



Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:

- a) náhodné nebo protiprávní zničení,
- b) ztráta,
- c) pozměňování,
- d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která:

- a) jedná z pověření správce nebo zpracovatele
  - b) má přístup k osobním údajům,
- zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

## Následující otázky se týkají praxe laboratoří obsluhujících praktické lékaře a ambulance

**Otázka č. 24: V rámci laboratorní dokumentace jsou vedeny karty pracovníků (např. v MS Word), kde jsou údaje osobní, o vzdělání, školení, prohlídkách, platovém zařazení atd. Lze je vést i nadále a za jakých podmínek? Je pro vedení takové dokumentace v laboratoři nově potřebný informovaný souhlas pracovníků?**

Odpověď:

*Je možné vést tyto údaje, vzhledem k tomu, že jde o povinnost stanovenou zákonem pro správce (dle zákoníku práce), ovšem opět je nutné zohlednit technická a organizační opatření k jejich zabezpečení.*

Právní stanovisko:

*Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a jsou zpracovávány osobní údaje pouze v odpovídajícím rozsahu:*

- a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- c) **zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;**
- d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.



## **Otázka č. 25: Změní nástup GDPR předávání dokumentace a výsledků mezi praxí lékařem a laboratoří?**

### Odpověď:

*Povinnosti se nemění, je potřeba zajistit bezpečnost jejich předávání vhodnými zárukami a odpovídajícími technickými prostředky. Nejen smluvními – předání musí být prováděno zabezpečenými cestami a nástroji a k těmto procesům by se měla vázat adekvátní analýza rizik a přijatá opatření k jejich minimalizaci. Otevřená komunikace elektronickou poštou (e-mailem) není bezpečnou cestou předávání citlivých údajů.*

*Smlouva mezi poskytovateli zdravotních služeb, kteří si předávají informace výlučně v rámci návazné péče, resp. spolupráce na zajištění zdravotní péče pacientovi, např. jak je to obvyklé mezi ambulancemi, nemocnicemi a laboratořemi, není povinná, ani nezbytná. Zároveň však jedním dechem dodáváme, že ji doporučujeme obzvláště v situacích, kdy opakovaně a dlouhodobě dochází k předávání osobních údajů, neboť si tak jednotliví poskytovatelé zdravotních služeb vymezí způsoby předávání osobních údajů a jejich ochranu, čímž přispějí k prevenci sporů a zároveň k zamezení neoprávněného přístupu k osobním údajům.*

### Právní stanovisko:

*Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:*

- a) pseudonymizace a šifrování osobních údajů;*
- b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
- c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
- d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*

*Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:*

- a) náhodné nebo protiprávní zničení,*
- b) ztráta,*
- c) pozměňování,*
- d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.*

*Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která:*

- a) jedná z pověření správce nebo zpracovatele*
  - b) má přístup k osobním údajům,*
- zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.*



Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

**Otázka č. 26: V laboratoři bývá na počítači adresář dodavatelů, servisů, jiných laboratoří, praktických lékařů z dané oblasti aj. Co je třeba učinit pro jeho zachování?**

Odpověď:

Je možné vést tyto údaje, vzhledem k tomu, že jde o běžné dodavatelské kontakty a kontakty spolupracujících subjektů. Ovšem opět je nutné zohlednit technická a organizační opatření k jejich zabezpečení.

Právní stanovisko:

Viz výše otázky 25 – 26.

**Otázka č. 27: V laboratoři je k dispozici „kniha výsledků“ (identifikace pacienta a jeho výsledky k odběru), může být v el. podobě i papírová. Bude možné ji nadále mít? A za jakých podmínek?**

Odpověď:

Laboratoř je poskytovatelem zdravotních služeb a na vedení těchto záznamů se vztahují stejná pravidla jako na primární zdravotnickou dokumentaci.

Právní stanovisko:

Ve smyslu ustanovení § 53 odst. 1 zákona o zdravotních službách je poskytovatel povinen vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle tohoto zákona a jiných právních předpisů. Podle odstavce 2 téhož ustanovení je zdravotnická dokumentace je souborem informací vztahujících se k pacientovi, o němž je vedena.

**Otázka č. 28: V informačním systému, v němž se řídí laboratorní dokumentace, jsou seznamy všech pracovníků, kteří mají k datům přístup se základní informací o nich. Je to nezbytné pro stanovení přístupových práv a sledování jejich práce s dokumenty. Nelze o ni kvůli GDPR přijít! – jak mají být tyto věci ošetřeny, aby laboratoř mohla pokračovat v činnosti?**

Odpověď:

Je nutné zavést taková opatření (organizační i technická), aby byly zmapovány všechny přístupy do informačního systému a uložené informace byly zabezpečeny. Smyslem GDPR není zakazovat vedení takové dokumentace, ale minimalizovat riziko zneužití a poškození práv subjektů údajů. Odpovědný správce dat pak musí být schopen doložit, že má zmapované, jaké osobní údaje vede, kde je vede, jak je zabezpečuje a jak kontroluje přístupy k nim.

Právní stanovisko:

Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;



- b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:

- a) náhodné nebo protiprávní zničení,
- b) ztráta,
- c) pozměňování,
- d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která:

- a) jedná z pověření správce nebo zpracovatele
  - b) má přístup k osobním údajům,
- zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

**Otázka č. 29: Je běžné a vstřícné ze strany laboratoře kolegům (lékařům) sdělit výsledky či další podrobnosti i telefonicky - někdy se ptají na předběžné (kultivační) výsledky, někdy nemohou papír najít, někdy je (ty zaslané) potřebují konzultovat. Co učinit, aby toto bylo nadále možné?**

Odpověď:

Pokud se komunikující strany vzájemně znají a spolupráce je dlouhodobě nastavena, není problém. Ovšem sdělovat citlivé údaje po telefonu neznámé osobě, bez smluvního zajištění a hesla, představuje riziko. Telefonické předání, vč. hesla pro tuto komunikaci, je vhodné upravit do smlouvy uzavíranou mezi lékařem a laboratoří, jako i další formy používané komunikace. Obecně musí být komunikace bezpečná a musí minimalizovat riziko zneužití a poškození práv subjektů údajů.

Právní stanovisko:

Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

- a) pseudonymizace a šifrování osobních údajů;
- b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;



d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:

- a) náhodné nebo protiprávní zničení,
- b) ztráta,
- c) pozměňování,
- d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která:

- a) jedná z pověření správce nebo zpracovatele
  - b) má přístup k osobním údajům,
- zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

**Otázka č. 30: V horské ordinaci je paní doktorka, která nemá a nebude mít počítač. Výsledky jí vozí kurýr, když jede pro odběry, nebo nosí pošta, když nelze jinak. Běžně jí laboratoř výsledky sděluje telefonicky. Jak to lze dělat i po květnu 2018?**

Odpověď:

Osobní i citlivé údaje je nutné předávat zabezpečenou formou. Telefonické předání, vč. hesla pro tuto komunikaci je vhodné upravit do smlouvy uzavíranou mezi lékařem a laboratoří. Obdobně takto může být ošetřena i jiná forma komunikace. Poštovní předání musí být adekvátně zabezpečeno, předávání osobní (kurýrem) proti prokázání totožnosti je rovněž možné.

Právní stanovisko:

Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

- a) pseudonymizace a šifrování osobních údajů;
- b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:

- a) náhodné nebo protiprávní zničení,



- b) ztráta,*
- c) pozměňování,*
- d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.*

*Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která:*

- a) jedná z pověření správce nebo zpracovatele*
  - b) má přístup k osobním údajům,*
- zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.*

*Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.*