

## **SMĚRNICE**

### **O ochraně osobních údajů**

# 1 Úvod

Tato směrnice je vydávána za účelem konkretizace povinností vyplývajících v Biotechnologickém ústavu Akademie věd České republiky, v. v. i. (dále jen „BTÚ“) z nařízení Evropského parlamentu a Rady EU č. 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“).

## 2 Základní pojmy

### Osobní údaje

Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“). Identifikovatelnou fyzickou osobu lze přímo či nepřímo identifikovat (odkazem na určitý identifikátor) – jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

### Zpracování osobních údajů

Jakákoli 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.

### Správce

Subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

### Zpracovatel

Subjekt, který zpracovává osobní údaje pro správce.

## 3 Základní zásady zpracování osobních údajů

Při zpracování osobních údajů je nutné dodržovat základní zásady uvedené v Nařízení.

- ve vztahu k subjektu údajů osobní údaje musí být zpracovávány korektně a zákonným a transparentním způsobem (**zákonnost, korektnost a transparentnost**)

- osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný, (**účelové omezení**),
- osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (**minimalizace údajů**),
- osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny (**přesnost**),
- osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány, (**omezení uložení**),
- osobní údaje musí být zpracovávány způsobem, který zajistí, náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření, (**omezení uložení**),
- osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (**integrita a důvěrnost**).

Základní zásady obsažené v Nařízení jsou základním vodítkem při zpracování osobních údajů a je potřeba z nich vždy vycházet při jakékoliv činnosti související se zpracováním osobních údajů. S osobními údaji je proto třeba zacházet pouze na základě právního důvodu, transparentně, se zřetelem ke stanovenému účelu zpracování, a pouze v nezbytném rozsahu.

### **3.1 Zpracování osobních údajů na základě právního titulu daného zákonem**

Jedná-li se o právní titul ke zpracování daný zákonem, je nutné se při posouzení oprávněnosti zpracování zaměřit na skutečnost, zda nejsou zpracovávány údaje nad rámec zákona (tedy zda zpracování všech dotčených údajů skutečně ze zákona vyplývá) a dále zda zpracovávání veškerých údajů, které se na základě právního titulu daného zákonem zpracovávají, je opravdu nezbytné v takovém rozsahu, ve kterém se zpracovávají.

### **3.2 Zpracování osobních údajů na základě souhlasu subjektu osobních údajů**

V případě zpracování osobních údajů na základě souhlasu subjektu zpracování je nutná kontrola všech náležitostí již udělených souhlasů subjektu a tedy souladu již udělených souhlasů s Nařízením. A dále je nutné precizně formulovat souhlasy nově udělované.

Mezi náležitosti souhlasu subjektu se zpracováním údajů patří především:

- konkrétní rozsah zpracovávaných údajů
- konkrétní účel (dostatečně určitý a legitimní)
- doba zpracování (konkrétní datum či doba určité činnosti)



Dostatečným souhlasem pro zpracovávání osobních údajů je svobodný, konkrétní, informovaný a jednoznačný projev vůle. Souhlas by měl být poskytnut písemně, tj. v podobě listinné nebo elektronické pro účely pozdějšího doložení souhlasu. Správce musí být po celou dobu zpracování údajů schopen doložit, že subjekt údajů souhlas udělal. V případě využití informačních systémů lze dovodit souhlas např. zaškrtnutím příslušného políčka v rámci informačního systému pro udělení souhlasu ke zpracování. Aby byl projev vůle považován za konkrétní, musí být naprosto jednoznačně definované, ke kterým údajům je udělován. Pro každý údaj musí být dohledatelné, byl-li k jeho zpracování poskytnut souhlas či nikoliv.

Dále je nutné přesně vymezit, na jakou dobu se souhlas poskytuje. Toto je možné stanovením konkrétního data, stanovením období, příp. stanovením určité činnosti. Dobu je nutné definovat tak, aby byl časový údaj pro každého srozumitelný a nezaměnitelný.

K udělení souhlasu se zpracováním osobních údajů subjekty zpracování nelze jakkoliv nutit. Souhlas se zpracováním může být subjektem zpracování kdykoliv odvolán. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

### **3.3 Zpracování osobních údajů na základě oprávněného zájmu správce**

Kritérium nezbytnosti zpracování určitých osobních údajů spočívá v posouzení, zda je možné daný proces realizovat bez zpracování těchto osobních údajů, aniž by toto vyžadovalo mnohem náročnější či nákladnější prostředky na základě provedení balančního testu.

Balanční test, tj. posouzení váhy oprávněného zájmu oproti zájmům nebo základním právům a svobodám subjektů údajů, je komplexním posouzením, které zahrnuje následující kroky:

- posouzení váhy oprávněného zájmu (např. zájem na zpracování údajů v rozsahu přesahujícím rozsah nezbytný pro plnění předmětu smlouvy, zajištění IT bezpečnosti, na snížení nákladů, na zamezení podvodnému jednání atd.),
- posouzení důsledků zpracování pro subjekty údajů:
  - posouzení veškeré přímé i nepřímé újmy, která může subjektům údajů vzniknout, včetně újmy, která jim může vzniknout následným jednáním třetí strany, např. po předání či zveřejnění osobních údajů; výsledek tohoto posouzení závisí na pravděpodobnosti, že určitá újma vznikne, a dále také na závažnosti této potenciální újmy;
  - zohlednění přiměřenosti osobních údajů, tj. v zásadě údaje nad rámec nezbytné identifikace těchto osob, pokud jsou takové údaje zpracovávány;
  - posouzení rozumných očekávání subjektů údajů
  - posouzení postavení BTÚ vůči subjektům údajů
- vyvážení oprávněného zájmu (tj. výhoda, která pro BTÚ ze zpracování plyne) s negativními důsledky zpracování (tj. s rizikem spočívajícím v pravděpodobnosti vzniku újmy a závažnosti vzniku újmy);
- v případě, že zájem subjektů nepřevažuje nad zájmem BTÚ, bude použit oprávněný zájem BTÚ jako právní titul pro zpracování osobních údajů; následně musí být přijata dodatečná organizační a/nebo technická opatření pro ochranu práv a svobod subjektů údajů.

### 3.4 Prověření náležitostí smluv a jejich úprava

Pro uvedení souladu veškerých činností s Nařízením je nutná kontrola uzavřených smluv, na základě nichž se zpracovávají osobní údaje externím dodavatelem a doplnění těchto smluv o konkrétní ustanovení (např. uzavřením dodatku ke smlouvě), dle přílohy č. 2 této směrnice, aby tak písemně byla stanovena pravidla zpracování osobních údajů dodavatelem (jakožto zpracovatelem) v souladu s Nařízením.

Při uzavírání nových smluv je nutné ustanovení dle přílohy č. 2 této směrnice včlenit přímo do smlouvy, příp. uzavřít s dodavatelem samostatnou Smlouvu o zpracování osobních údajů, která bude obsahovat ustanovení dle přílohy č. 2 této směrnice a bude na ni v oblasti zpracování osobních údajů navázána původní smlouva (např. smlouva o dílo).

Ve smlouvě mezi správcem a zpracovatelem musí být vždy jednoznačně stanoven předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů a veškeré povinnosti a práva správce a zpracovatele.

Doba trvání zpracování by měla být vždy totožná s dobou platnosti smlouvy, protože po skončení platnosti zpracovatel údaje vrátí zpět správci, nebo bude mít povinnost je vymazat.

Pojmem povaha osobních údajů se rozumí údaj, jak se tyto údaje budou zpracovávat, tj. zda písemně, či elektronicky – to se týká nejen zpracování samotného, ale i získávání údajů od subjektů údajů.

Účelem bude konkretizace potřeby zpracování osobních údajů. Typem osobních údajů lze rozumět konkrétní identifikaci těchto údajů, jméno a příjmení, datum narození, RČ, číslo OP/či pasu, bydliště, kontakty, pohlaví, nemoci atd. Pod kategorií subjektu údajů patří, zda jde o dospělého, či dítě, zaměstnance, či studenta, pacienta, či další třetí osobu, smluvní stranu apod.

## 4 Přehled o rozsahu a struktuře zpracovávaných osobních údajů

Přehled o rozsahu a struktuře osobních údajů zpracovávaných v rámci BTÚ je obsažen v samostatném interním dokumentu BTÚ - **Soupis zpracovávaných osobních údajů**.

Tento dokument je členěn podle jednotlivých agend, v jejichž rámci jsou zpracovávány osobní údaje:

- Personální a mzdová agenda
- Stáže
- Účetní systém
- Pořádání konferencí
- Školení
- Publikační činnost
- Ubytovna
- Smlouvy
- Web
- Atestace
- Projekty
- Veřejné zakázky
- Práce s ionizujícím zářením



**Soupis zpracovávaných osobních údajů** obsahuje výčet činností, resp. dokumentů zpracovávajících osobní údaje v rámci jednotlivých agend. K jednotlivým kategoriím zpracovávaných osobních údajů jsou pak uvedeny další informace o tom, jak je nutno v daném případě dodržet základní zásady zpracování osobních údajů (odst. 2), informace o odpovědných osobách za zpracování předmětných osobních údajů a informace o způsobu ochrany těchto údajů.

V rámci BTÚ nesmějí být zpracovávány osobní údaje, které nejsou uvedeny v **Soupisu zpracovávaných osobních údajů**.

V případě, že vznikne potřeba zpracování dalších osobních údajů neuvedených v **Soupisu zpracovávaných osobních údajů**, je třeba neprodleně soupis doplnit.

Při zpracování osobních údajů používají příslušní pracovníci BTÚ **vzory souhlasů a dalších dokumentů**, které má BTÚ vypracovány pro vnitřní potřebu.

## 5 Práva subjektu údajů

### 5.1 Právo na výmaz

Nařízení upravuje tzv. právo subjektu být zapomenut (právo na výmaz). Tomuto právu subjektu odpovídá povinnost správce, který osobní údaj zpracovává, jej vymazat a informovat všechny další správce, kteří tyto osobní údaje zpracovávají o skutečnosti, že subjekt údajů žádá o výmaz veškerých odkazů na osobní údaje, jejich kopie či replikace. Základním právem subjektu údajů je právo na to, aby jeho údaje byly vymazány a nebyly dále zpracovávány, pokud již nejsou potřebné pro účely, pro které byly zpracovány, příp. pokud subjekt údajů odvolal svůj souhlas se zpracováním a neexistuje žádný další důvod pro zpracování, subjekt údajů, vznesl námitku proti zpracování osobních údajů, které se ho týkají nebo pokud je zpracování jeho osobních údajů v rozporu s Nařízením.

Nařízení stanoví povinnost správce vymazat nepřesné údaje a údaje, u nichž důvod zpracování již pominul. Obdrží-li správce žádost subjektu o výmaz osobních údajů, je povinen bez zbytečného odkladu zajistit výmaz, za předpokladu, že neexistuje jiný právní důvod pro zpracování a uchování osobních údajů.

### 5.2 Právo na omezení zpracování

Dále Nařízení upravuje tzv. právo subjektu na omezení zpracování, přičemž omezení může být dočasné nebo trvalé. Omezením se rozumí aktivita správce, který vyloučí příslušné údaje ze zpracování, např. přesunem do jiného systému, znepřístupněním vybraných osobních údajů, popř. jejich zvláštním označením. Toto omezení nastupuje v případě, že se subjekt údajů domáhá opravy osobních údajů, přičemž nelze ověřit, že jsou zpracované osobní údaje nepřesné, byla vznesena námitka proti zpracování a doposud nebyla posouzena, ale dále i např. v případě, že již odpadl důvod zpracování osobních údajů, ovšem subjekt údajů nesouhlasí s jejich likvidací. Omezené osobní údaje je možné zpracovávat jen se souhlasem subjektů. V případě, že odpadne důvod k omezení, tedy že bude rozhodnuto o námitkách či dojde k opravě osobních údajů, je správce povinen informovat subjekt údajů, který omezení požadoval, že dojde ke zrušení tohoto opatření. Omezením zpracování není možno rozumět úplný zákaz zpracování. Přestože došlo k omezení zpracování, je správce nebo zpracovatel oprávněn osobní údaje zpracovávat z důvodu určení, výkonu, obhajoby právních nároků (např. při vymáhání dluhů, škod nebo plnění ze smluv, např. pojistných).



### **5.3 Právo na přenositelnost údajů**

Dalším právem subjektu je právo na přenositelnost údajů – v případě zpracování osobních údajů na základě souhlasu či za účelem splnění smlouvy, pokud se zároveň provádí zpracování automatizovaně, má subjekt údajů právo získat osobní údaje, které se ho týkají ve strukturovaném, strojově čitelném formátu, příp. může správce požádat, aby jeho údaje byly takto poskytnuty dalšímu správci. Toto ustanovení se vztahuje pouze na údaje zpracovávané v elektronické podobě, kdy strukturovaným souborem se rozumí takový, v němž mohou softwarové aplikace snadno nalézt, rozpoznat a získat konkrétní údaje. Na žádost subjektů mohou být takové údaje předány i přímo mezi správci.

### **5.4 Právo subjektu vznést námitku**

Nařízení dále upravuje právo subjektu vznést námitku proti zpracování osobních údajů, a to především s ohledem na důvod zpracování. Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoliv vznést námitku proti zpracování osobních údajů, které se ho týkají. Správce osobní údaje nadále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů nebo pro určení, výkon nebo obhajobu právních nároků.

### **5.5 Právo subjektu na přístup k osobním údajům**

Každý subjekt údajů má právo na přístup k osobním údajům, které se ho týkají a měl by mít možnost toto právo snadno a v přiměřených časových odstupech uplatňovat. Informace o samotném zpracování údajů je zásadní pro následné ověření jeho zákonnosti. Správce musí subjektu údajů na jeho žádost kdykoliv poskytnout kopii zpracování osobních údajů. Za tento postup může účtovat přiměřený poplatek na základě administrativních nákladů. Preferovaná je však bezplatnost a elektronická forma. Subjekt údajů je oprávněn se kdykoliv obrátit na správce s dotazem, zda vůbec zpracovává jeho osobní údaje a získat o tom potvrzení.

### **5.6 Žádosti subjektu**

Subjekt se obrací na správce žádostí. Správce musí dát subjektům údajů možnost obracet se na něj elektronicky a také stejnou formou včas sdělit požadované informace, příp. informace o provedených opatřeních. Odpovědi na žádosti jsou poskytovány bez zbytečného odkladu, tedy v nejkratším možném termínu, nejpozději do jednoho měsíce od obdržení žádosti. Lhůtu pro odpověď je možné z oprávněných důvodů prodloužit až o dva měsíce, ale i v tomto případě je nutné o tom do jednoho měsíce od podání žádosti informovat žadatele a tento postup dostatečně odůvodnit. Záměrem Nařízení je poskytnout subjektům údajů efektivní nástroj ke komunikaci se správcem, příp. k obraně svých zájmů. Pro účely žádosti subjektu osobních údajů týkajících se osobních údajů a výkonu práv subjektu osobních údajů v souvislosti s Nařízením je vyhotoven formulář, který je přílohou č. 1 této směrnice a který usnadňuje subjektům údajů uplatnění svých práv vůči správci. Formulář je dostupný na webových stránkách BTÚ.

Správce nicméně není povinen provést veškerá opatření požadovaná ze strany subjektu údajů, např. pokud taková opatření nejsou technicky možná, nejsou v souladu se zákonem (subjekt např. požaduje výmaz svých údajů, třebaže ke zpracování existuje zákonný důvod). I v těchto případech je však nutné o tom, že nebudou přijata tato opatření, informovat subjekt údajů do jednoho měsíce od obdržení žádosti, tento postup náležitě odůvodnit a konkrétně popsat veškeré důvody k nepřijetí

opatření a hlavně informovat ve své odpovědi subjekt údajů o možnosti podat stížnost u dozorového orgánu či se domáhat ochrany svých práv u soudu.

Veškerá sdělení a úkony poskytované správcem musí být v souladu s nařízením bezplatné, ovšem v případech, kdy jsou žádosti podané subjektem údajů zjevně nepřiměřené nebo nedůvodné, např. opakují se či nesouvisí s činností správce, je správce oprávněn uložit za poskytnutí informace či uložení opatření přiměřený poplatek pokrývající administrativní náklady, příp. odmítnout žádosti vyhovět. Nepřiměřenost či nedůvodnost žádosti dokládá správce. Tento postup tak lze použít pouze v těch případech, kdy jsou výše uvedené podmínky splněny jednoznačně a správce je schopen tuto skutečnost (nepřiměřenost či nedůvodnost žádosti) prokázat. Lze doporučit maximální obezřetnost a krajní využívání tohoto institutu.

## 6 Zpracování zvláštních kategorií osobních údajů

Jedná se o údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém 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.

Do výše uvedených kategorií tak spadá celá škála citlivých osobních údajů. Primárně je zpracování těchto citlivých údajů zakázáno, s výjimkou případů, které stanoví právní předpisy nebo v případě poskytnutí výslovného souhlasu subjektu se zpracováním těchto údajů. V těchto případech lze doporučit přísnější kritéria pro udělení souhlasu – např. vlastnoručně či elektronickým podpisem podepsaný souhlas, potvrzovací email propojený s SMS zprávou, apod.

## 7 Záznamy o činnostech

Správce i zpracovatel jsou povinni vést záznamy o činnostech zpracování.

Povinné obsahové náležitosti záznamů o činnostech zpracování prováděných správcem jsou:

- jméno a kontaktní údaje správce
- účel zpracování
- popis kategorie subjektů údajů a kategorií osobních údajů
- kategorie příjemců
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci
- plánované lhůty pro výmaz kategorií údajů (pouze pokud je to možné)
- obecný popis bezpečnostních opatření (pouze pokud je to možné).



## 8 Odpovědnost správce

### 8.1 Obecná odpovědnost správce

Správce osobních údajů nese odpovědnost za to, že zpracovává osobní údaje člověka v souladu s Nařízením. Tuto odpovědnost nelze přenést na někoho jiného.

Správce tak musí mít přehled o tom, jaké osobní údaje zpracovává, na základě čeho je zpracovává a jakým způsobem je zpracovává. Správce je povinen přijmout veškerá možná opatření, která zajistí, aby bylo nařízení po celou dobu své účinnosti dodržováno. V případě BTÚ se jedná o **Soupis zpracovávaných osobních údajů** (odst.4.)

Při volbě opatření k zabezpečení osobních údajů je nutné zohlednit rozsah zpracování, kontext zpracování, účel zpracování a míru rizika zpracování pro člověka, jehož osobní údaje jsou zpracovávány a dále také přihlédnout k povaze osobních údajů. Zpracovány mohou být pouze takové údaje, které jsou pro daný účel zpracování nezbytné, a to pouze na nezbytně nutnou dobu.

Pokud externí subjekt jakýmkoliv způsobem zpracovává osobní údaje, je tento subjekt zpracovatelem. Správce je povinen dohodnout se pouze s takovým zpracovatelem, který je schopen zajistit dostatečnou ochranu práv člověka v souvislosti se zpracováním osobních údajů, tj. je schopen zajistit dodržení pravidel pro nakládání s osobními údaji dle Nařízení.

V příloze č. 2 této směrnice jsou uvedena konkrétní ustanovení týkající se zpracování osobních údajů, která musí být uvedena ve všech smlouvách uzavíraných v souvislosti BTÚ, na základě kterých dochází ke zpracování osobních údajů.

Správce je povinen poskytovat součinnost dozorovému orgánu a na vyžádání poskytovat informace, umožnit přístup k osobním údajům a přístup do prostor, v nichž správce působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů. Správce je rovněž povinen úřadu na vyžádání poskytnout své záznamy o činnostech zpracování osobních údajů.

Správce je vždy povinen pokusit se o co nejkompexnější zmírnění rizik úniku a zneužití osobních údajů, a to za pomoci např. kvalitního softwarového a hardwarového vybavení, které bude k uskladnění dat sloužit, popř. v šifrování či pseudonymizaci osobních údajů. Rovněž v případě práce s informačními systémy, které zajišťuje externí subjekt, je nezbytné smluvně zajistit, jakým způsobem (pokud vůbec) bude tento subjekt s údaji nakládat. I zde platí, že minimalizace zpracování osobních údajů přispívá k bezpečnosti tohoto zpracování. Dále je vhodné minimalizovat počet osob, které budou s osobními údaji pracovat a řádně je proškolit. Nezbytným opatřením ke zmírnění rizik je rovněž krátkodobost zpracování osobních údajů, tedy maximální zkrácení doby zpracování údajů, které snižuje riziko jejich úniku či zneužití.

### 8.2 Ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu

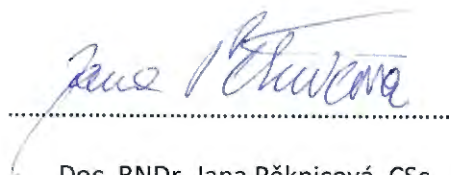
Nařízení dále zavádí novou povinnost správce i zpracovatele osobních údajů, a to ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu, bez zbytečného odkladu, nejdéle do 72 hodin od okamžiku, kdy se o tomto porušení správce dozvěděl, ledaže je nepravděpodobné, že by toto porušení mělo za následek vysoké riziko pro práva a svobody fyzických osob, přičemž tuto skutečnost musí být správce schopen doložit. V pochybnostech, zda porušení mělo či nemělo za následek riziko pro práva a svobody fyzických osob, lze doporučit ohlášení dozorovému orgánu preventivně učinit. Toto oznámení následně může vést k zásahu dozorového orgánu v souladu s

nařízením. Je třeba brát zřetel na skutečnost, že není-li jakékoliv porušení zabezpečení osobních údajů řešeno včas a náležitě, může to fyzickým osobám způsobit újmu.

### 8.3 Posouzení vlivu na ochranu osobních údajů

Mohou nastat situace, kdy správce či zpracovatel vyhodnotí, že určitý způsob zpracování bude mít riziko pro práva a svobody fyzických osob. V takovém případě provede správce či zpracovatel posouzení vlivu na ochranu osobních údajů s cílem vyhodnotit konkrétní pravděpodobnost a závažnost, pro zajištění ochrany osobních údajů a prokázání souladu postupu s nařízením. V pochybnostech o míře rizika lze doporučit posouzení vždy provést. Lze přistoupit i ke konzultaci s dozorovým orgánem – Úřadem pro ochranu osobních údajů, a to před samotným rizikovým zpracováním.

Posouzení provede zodpovědná osoba ve spolupráci se svým nadřízeným a pořídí o něm protokol.



Doc. RNDr. Jana Pěkníková, CSc.  
Ředitelka BTÚ

BIOTECHNOLOGICKÝ ÚSTAV  
AV ČR, v. v. i.  
Průmyslová 595  
252 50 Vestec

#### **Přílohy:**

Příloha č. 1 – Vzor žádosti subjektu

Příloha č. 2 – Podstatné náležitosti smlouvy v oblasti zpracování osobních údajů



**Správce osobních údajů:** Biotechnologický ústav AV ČR, v. v. i. se sídlem Průmyslová 595, 252 50 Vestec, IČO: 86652036 (dále jen „správce“)

**Subjekt osobních údajů:**.....

(dále jen „subjekt“)

Výše uvedený subjekt podává tuto

### ŽÁDOST

správci osobních údajů.

Subjekt žádá o:

**Výmaz** osobních údajů

specifikace osobních údajů.....

**Omezení zpracování** osobních údajů

specifikace osobních údajů.....

**Přenesení** osobních údajů

- subjekt žádá přenesení osobních údajů správcem k jinému správci  
specifikace jiného správce.....  
specifikace osobních údajů.....

- subjekt žádá výpis zpracovávaných osobních údajů, které se ho týkají

Subjekt vznáší **námítku** proti zpracování svých osobních údajů

specifikace osobních údajů, důvodu zpracování a odůvodnění námítky .....

Subjekt **odvolává** svůj souhlas ke zpracování osobních údajů

specifikace souhlasu (kdy a jak udělený), osobních údajů a důvodu zpracování .....

V ..... dne.....

## Náležitosti smlouvy v oblasti zpracování osobních údajů

Práva a povinnosti správce a zpracovatele mohou být široce vymezeny, ale v každém případě by ve smlouvě měla být obdoba dále uvedených ustanovení:

- „Bez předchozího písemného souhlasu správce není zpracovatel oprávněn přenést ani část svých povinností, vyplývajících z této smlouvy, na další třetí osobu (na dalšího zpracovatele). Pokud dojde k přenesení všech, nebo části povinností zpracovatele se souhlasem správce na třetí osobu, odpovídá zpracovatel za případnou škodu způsobenou touto třetí osobou tak, jakoby škodu způsobil sám, a to bez jakéhokoliv omezení.“
- Pokud bude ke zpracování osobních údajů třeba předchozí souhlas subjektu údajů, je třeba tuto skutečnost uvést do smlouvy – „Správce/zpracovatel se zavazuje získat souhlas se zpracováním osobních údajů dle této smlouvy od jednotlivých subjektů osobních údajů, jejichž osobní údaje budou dle této smlouvy zpracovávány.“
- „Zpracovatel se zavazuje zajistit všechna bezpečnostní, technická a organizační zabezpečení ochrany osobních údajů a jiná opatření požadovaná v čl. 32 Nařízení; zejména přijmout veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, jakož i jejich zneužití, včetně opatření týkajících se práce s informačními systémy, v nichž jsou tyto osobní údaje zpracovávány.

Zpracovatel se dále zavazuje:

- a) neužívat osobní údaje k jinému než stanovenému účelu podle této smlouvy a zpracovávat osobní údaje pouze na základě doložených pokynů správce s výjimkou těch případů, kdy tato povinnost je zpracovateli uložena přímo právním předpisem;
- b) učinit s odbornou péčí všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů a umožní kontroly, audity či inspekce prováděné správcem nebo jiným příslušným orgánem dle právních předpisů;
- c) s odbornou péčí dodržovat všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů;
- d) poskytnout správci bez zbytečného odkladu nebo ve lhůtě, kterou stanoví správce, součinnost potřebnou pro plnění zákonných povinností správce spojených s ochranou osobních údajů, jejich zpracováním a s plněním smlouvy o zpracování osobních údajů;
- e) informovat správce o všech skutečnostech majících vliv na zpracování osobních údajů;
- f) oznámit správci každou pochybnost o dodržování zákona či narušení bezpečnosti osobních údajů;
- g) bude-li to třeba, poskytnout správci veškerou podporu a pomoc při styku a jednáních s Úřadem pro ochranu osobních údajů a se subjekty údajů;
- h) neprodleně reagovat na žádosti subjektů, tyto informovat o všech jejich právech a na žádost umožnit přístup k informacím o zpracování;
- i) po ukončení poskytování služeb spojených se zpracováním dle potřeb správce řádně naložit se zpracovávanými osobními údaji, tj., všechny osobní údaje buď vymazat, nebo je vrátit správci, a to dle pokynu správce;



- j) dodržovat všechny ostatní povinnosti stanovené právními předpisy, i pokud tak není výslovně uvedeno ve smlouvě;
  - k) vynaložit veškeré možné úsilí na odstranění protiprávního stavu ve vztahu k převedeným osobním údajům dle této smlouvy, kterým by došlo k porušení povinností jedním příslušné smluvní strany, a to neprodleně poté, co taková skutečnost nastane.
- Veškeré informace obsahující osobní údaje, které si smluvní strany při realizaci této smlouvy poskytnou, jsou důvěrné. Zpracovatel se zavazuje, že tyto informace neposkytne třetí osobě ani je nepoužije v rozporu s účelem jejich poskytnutí za účelem splnění této smlouvy, není-li touto smlouvou stanoveno jinak. Zpracovatel se zavazuje, že neprozradí informace vztahující se k této smlouvě žádné další osobě a že tyto informace nikdy nepoužije k jinému než účelu stanovenému touto smlouvou, a to jak po dobu trvání této smlouvy, tak i po jejím ukončení (s výjimkou případů, kdy mu to přikáže právní předpis nebo, kdy se na tomto obě smluvní strany písemně dohodnou). Zpracovatel dále zajistí, aby se osoby oprávněné zpracovávat osobní údaje, zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.“

Za dodržování výše uvedených povinností a závazků zpracovatele bude nutno stanovit ve smlouvě smluvní pokuty a v případě opakování porušování ze strany zpracovatele i možnost na okamžité odstoupení od smlouvy.

V případě, kdy správce by byl sankcionován pokutou za porušení nařízení či zákona v oblasti ochrany osobních údajů v důsledku porušení povinnosti zpracovatele, je zpracovatel povinen nahradit pokutou vzniklou škodu správci.

Všechny dokumenty, které se týkají zpracování osobních údajů, ať již správcem a poskytnutých zpracovateli, nebo zpracovatelem samotným, musí být uloženy a archivovány na bezpečném místě, na adrese .....

V případě, že zpracovatel by byla zahraniční osoba, je nutné stanovit do smlouvy, že:

- všechny dokumenty a komunikace, týkající se zpracování osobních údajů a zajištění činností dle smlouvy, budou v českém jazyce a případné spory se budou řešit dle českého práva u soudu místně a věcně příslušného sídla správce. Rozhodčí řízení je vyloučené;
- I v případě, že smlouva bude uzavřena na dobu určitou, je účelné do smlouvy doplnit i možnost předčasné výpovědi smlouvy, a to pro případ, že dojde k pochybením ze strany zpracovatele, která sice nezaloží právo na odstoupení, ale přesto bude obezřetné smlouvu ukončit, popř. to bude pro správce ekonomicky výhodné, protože bude k dispozici jiný a lepší zpracovatel. Protože však výpověď by měla být reciproční, měla by se stanovit taková délka výpovědní doby, aby správce nebyl ohrožen při výpovědi ze strany zpracovatele.