracování a ochranu osobních údajů, vnitřními předpisy a interními pokyny a opatřeními vrchního soudu včetně metodických pokynů nebo pokynů příslušného pověřence pro ochranu osobních údajů.

ČÁST DRUHÁ
ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

HLAVA I
ORGANIZAČNÍ A TECHNICKÁ OPATŘENÍ

Čl. 4
Základní vymezení

(1) Organizační a technická opatření k tomu, aby osobní údaje byly zpracovávány v souladu se zásadami uvedenými v čl. 3 této směrnice, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování a rizikům pro práva a svobody fyzických osob, přijímají a zajišťují vedoucí úseků a vedoucí oddělení.

(2) Organizačními a technickými opatřeními při zpracování osobních údajů podle odstavce 1 se rozumí např.: pokyny týkající se určení osobních údajů, které se při dané činnosti zpracovávají, stanovení doby uchovávání osobních údajů, pokud tato pravidla nevyplývají z obecně závazných právních předpisů a vnitřních předpisů, nebo zajištění technického nastavení systému jejich shromažďování či ukládání.
(3) Vedoucí správce počítačové sítě zajišťuje, aby funkce informačních systémů a jejich správa ve vztahu ke zpracování osobních údajů byly nastaveny v souladu se zásadami minimalizace a omezení uložení, a v této souvislosti navrhuje organizační a technická opatření.
(4) Metodik GDPR pravidelně vyhodnocuje, zda osobní údaje zpracovávané a evidované v rámci agend výkonu soudních pravomocí odpovídají zásadám minimalizace a omezení uložení a navrhuje opatření, která zajistí, aby byly zpracovávány v nezbytně nutném množství a rozsahu pro příslušný konkrétní účel, a zpřístupňovány pouze nezbytně nutnému počtu osob.

Čl. 5
Rejstříky, evidenční pomůcky a jiné další evidence

(1) Zpracovávat osobní údaje umožňující identifikaci subjektu údajů lze pouze v takových rejstřících, evidenčních pomůckách či jiných evidencích (dále jen „evidence“), které jsou:
a) součástí informačních systémů VSOL, nebo
b) vyjmenovány ve Vnitřním a kancelářském řádu pro okresní, krajské a vrchní soudy (dále jen „vnitřní a kancelářský řád“), nebo
c) evidencí vedenou podle zvláštních předpisů (např.: evidence v oblasti informačních technologií), nebo
d) pomocnou evidencí pro plnění pracovních úkolů, která je uspořádaným souborem v listinné podobě nebo vedená pomocí výpočetní techniky, pokud je vedena v souladu s odstavcem 3.

(2) V evidencích uvedených v odstavci 1 písm. a) až c) mohou zpracovávat osobní údaje jen zaměstnanci, kteří jsou k příslušným úkonům zpracování pověřeni vnitřními předpisy (např.: organizačním řádem VSOL), a to v souladu s pravidly uvedenými v odstavci 3.
(3) V evidencích uvedených v odstavci 1 musí být osobní údaje:
a) evidovány jen v nezbytném rozsahu,
b) je-li to technicky možné, pravidelně aktualizovány,
c) po uplynutí účelu zpracování vymazány, a to v souladu s příslušným konkrétním účelem zpracování specifikovaném v záznamech o činnostech zpracování a zásadou minimalizace,
d) v případě oprávněné žádosti subjektu údajů na opravu či výmaz osobních údajů (viz část šestá této směrnice) opraveny nebo vymazány.

(4) Pravidlo uvedené v odstavci 3 písm. c) nebo d) se nepoužije v případě, kdy výmaz osobních údajů nelze provést z důvodu technických možností informačního systému.
(5) Soulad evidencí uvedených v odstavci 1 písm. a) až c) s pravidly uvedenými v odstavci 3 zajišťují vedoucí úseků nebo jimi pověření zaměstnanci ve vztahu k evidencím na jejich úseku.
(6) U evidencí vedených podle odstavce 1 písm. d) zajistí soulad s odstavcem 3 zaměstnanec, který tuto evidenci vede. V případě, že si evidenci vede zaměstnanec pouze pro svoji potřebu v souvislosti s plněním pracovních úkolů, nesmí ji dále nikomu poskytnout nebo zpřístupnit a je povinen ji při skončení pracovního poměru nebo výkonu funkce smazat.
(7) Zaměstnanec pověřený vedením příslušné evidence uvedené v odstavci 1 písm. a) až c) v případě, že zjistí při vlastní činnosti, nebo na základě oznámení podle čl. 9 odst. 4 této směrnice, že jsou osobní údaje nepřesné nebo neaktuální, zajistí jejich opravu. Dále tento zaměstnanec provede opravu nebo výmaz osobních údajů, nebrání-li tomu technické možnosti informačního systému, a to na základě pokynu svého přímého nadřízeného nebo v případě oprávněné žádosti subjektu údajů na opravu či výmaz jeho osobních údajů (viz část šestá této směrnice). V rámci

výkonu soudních pravomocí může pokyn k opravě nebo výmazu udělit též předseda soudu, místopředsedové soudu, předsedové senátu a ředitel správy, popřípadě jimi pověřené osoby.
(8) Specifickou evidencí vedenou v souladu s nařízením je evidence souhlasů. V případě, že je evidence vedena, je zaměstnanec povinen tuto evidenci vést ve spise, za tím účelem vytvořeným. Je-li tato evidence vedena jen v elektronické podobě, je pověřený zaměstnanec vždy k datu 31. 12. každého roku povinen vytisknout výpis z této evidence a založit jej do spisu.

Čl. 6
Spisová služba

Vedoucí soudní podatelny a archivu zajistí, aby v rámci spisové služby byla s ohledem na technické možnosti přijímána taková organizační a technická opatření, která zajistí dodržování zásad minimalizace a omezení uložení osobních údajů.

HLAVA II
ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Čl. 7
Zpracování a kontrola záznamů

(1) Účely zpracování osobních údajů a doba jejich zpracování se eviduje pro jednotlivé agendy v záznamech o činnostech zpracování podle čl. 30 nařízení (dále jen „záznamy o zpracování“). Tyto záznamy vypracovává, monitoruje a aktualizuje metodik GDPR.
(2) Konzultant GDPR poskytuje v souvislosti se zpracováním a aktualizací záznamů o zpracování odborné konzultace z hlediska souladu s požadavky nařízení a společně s metodikem GDPR monitoruje, zda jsou záznamy o zpracování v souladu s nařízením. V případě zjištění nedostatků v záznamech o zpracování navrhuje konzultant GDPR úpravy či doplnění.
(3) Konzultant GDPR v součinnosti s metodikem GDPR provádí dohled ve vztahu k záznamům o zpracování v oblasti výkonu soudních pravomocí.

ČÁST TŘETÍ
ZABEZPEČENÍ A OCHRANA OSOBNÍCH ÚDAJŮ

Čl. 8
Obecná opatření

(1) Organizační a technická opatření k zabezpečení ochrany osobních údajů za účelem minimalizace rizik pro subjekty osobních údajů z hlediska ochrany osobních údajů provádějí:

a) ředitel správy soudu při zajišťování organizačních záležitostí souvisejících s provozem soudu,
b) bezpečnostní ředitel při zajišťování fyzické bezpečnosti soudu,
c) referent státní správy v rámci správy majetku,
d) vedoucí správce počítačové sítě v rámci informačních a komunikačních technologií,
e) mzdová účetní v rámci účetní a mzdové agendy,
f) personalista v rámci vedení personálních spisů,
g) dozorčí úřednice v rámci správy aplikací ISIR a ISVKS,
h) vedoucí soudní podatelny a archivu v rámci spisové služby a datových schránek.

(2) Organizačními a technickými opatřeními při zabezpečení osobních údajů podle odstavce 1 se rozumí např.: vydání konkrétních pokynů, týkajících se přístupových oprávnění, nejsou-li tato pravidla stanovena obecně závaznými právními předpisy či vnitřním předpisem, včetně zajištění technického nastavení přístupových oprávnění.

(3) Přijatá organizační a technická opatření podle odstavce 1 jsou dle potřeby a vývoje technologií revidována a aktualizována.
(4) Konzultant GDPR doporučuje přijetí organizačních a technických opatření podle odstavce 1 a poskytuje odborné konzultace z hlediska jejich souladu s nařízením a předpisy v oblasti ochrany osobních údajů.
(5) V případě, že metodik GDPR či konzultant GDPR zjistí nedostatky v zabezpečení osobních údajů, informuje předsedu soudu a odpovědné zaměstnance o této skutečnosti a společně s konzultantem GDPR doporučí, jaká opatření lze v této souvislosti přijmout. Odpovědní zaměstnanci navrhnou konkrétní opatření po konzultaci s metodikem GDPR či konzultantem GDPR a po jejich schválení předsedou soudu zajistí jejich realizaci.
(6) Ochrana osobních údajů je zajišťována také prostřednictvím organizačních a technických opatření stanovených vnitřními předpisy a instrukcemi Ministerstva spravedlnosti, které se týkají zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií.
(7) Pravidla pro skartaci spisů a dokumentů jsou stanovena v instrukci Ministerstva spravedlnosti, kterou se vydává skartační řád pro okresní, krajské a vrchní soudy, a to v platném a účinném znění.

Čl. 9
Povinnosti zaměstnanců

(1) Zaměstnanci jsou povinni zpracovávat osobní údaje tak, aby nemohlo dojít k porušení zabezpečení osobních údajů. Jsou povinni zpracovávat osobní údaje výhradně za účelem plnění svých pracovních povinností vyplývajících z jejich pracovní náplně, a to v nezbytném rozsahu pro plnění konkrétních úkolů a pouze za účelem, pro který jim oprávnění zpracovávat osobní údaje bylo uděleno.
(2) Zaměstnanci jsou povinni dodržovat organizační a technická opatření stanovená vedoucími zaměstnanci, vnitřním a kancelářským řádem a předpisy vztahujícími se k fyzické bezpečnosti objektu soudu a bezpečnosti při používání informačních a komunikačních technologií.
(3) Zaměstnanci jsou povinni důsledně dodržovat povinnost mlčenlivosti a chovat se tak, aby nemohlo dojít k porušení integrity (poškození, ztrátě či zničení) a důvěrnosti osobních údajů nebo dokumentů obsahujících osobní údaje, jak v elektronické tak listinné podobě. Za dodržování této povinnosti odpovídá vždy zaměstnanec, který osobní údaje zpracovává.
(4) V případě, že zaměstnanci, kteří zpracovávají osobní údaje, zjistí, že jsou osobní údaje v evidencích uvedených v čl. 5 odst. 1 této směrnice nepřesné nebo neaktuální, jsou povinni oznámit tuto skutečnost zaměstnanci pověřenému vedením příslušné evidence k provedení nápravy.
(5) Zaměstnanci jsou povinni uchovávat osobní údaje jen po dobu stanovenou právními předpisy a vnitřními předpisy nebo, není-li tak stanoveno, po dobu, jež je nezbytně nutná pro účely, pro které jsou zpracovávány.
(6) Zaměstnanci jsou povinni zpracovávat osobní údaje tak, aby nemohlo dojít k porušení jejich zabezpečení.
(7) Zaměstnancům je zejména zakázáno:
a) ukládat osobní údaje nebo dokumenty s osobními údaji na sdílená úložiště s výjimkou plnění povinností podle obecně závazných právních předpisů[1],
b) ukládat osobní údaje na sociální sítě, [1]
c) zpřístupnit či předat osobní údaje nebo dokumenty obsahující osobní údaje neoprávněné osobě, která není na základě obecně závazných právních předpisů nebo vnitřních předpisů či instrukcí Ministerstva spravedlnosti oprávněna ke zpracování konkrétních osobních údajů.

[1] Např.: zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

(8) Pro nakládání s osobními údaji platí další pravidla stanovená v dokumentu „Politika bezpečného chování uživatelů“, která je přílohou instrukce č. 5/2022.
(9) Zaměstnanci jsou povinni metodikovi GDPR a konzultantovi GDPR pro účely výkonu jejich působnosti poskytnout veškeré relevantní informace a nezbytnou součinnost.

Čl. 10
Zabezpečení ICT

(1) Každý zaměstnanec je povinen zabezpečit prostředky výpočetní techniky (např.: počítač, notebook, tablet, mobilní telefon apod.), které mu byly poskytnuty pro plnění pracovních povinností a jimiž zpracovává osobní údaje nebo jsou jejich prostřednictvím osobní údaje dostupné (dále jen „prostředky výpočetní techniky“), nebo datové nosiče (např.: flash disky, externí HDD, CD apod.) tak, aby neumožnil neoprávněným osobám přístup k osobním údajům uloženým na těchto zařízeních. Přenosné prostředky výpočetní techniky (např.: notebook, tablet, mobilní telefon) je zaměstnance povinen zabezpečit heslem, nebo pinem. Je třeba důsledně dodržovat pravidla pro bezpečné vytváření a zacházení s hesly, zejména nesmí být nikomu sdělovány a být zapsány v listinné podobě a umístěny na viditelném nebo běžně přístupném místě (např.: monitoru počítače, pracovním stole nebo kalendáři), případně být uchovány v souborech v prostředcích výpočetní techniky.
(2) Při každé ztrátě kontroly nad přístupem k prostředkům výpočetní techniky, musí být tyto prostředky zabezpečeny uzamknutím obrazovky, nebo displeje (např.: zadáním pinu). Na počítači, notebooku, mobilním telefonu či tabletu musí být nastaveno automatické uzamčení po určité době nečinnosti.
(3) Pro vzdálený přístup platí pravidla stanovená v instrukci Ministerstva spravedlnosti, týkající se kybernetické bezpečnosti.
(4) Všechny informační systémy a jiné aplikace používané na VSOL, které obsahují osobní údaje (např.: personální a mzdový informační systém), musí být zabezpečeny heslem.
(5) V případě skončení pracovního poměru zaměstnance jsou zrušeny jeho přístupy do informačních systémů a aplikací v souladu s vnitřními předpisy.

Čl. 11
Elektronické dokumenty

(1) Pracovní dokumenty s osobními údaji v elektronické podobě lze ukládat také na přenosné prostředky výpočetní techniky poskytnuté VSOL pro plnění pracovních povinností a na povolené datové nosiče v souladu s vnitřními předpisy.
(2) Zaměstnanec je povinen pracovní dokumenty předávat v elektronické podobě pouze prostředky a způsobem povoleným nebo schváleným VSOL. Zakazuje se pro tyto účely používat soukromý e-mail.
(3) Přenos pracovních dokumentů v elektronické podobě v elektronických sítích se řídí instrukcí Ministerstva spravedlnosti, týkající se kybernetické bezpečnosti.
(4) V případě skončení pracovního poměru zaměstnance nebo funkce soudce se předávají elektronické dokumenty s osobními údaji v souladu s vnitřním předpisem. Vedoucí správce počítačové sítě je povinen zajistit bezpečné smazání všech elektronických dokumentů s osobními údaji na svěřených prostředcích výpočetní techniky a nosičích dat.

Čl. 12
Skenování a tisk

(1) Každý zaměstnanec je povinen skenovat do svého pracovního e-mailu prostřednictvím lokálně připojené tiskárny.

(2) Dokumenty mohou být tištěny na lokální tiskárně, která je umístěna v kanceláři zaměstnance, nebo na chodbové tiskárně. Uživatel je povinen počkat u tiskárny, než se dokumenty vytisknou, a ihned je po vytištění odebrat. Obdobné podmínky bezpečnosti je nutné dodržovat také při skenování dokumentů.

Čl. 13
Přístup do informačních a jiných systémů, rejstříků a evidencí

(1) Pravidla nastavení přístupových oprávnění do informačních systémů (ISVKS, ISIR a IRES) a do jednotlivých rejstříků, evidenčních pomůcek a modulů těchto systémů jsou stanovena vnitřním a kancelářským řádem. Přístup do modulů sloužících k lustraci osob mají pouze pověření zaměstnanci, a to výlučně pro pracovní účely a jen v nezbytném rozsahu.
(2) Za nastavení přístupů do evidencí vedených v čl. 5 této směrnice, jak v analogové, tak elektronické podobě, odpovídá přímý nadřízený zaměstnance, který je pověřený vedením příslušné evidence.
(3) Přístupová oprávnění zaměstnancům do základních registrů a obdobných evidencí, vedených jinými subjekty, lze zřídit pouze se souhlasem předsedy soudu.
(4) Při nastavení přístupů podle odstavce 1 až 3 platí, že je třeba důsledně dbát na to, aby přístup měli jen zaměstnanci, kteří jej potřebují pro plnění svých pracovních povinností, a to jen v nezbytném rozsahu.
(5) Přístup zaměstnance do těchto evidencí je možný pouze na základě nezbytné potřeby vyplývající z výkonu funkce a stanoveného úkolu. Při každém přístupu do rejstříku je zaměstnanec oprávněn zpracovávat osobní údaje jen v nezbytném rozsahu a pouze za účelem plnění konkrétní pracovní povinnosti.
(6) Přístupy do analogových či elektronických evidencí musí být s ohledem na technické možnosti vhodným způsobem dokumentovány. Povinnost zdokumentování těchto přístupů je splněna např.: pořízením záznamu o přístupu nebo prostřednictvím logování operací, včetně uvedení důvodu tohoto přístupu. Za nastavení způsobu této dokumentace odpovídají zaměstnanci uvedení v čl. 8 odst. 1 této směrnice.

Čl. 14
Webové stránky a Intranet VS

(1) Na webových stránkách VSOL lze zveřejňovat osobní údaje jen v případě, že tak stanoví obecně závazný právní předpis nebo vnitřní předpis nebo je dán jiný právní titul zpracování podle nařízení. Intranet VSOL slouží ke sdílení interních informací a lze na něm zveřejňovat osobní údaje jiných osob, pokud s tím vyslovili souhlas nebo je dán oprávněný zájem VSOL na jejich zveřejnění.
(2) Oprávnění ke vkládání osobních údajů nebo dokumentů s osobními údaji na webové stránky nebo Intranet VS, jejich pravidelnou aktualizaci a dobu jejich uchovávání stanoví předseda soudu.
(3) Metodik GDPR v rámci své působnosti poskytuje odborné konzultace k právním titulům zveřejnění osobních údajů podle odstavce 1.

Čl. 15
Uchovávání dokumentů a spisů a jejich předávání

(1) Zaměstnanec je povinen dokument určený k zařazení do spisu uchovávat tak, aby k němu neměly přístup neoprávněné osoby. Přístup k těmto dokumentům a spisům je povolen jen zaměstnancům, kteří jsou oprávněni seznamovat se s příslušnými dokumenty či spisy, nebo jsou pověřeni k jejich předání a převzetí. Konkrétní vhodný způsob zabezpečení spisů musí být volen

s ohledem na povahu osobních údajů a riziko možného neoprávněného přístupu ke spisům. Za vhodný způsob uchovávání spisů se považuje uzamčená místnost nebo jinak zabezpečený prostor, uzamčená skříň či stůl, pokud obecně závazné právní předpisy nestanoví jiný způsob zabezpečení[2]. Za zajištění vhodných technických prostředků k zabezpečení ochrany dokumentů a spisů odpovídá ředitel správy soudu.
(2) V případě, že jde o zvláštní kategorie osobních údajů nebo existuje zvýšené riziko porušení ochrany osobních údajů (např.: při stavebních či jiných technických úpravách kanceláří), jsou zaměstnanci povinni věnovat zvýšenou pozornost ochraně osobních údajů při dodržování povinností podle odstavce 1 a volit způsob uchování, který poskytuje nejvyšší vhodnou záruku jejich ochrany.
(3) Jestliže bude nezbytné umožnit přístup třetí osobě (např.: řemeslníkovi) na pracoviště zaměstnance v případě jeho nepřítomnosti, ředitel správy soudu nebo jím pověřený zaměstnanec upozorní dotyčného zaměstnance na tuto skutečnost, například prostřednictvím e-mailu. Uvedený zaměstnanec v takovém případě přijme vhodná opatření, aby nemohlo dojít k neoprávněnému přístupu ke spisům či dokumentům obsahujícím osobní údaje.
(4) Předávání spisů a otázky s tím související blíže upravuje vnitřní pokyn o spisovém oběhu.

ČÁST ČTVRTÁ

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

HLAVA I
BEZPEČNOSTNÍ INCIDENTY V OBLASTI ICT

Čl. 16
Oznamovací povinnost

(1) Každý zaměstnanec je povinen v případě bezpečnostního incidentu v oblasti ICT, v jehož důsledku může dojít k porušení zabezpečení osobních údajů spočívajícího např.: ve ztrátě či krádeži přenosného prostředku výpočetní techniky nebo povoleného datového nosiče, vyzrazení hesla nebo pinu nebo podezření na jejich zneužití, zaslání e-mailu na nesprávnou e-mailovou adresu nebo v jiném poskytnutí či zpřístupnění osobních údajů v elektronické podobě neoprávněným třetím osobám (např.: v důsledku kybernetického útoku), oznámit tuto skutečnost ihned po jejím zjištění:

a) vedoucímu správci počítačové sítě a
b) metodikovi GDPR.

(2) Bezpečnostní incident, který byl zjištěn oddělením informatiky a má za následky porušení zabezpečení osobních údajů, oznamuje vedoucí správce počítačové sítě metodikovi GDPR.
(3) Oznámení o bezpečnostním incidentu podle odstavce 1 a 2 se podává na formuláři, který je přílohou č. 1 této směrnice. Metodikovi GDPR i vedoucímu správci počítačové sítě se tento vyplněný formulář zasílá na jejich pracovní e-maily s tím, že je následně nutné předat originál formuláře opatřený vlastnoručním podpisem též fyzicky.

Čl. 17
Posouzení incidentu

(1) Vedoucí správce počítačové sítě posoudí stav technického zabezpečení osobních údajů, přijatá technická a organizační opatření, zda došlo k porušení zabezpečení osobních údajů nebo je vysoká míra pravděpodobnosti, že mohlo k takovému porušení dojít. Svá zjištění a návrhy dalšího

[2] Např.: zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

opatření do budoucna, uvede v záznamu o bezpečnostním incidentu na formuláři, který je přílohou č. 2 této směrnice. Vedoucí správce počítačové sítě bez zbytečného odkladu předá metodikovi GDPR kopii záznamu vyhotoveného pro účely oznámení příslušnému orgánu v oblasti kybernetické bezpečnosti.
(2) V případě zjištění, že bezpečnostní incident vedl k porušení zabezpečení osobních údajů nebo v případě, že je vysoká míra pravděpodobnosti, že k porušení zabezpečení osobních údajů mohlo dojít, předá vedoucí správce počítačové sítě záznam o bezpečnostním incidentu metodikovi GDPR do 24 hodin od obdržení oznámení podle čl. 16 odst. 1 této směrnice, nebo po zjištění učiněném ve smyslu čl. 16 odst. 2 této směrnice.
(3) Pokud bylo zjištěno, že bezpečnostní incident neměl následky uvedené v odstavci 2, činí délka lhůty pro předání záznamu o bezpečnostním incidentu 10 pracovních dní.
(4) Metodik GDPR posoudí následky porušení zabezpečení osobních údajů vzniklé v souvislosti s bezpečnostním incidentem a rizika pro práva a subjekty údajů. Svá zjištění uvede v záznamu o porušení zabezpečení ochrany a posouzení následků na formuláři, který je přílohou č. 3 této směrnice.

HLAVA II
OSTATNÍ BEZPEČNOSTNÍ INCIDENTY

Čl. 18
Oznamovací povinnost

(1) Jakýkoliv jiný bezpečnostní incident, než uvedený v čl. 16 odst. 1 této směrnice, je povinen každý zaměstnanec ihned po jeho zjištění oznámit vedoucímu příslušného úseku.
(2) Oznámení o bezpečnostním incidentu se podává na formuláři, který je přílohou č. 1 této směrnice, a to způsobem uvedeným v čl. 16 odst. 3, věty druhé této směrnice.
(3) V případě ztráty spisu, kdy je vysoká pravděpodobnost, že nedošlo k neoprávněnému zpřístupnění jeho obsahu (spis se například nachází v budově soudu), se oznámení ve smyslu odstavce 1 a 2 podává v případě, že spis není nalezen do 48 hodin od zjištění jeho ztráty.

Čl. 19
Posouzení ostatních bezpečnostních incidentů

(1) V případě, že se jedná o bezpečnostní incident podle čl. 18 odst. 1 této směrnice, vedoucí úseku, v němž k incidentu došlo, posoudí, zda má incident za následek porušení zabezpečení osobních údajů. V případě, že došlo k porušení zabezpečení osobních údajů, zpracuje záznam o bezpečnostním incidentu na formuláři, který je přílohou č. 2 této směrnice a předá jej metodikovi GDPR.
(2) Metodik GDPR posoudí následky porušení zabezpečení osobních údajů a rizika pro práva a subjekty údajů. Svá zjištění uvede v záznamu o porušení zabezpečení ochrany a posouzení následků na formuláři, který je přílohou č. 3 této směrnice.

HLAVA III
OHLAŠOVÁNÍ A OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ

Čl. 20

(1) Pokud je na základě posouzení podle čl. 17 a čl. 19 této směrnice pravděpodobné, že porušení zabezpečení mělo za následek riziko pro práva a svobody fyzických osob, tak metodik GDPR po konzultaci s konzultantem GDPR a po projednání s předsedou soudu ohlásí tuto skutečnost dozorovému orgánu v souladu s čl. 33 nařízení. Pokud jde o porušení zabezpečení v rámci výkonu soudních pravomocí, ohlásí se tato skutečnost pověřenci pro ochranu osobních údajů Nejvyššího

soudu. V ostatních případech nespadajících do výkonu soudních pravomocí se hlásí tato skutečnost Úřadu pro ochranu osobních údajů. Pokud je to možné, učiní tak nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl.

(2) Je-li na základě posouzení podle odstavce 1 pravděpodobné, že porušení zabezpečení mělo za následek vysoké riziko pro práva a svobody fyzických osob, oznámí metodik GDPR v souladu s čl. 34 nařízení toto porušení bez zbytečného odkladu subjektu údajů. Oznámení subjektu údajů se nevyžaduje v případě, že je splněna kterákoli z následujících podmínek podle čl. 34 odst. 3 nařízení:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování,
b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví,
c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení, nebo podobného opatření.

ČÁST PÁTÁ
METODIK GDPR A KONZULTANT GDPR

Čl. 21
Postavení metodika GDPR

(1) Metodik GDPR vykonává úkoly v souladu s organizačním řádem VSOL a § 122d odst. 4 zákona o soudech a soudcích v platném znění.

(2) Metodikovi GDPR:

a) musí být umožněno, aby byl náležitě a včas zapojen do řešení záležitostí, které mají dopad na ochranu osobních údajů, jak zaměstnanců VSOL, tak externích subjektů,
b) musí mu být poskytnuty zdroje nezbytné k plnění jeho úkolů, zajištěn přístup k osobním údajům a operacím jejich zpracování a k prohlubování jeho odborných znalostí,

(3) Metodik GDPR plní úkoly orgánu dohledu dle § 122d odst. 4 zákona o soudech a soudcích, v platném znění. Při výkonu této působnosti je nezávislý, postupuje nestranně a řídí se pouze přímo použitelnými unijními právními předpisy a vnitrostátními právními předpisy.

(4) Vedoucí úseků a vedoucí oddělení jsou povinni metodikovi GDPR poskytovat při vykonávání jeho úkolů potřebnou součinnost.

Čl. 22
Postavení konzultanta GDPR

(1) Konzultant GDPR vykonává úkoly v souladu s organizačním řádem VSOL a § 122d odst. 1 a 2 zákona o soudech a soudcích v platném znění.

(2) Konzultantovi GDPR:

a) musí být umožněno, aby byl náležitě a včas zapojen do řešení záležitostí, které mají dopad na ochranu osobních údajů, jak zaměstnanců VSOL, tak externích subjektů,
b) musí mu být poskytnuty zdroje nezbytné k plnění jeho úkolů, zajištěn přístup k osobním údajům a operacím jejich zpracování a k prohlubování jeho odborných znalostí,

(3) Konzultant GDPR plní úkoly orgánu dohledu nad zpracováním osobních údajů (dále jen „orgán dohledu“) ve smyslu § 122d odst. 1 a 2 zákona o soudech a soudcích, v platném znění. Při výkonu této působnosti je nezávislý, postupuje nestranně a řídí se pouze přímo použitelnými unijními právními předpisy a vnitrostátními právními předpisy.

(4) Konzultant GDPR plní úkoly orgánu dohledu ve smyslu § 122d odst. 1 a 2 zákona o soudech

a soudcích v platném znění v případě sledování postupů krajských soudů.
(5) Vedoucí úseků a vedoucí oddělení jsou povinni konzultantovi GDPR poskytovat při vykonávání jeho úkolů potřebnou součinnost.

Čl. 23
Působnost metodika GDPR

(1) Metodik GDPR vykonává úkoly ve vztahu ke zpracování osobních údajů, nespadajících pod výkon soudních pravomocí[3], v rámci:
a) úseku kanceláře předsedy soudu,
b) úseku správy soudu,
c) úseku soudního výkonu a dozoru,
d) úseku soudních podatelen, archivu a knihovny,
e) úseku bezpečnostního ředitele.
(2) Metodik GDPR dále vykonává úkoly ve vztahu ke zpracování osobních údajů v rámci výkonu soudních pravomocí VSOL, jimiž se rozumí rozhodovací činnost a úkony s ní úzce související, na úseku trestním, občanskoprávním a insolvenčním a konkursním.
(3) Metodik GDPR při plnění úkolů podle odstavce 1 písm. e) nepřistupuje k utajovaným informacím.

Čl. 24
Působnost konzultanta GDPR

(1) Ustanovení čl. 23 ve vztahu ke konzultantovi platí obdobně s tím, že konzultant GDPR poskytuje součinnost metodikovi GDPR při výkonů jeho úkolů, a to zejména poradenstvím a konzultacemi.
(2) Konzultant GDPR při plnění úkolů nepřistupuje k utajovaným informacím.

Čl. 25
Úkoly a postupy metodika GDPR

(1) Metodik GDPR v rámci výkonu své působnosti a podle § 122d odst. 4 zákona o soudech a soudcích:
a) sleduje, zda postupy VSOL při zpracování osobních údajů jsou v souladu s unijními a vnitrostátními právními předpisy v oblasti ochrany osobních údajů,
b) přijímá podněty a prošetřuje skutečnosti v nich uvedené,
c) informuje subjekty údajů o způsobu jejich vyřízení, tak, aby předcházel ohrožení:
   - plnění úkolu v oblasti předcházení, vyhledávání a odhalování trestné činnosti a stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky, veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,
   - řízení o přestupku, kázeňském přestupku nebo jednání, které má znaky přestupku,
   - ochrany utajovaných informací, nebo
   - oprávněných zájmů třetí osoby.

(2) Zjistí-li metodik GDPR v souvislosti s výkonem své pravomoci nedostatky v postupu VSOL, vyrozumí o tom předsedu soudu a konzultanta GDPR, a společně s konzultantem GDPR uvede, jak je napravit.

[3] Tím se rozumí činnosti vytvářející předpoklady pro výkon soudnictví po stránce materiální, organizační a personální.

(3) Za účelem výkonu své působnosti orgánu dohledu je metodik GDPR oprávněn požadovat zpřístupnění soudních spisů, poskytnutí potřebných vysvětlení, vyjádření či jiných podkladů.

Čl. 26
Úkoly a postupy konzultanta GDPR

(1) Konzultant GDPR v rámci výkonu své působnosti:
a) konzultuje s metodikem GDPR, zda postupy VSOL při zpracování osobních údajů jsou v souladu s unijními a vnitrostátními právními předpisy v oblasti ochrany osobních údajů,
b) sleduje jako orgán dohledu, zda postupy při zpracování osobních údajů krajských soudů jsou v souladu s unijními a vnitrostátními právními předpisy v oblasti ochrany osobních údajů,
c) doporučuje přijetí organizačních a technických opatření v souvislosti s ochranou osobních údajů a jejich zpracováním,
d) poskytuje odborné konzultace v souvislosti s ochranou osobních údajů,
e) vede jednání s orgány dohledu a pověřenci a zapracovává jejich výtky do návrhů organizačních a technických opatření v souvislosti s ochranou osobních údajů a jejich zpracováním,
f) poskytuje poradenství metodikovi GDPR v případě žádostí nebo námitek dle čl. 27 a násl. této směrnice.

(2) Zjistí-li konzultant GDPR v souvislosti s výkonem své pravomoci podle odstavce 1 nedostatky v postupu VSOL, vyrozumí o tom předsedu soudu a metodika GDPR, a společně s metodikem GDPR uvede, jak je napravit.

(3) Za účelem výkonu své působnosti je konzultant GDPR oprávněn požadovat zpřístupnění soudních spisů, poskytnutí potřebných vysvětlení, vyjádření či jiných podkladů.

ČÁST ŠESTÁ
PRÁVA SUBJEKTŮ ÚDAJŮ

Čl. 27
Žádosti subjektů údajů

(1) Žádosti nebo námitky (dále jen „žádosti“), jimiž subjekt údajů uplatnil svá práva podle čl. 15 až 22 nařízení, vyřizuje metodik GDPR, jemuž poskytuje nezbytnou součinnost, zejména poradenství, konzultant GDPR.

(2) Žádosti lze podat v písemné formě poštou nebo elektronicky na adresu podatelna@vsoud.olc.justice.cz, prostřednictvím datové schránky, nebo osobně v úředních hodinách na podatelně VSOL. V ústní formě může subjekt údajů tuto žádost podat osobně v úředních hodinách po prokázání své totožnosti. Je-li možné ústní žádost vyřídit ihned, sepíše metodik GDPR o jejím vyřízení písemný záznam. V opačném případě se ústní žádost zaznamená a je vyřízena ve stejné lhůtě jako písemná žádost. Informace pro subjekty údajů, týkající se podávání žádostí, jsou uveřejněny na webových stránkách VSOL.

(3) Jestliže subjekt údajů podává žádost v elektronické formě, odpoví metodik GDPR na tuto žádost rovněž v elektronické formě, pokud subjekt údajů nepožádá o jiný způsob vyřízení, tj. písemně v listinné formě, nebo datovou schránkou.

(4) Pokud nebude možné zjistit nebo ověřit totožnost subjektu údajů ani po dodatečné výzvě, odmítne metodik GDPR takové žádosti vyhovět.

(5) Žádosti se zásadně vyřizují bezplatně. Pokud je žádost subjektu údajů zjevně nedůvodná nebo nepřiměřená (např.: opakující se), může metodik GDPR:
a) uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím

požadovaných informací, nebo
b) žádosti nevyhovět.

Čl. 28
Postup při vyřizování žádostí nespadajících pod výkon soudních pravomocí

(1) Metodik GDPR bez zbytečného odkladu po obdržení žádosti subjektu údajů nespadající do výkonu soudních pravomocí VSOL posoudí, zda subjekt údajů uplatňuje svá práva v souladu s nařízením.
(2) V případě, že shledá žádost subjektu údajů jako důvodnou, vypracuje k tomu písemné stanovisko, které po projednání s předsedou soudu předá věcně příslušnému vedoucímu zaměstnanci s pokynem předsedy soudu k provedení příslušných opatření, jimiž se žádosti subjektů údajů vyhovuje. Pokyn se uděluje na formuláři, který je přílohou č. 4 této směrnice.
(3) Opatření podle odstavce 2, kterými se vyhovuje žádosti subjektu údajů, spočívají:
a) ve sdělení potřebných informací pro výkon práva na přístup podle čl. 15 nařízení,
b) v provedení opravy podle čl. 16 nařízení nebo práva subjektu na výmaz podle čl. 17 nařízení,
c) v omezení zpracování podle čl. 18 nařízení (např.: znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění osobních údajů z webových stránek VSOL),
d) v provedení úkonů potřebných k výkonu práva na přenositelnost podle čl. 20 nařízení,
e) v zastavení zpracování osobních údajů na základě námitky subjektů údajů podle čl. 21 nařízení.
(4) Vedoucí zaměstnanec bez zbytečného odkladu a nejpozději do 7 pracovních dnů po obdržení pokynu předsedy soudu podle odstavce 2:
a) zajistí provedení požadovaných opatření a tuto skutečnost potvrdí na předaném pokynu, který vrátí metodikovi GDPR, nebo
b) zjistí-li, že nelze požadované opatření z technických důvodů provést, vrátí předaný pokyn, na kterém uvede tuto skutečnost, nebo
c) vyjádří nesouhlas s provedením požadovaných opatření, což uvede na předaném pokynu společně s důvody svého nesouhlasu, a takto vyplněný pokyn vrátí metodikovi GDPR.
(5) V případě nesouhlasu vedoucího zaměstnance podle odstavce 4 písm. c) se metodik GDPR obrátí na předsedu soudu s žádostí o rozhodnutí, jak dál v této věci postupovat.

Čl. 29
Postup při vyřizování žádostí spadajících pod výkon soudních pravomocí VS

(1) Metodik GDPR žádost subjektu údajů týkající se výkonu soudních pravomocí bez zbytečného odkladu předá vedoucímu příslušného soudního úseku k písemnému vyjádření. Vedoucí úseku ve svém vyjádření uvede, zda výjimku uvedenou v § 122e zákona o soudech a soudcích, kterou se omezí některá práva subjektu údajů:
a) lze aplikovat, nebo
b) nelze aplikovat a v takovém případě uvede, zda a v jakém rozsahu se má žádosti subjektu údajů vyhovět.
(2) V případě, že se výjimka podle 122e zákona o soudech a soudcích uplatní, postupuje se dále podle čl. 27 odst. 1 písm. a) této směrnice. Pokud se tato výjimka neuplatní a jsou splněny podmínky pro výkon práva subjektu údajů, metodik GDPR předá věcně příslušnému vedoucímu zaměstnanci pokyn předsedy soudu k provedení příslušných opatření uvedených v čl. 25 odst. 3 této směrnice, jimiž se žádosti subjektu údajů vyhovuje. Pokyn se uděluje na formuláři, který je přílohou č. 4 této směrnice. Dále se postupuje podle čl. 25 a 27 této směrnice.

Čl. 30
Vyrozumění subjektu údajů

(1) Metodik GDPR vyrozumí subjekt údajů o:
a) uplatnění výjimky pro omezení některých práv subjektů údajů podle 122e zákona o soudech a soudcích, nebo
b) o přijatých opatřeních podle čl. 25 nebo čl. 26 této směrnice, nebo
c) o důvodech nepřijetí opatření, o něž subjekt údajů požádal, a dále o skutečnostech uvedených v čl. 12 odst. 4 nařízení.

(2) Vyrozumění podle odstavce 1 zašle metodik GDPR bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení žádosti subjektu údajů. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce.

Čl. 31
Společná ustanovení

(1) V případě, že je na základě žádosti subjektu údajů proveden výmaz, oprava nebo omezení zpracování osobních údajů, informuje metodik GDPR v souladu s čl. 19 nařízení příjemce, jimž byly příslušné osobní údaje zpřístupněny, o provedení těchto úkonů, s výjimkou případů, kdy je to nemožné nebo to vyžaduje nepřiměřené úsilí. Pokud o to subjekt údajů požádá, informuje jej metodik GDPR o těchto příjemcích.
(2) Vedoucí úseků a oddělení jsou povinni poskytnout metodikovi GDPR součinnost při vyřizování žádostí subjektů údajů tak, aby je bylo možné vyřídit ve lhůtách stanovených nařízením.

ČÁST SEDMÁ
PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

Čl. 32
Závěrečná ustanovení

(1) Přílohy k této směrnici jsou udržovány v aktuálním stavu kontinuálně a jednotlivé položky se v nich doplňují bez nutnosti schválení celé směrnice.
(2) Za aktuálnost této směrnice odpovídá konzultant GDPR.
(3) V textu se pojmy zaměstnanec, soudce, ředitel, vedoucí apod. rozumí genderově neutrální označení, znamenající označení jak pro muže, tak pro ženy.

Čl. 33
Přechodná a zrušující ustanovení

(1) Evidence obsahující osobní údaje umožňující identifikaci subjektu údajů musí být uvedeny do souladu s čl. 5 této směrnice nejpozději do 6 měsíců od účinnosti této směrnice s výjimkou evidencí uvedených v čl. 5 odst. 1 písm. a) této směrnice.
(2) Tato směrnice nahrazuje Směrnici předsedy Vrchního soudu v Olomouci č. S 282/2021, o ochraně osobních údajů ze dne 11. 11. 2021.

Čl. 34
Účinnost

Tato směrnice nabývá účinnosti dnem 1. 11. 2022.

V Olomouci dne 17. 10. 2022

JUDr. Václav Čapka
předseda Vrchního soudu v Olomouci

Příloha č. 1 - Oznámení o bezpečnostním incidentu
Příloha č. 2 - Záznam o bezpečnostním incidentu
Příloha č. 3 - Záznam o porušení zabezpečení ochrany a posouzení následků
Příloha č. 4 - Pokyn k výkonu práv subjektu údajů a záznam o jeho provedení