Jabok – Vyšší odborná škola sociálně pedagogická a teologická
Jabok – Akademie für Sozialpädagogik und Theologie / Jabok – Institute of Social Pedagogy and Theology
Salmovská 8, 120 00 Praha 2, tel.: +420 211 222 440, fax: 211 222 441
e-mail: jabok@jabok.cz, www.jabok.cz

Č. j. Jabok/2019/0477

Řád o dodržování ochrany osobních údajů

na Jaboku - Vyšší odborné škole sociálně pedagogické a teologické

Tento vnitřní řád **Jaboku – Vyšší odborné školy sociálně pedagogické a teologické (**dále jen Jabok**), Salmovská 8, 12000 Praha,** (dále jen zaměstnavatel) upravuje zodpovědnosti a pravidla ochrany a zpracování osobních údajů zaměstnanců, studentů a partnerů školy.

Vyhotovil: Mgr. Eva Hernová	**Účinnost od:** **25.5.2018**
datum:	**podpis:** Dr. Ing. Alois Křišťan, Th.D., ředitel školy
S dokumentem se seznámili:	

Přehled změn dokumentu

Poř. č. vydání	Obsah změny	Platnost od	Změnu provedl
1	Nový dokument	25.5.2018	
2	Úprava dokumentu	25.4.2019	

OBSAH

1 Definice použitých pojmů a seznam zkratek

Pojem/zkratka	Význam
Anonymizované osobní údaje	Údaje, které ani nepřímo nepomáhají v identifikaci určitého člověka a nejsou s ním tedy nijak spojitelné
BCP	Business Continuity Planning - plán zajištění kontinuity ICT služeb
DPO	Data Protection Officer - Pověřenec pro ochranu osobních údajů
GDPR	General Data Protection Regulation - evropské nařízení k ochraně os. údajů (2016/679)
ZZOÚ	Zákon o zpracování osobních údajů č. 110/2019 Sb.
IA	Interní audit
ICT	Informační a telekomunikační technologie
IDM	Identity management – nástroj pro identifikaci a autorizaci uživatelů IT služeb
IS	Informační systém
NDA	Non-disclosure agreement - Dohoda o mlčenlivosti
OÚ	Osobní údaj
Pseudonymizace	Proces skrytí identity, jehož účelem je mít možnost sbírat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost
SOÚ	Subjekt osobních údajů
Správce OÚ	Subjekt, který určuje účel a prostředky zpracování osobních údajů ke stanovenému účelu
Zpracování OÚ	Jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ, 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.
Zpracovatel OÚ	Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Odpovídá správci OÚ za zpracování a ochranu dat dle dohodnutého smluvního vztahu.

2 Odpovědnosti a pravomoci

2.1 Dokument určuje povinnosti a zodpovědnosti správce osobních údajů (zastoupeného statutárním orgánem Jaboku - ředitel), DPO a všech dalších osob, které se podílejí na shromažďování, evidenci a zpracování osobních údajů.

3 Osobní údaje

3.1 Osobním údajem se rozumí každý údaj nebo jejich skupina, kterým lze jednoznačně identifikovat osobu.
Uložené/zaznamenané OÚ jsou souborem dat, tj. záznam údajů resp. jejich dílčích částí technickými či jinými prostředky, včetně záznamu OÚ na papírovém nosiči.

Zpracováním údajů rozumíme shromažďování, třídění, filtrování, kopírování (opisování) a vzájemné propojování dat.

3.2 Typové osobní údaje:
- údaje zvláštní kategorie/citlivé údaje (údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství, informace o zdravotním stavu, sexuální orientaci, biometrické a genetické údaje, soudní rozhodnutí, os. údaje dětí*.)*
- personální údaje pro různé evidence (jméno, příjmení, titul, data ve vztahu k osobě, rodinní příslušníci, mzdové a další finanční údaje, podpisové vzory, vzdělání a CV, přidělená evidenční čísla, vlastnictví majetku, apod., …)
- kontaktní údaje (adresy fyzické, elektronické a síťové adresy, tel. čísla, čísla průkazů, ID karet, …)
- přidělené konkrétní identifikovatelné technické prostředky (IT zařízení, MT, další vybavení)
- přidělené role v zaměstnaneckém či jmenovaném pracovním vztahu
- kamerové záznamy a záznamy hovorů, fotografie
- zahrnutí osoby do konkrétního seznamu, adresáře
- pravidelné aktivity osoby (pravidelné cesty, účast ve sportovním či skautském oddíle, hudebním tělese, mládežnické skupině apod., …)
- technické záznamy o aktivitách uživatele při využívání IT prostředků a nástrojů.

3.3 Osobní záznamy spojené s pracovní činností a pomocné soubory jednotlivých uživatelů jsou určeny pro účely daného zaměstnance, nejsou součástí zpracování OÚ na Jaboku a podléhají standardním postupům ochrany dat viz *Příloha č.3*.

3.4 Jabok k osobním údajům (jejich skupinám) eviduje informace o využití a zabezpečení těchto údajů:
- zodpovědnou osobu za OÚ nebo jejich skupinu – konkrétní odborný pracovník, dle spisu či dokumentu,
- kde (v jakém systému) jsou OÚ uloženy/zpracovávány,
- na základě jakého požadavku a k jakému účelu údaje OÚ jsou uchovávány,
- informace o zveřejnění, poskytování údajů mimo Jabok, který data získal a o mezinárodním předávání osobních údajů,
- zajištění ochrany OÚ (technická a organizační opatření),
- zda a případně jak je proveden souhlas osoby se zpracováním dotčených osobních údajů,
- způsob vedení evidence o činnostech zpracování údajů (např. dle mzdové agendy, či provozu IT systémů apod.).

3.5 Přehled zpracovávaných osobních údajů je uložen u DPO na Jaboku.

4 Správce osobních údajů

4.1 Správce OÚ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů. Správce rozhoduje o účelu a prostředcích zpracování osobních údajů, nese odpovědnost za jejich zpracování a jeho kontrolu.
Správcem mohou být veřejné orgány, místní samosprávy, podnikatelské subjekty nebo fyzické osoby, pokud rozhodují o účelu a prostředcích zpracování osobních údajů.

4.2 Správce osobních údajů je zastoupen statutárním orgánem (ředitelem) Jaboku.

4.3 Správce osobních údajů odpovídá:
- za jmenování DPO,

- za dodržování zásad zpracování OÚ a zavedení odpovídající ochrany IT systémů, včetně kontroly a posouzení použitých zabezpečení a za vedení dokumentace o zpracovávaných osobních údajích,
- za vedení evidence o činnostech zpracování údajů,
- za ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a za oznámení porušení zabezpečení osobních údajů SOÚ (smluvním partnerům a fyzickým osobám, jichž se údaje týkají),
- za prokazatelné proškolení zaměstnanců z oblasti ochrany osobních údajů a potřebných souvisejících procesů v organizaci,
- za bezpečné ukládání písemných dokumentů s OÚ,
- za zajištění podpisu dohod o mlčenlivosti (NDA) se zaměstnanci, kteří přicházejí do styku s osobními údaji při jejich zpracování (včetně procesů návrhu a testování IS).

4.4 Správce OÚ může pověřit zpracováním dat externího zpracovatele OÚ, který pak odpovídá za zpracování a ochranu dat dle dohodnutého smluvního vztahu. Vrcholová odpovědnost však zůstává na správci.

5 Zpracovatel osobních údajů

5.1 Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Odpovídá správci OÚ za zpracování a ochranu dat dle dohodnutého smluvního vztahu.

5.2 Jabok vystupuje v roli správce OÚ. Má uzavřeny zpracovatelské smlouvy, případně dohody s externími zpracovateli.

5.3 Při interním zpracování OÚ se Jabok řídí interními dokumenty a využívá interní procesy zajištění informační bezpečnosti a ochrany, ochrana OÚ je pravidelně kontrolována.

5.4 Pokud Jabok nezpracovává OÚ přímo vlastními prostředky, ale využívá dodavatele (externího zpracovatele OÚ), musí být zpracování OÚ externím zpracovatelem upraveno se písemnou smlouvou. Tato smlouva musí mít stanoven předmět, účel a dobu trvání zpracování, povinnosti a práva zpracovatele i správce OÚ.

5.5 Externí zpracovatel odpovídá Jaboku za zpracování a ochranu dat dle smluvního vztahu. Je vždy povinen vést evidenci zpracovávaných osobních údajů a plnit další náležitosti:
- disponovat dokumentací a postupovat podle dokumentace při zpracování dat a zajištění informační bezpečnosti,
- mít zpracován a podepsán závazek mlčenlivosti a poučení a to i pro své zaměstnance nebo i své další návazné dodavatele,
- disponovat dokumentací informačních systémů a IT služeb, kde dochází ke zpracování osobních údajů,
- provádět kontrolu dodržování zásad ochrany OÚ a postoupit na vyžádání výstupy těchto kontrol správci OÚ,
- na vyžádání správce OÚ a za přítomnosti správcem OÚ pověřených osob, provést mimořádnou kontrolu zajištění ochrany osobních údajů.

6 Pověřenec k ochraně osobních údajů (DPO)

6.1 DPO je jmenován správcem OÚ – ředitelem Jaboku dle zásad GDPR. Přitom musí správce OÚ zajistit, aby měl DPO možnost plnit úkoly efektivně.

6.2 DPO je při výkonu svých úkolů vázán mlčenlivostí v souladu s veřejnou legislativou i vnitřními dokumenty Jaboku.

6.3 Hlavním úkolem DPO je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími ze zákonných požadavků, provádění interních auditů, školení pracovníků, prosazování odstranění případných nedostatků a podílí se i na řízení celkové agendy interní ochrany dat.

6.4 DPO nenese osobní odpovědnost za nedodržování požadavků na ochranu osobních údajů. Tuto zodpovědnost má správce OÚ nebo příslušní zpracovatelé OÚ dle smluvního vztahu.

6.5 Z hlediska profesních kvalit DPO jsou potřeba vědomosti z oblasti legislativy ochrany osobních údajů, základní znalost činností a organizace Jabok a znalost operací zpracování a zavedení ochrany informací a dat.

6.6 DPO organizuje 1x ročně analýzu rizik zpracování OÚ.

7 Principy ochrany osobních údajů

7.1 Správce osobních údajů má odpovědnost:
- za dodržení zásad korektního a transparentního shromažďování, zpracování osobních údajů pouze za přiměřenými a legitimními účely (minimalizace údajů),
- odpovědnost za přijetí veškerých rozumných opatření k zajištění přesnosti a důvěrnosti zpracování a uchování osobních údajů po minimální potřebnou dobu („integrita a důvěrnost“),
- zodpovědnost za doložení nastavení a kontroly dodržování těchto zásad.

7.2 Přístup založený na riziku – zpracování OÚ musí brát v potaz povahu, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody SOÚ a tomu přizpůsobit i zabezpečení osobních údajů.

7.3 Základní požadavky ochrany osobních údajů:
- minimalizovat množství osobních údajů,
- minimalizovat dobu uložení osobních údajů,
- znát právní důvod (legitimní účel) zpracování osobních údajů.

7.4 Komplexní ochrana osobních údajů zahrnuje oblasti:
- právní – legislativní požadavky a jejich aplikace na Jaboku,
- procesní – nastavení procesů v organizaci tak, aby odpovídaly právním a bezpečnostním požadavkům,
- technologické – výběr a použití technologií na zajištění zpracování dat a podporu nastavených procesů,
- personální – školení a formace uživatelů v práci s osobními údaji – získávání a utvrzování bezpečnostních návyků.

7.5 Správce OÚ zajistí likvidaci osobních údajů SOÚ, jakmile pomine účel, pro který byly osobní údaje zpracovány v souladu s vnitřním dokumentem Jaboku „Spisový řád“ v době stanovené skartační lhůty. Výjimkou z likvidace jsou osobní údaje SOÚ uchovávané pro účely archivnictví.

7.6 Stručně jsou obecné požadavky zásad ochrany osobních údajů uvedeny v Příloze 1 tohoto dokumentu.

8 Podmínky shromažďování a zpracovávání osobních údajů

8.1 Základním nezbytným předpokladem je existence právního důvodu zpracování osobních údajů, kterým správce OÚ musí disponovat, aby mohl osobní údaje zpracovávat.

8.2 Osobní údaje lze zpracovávat pouze na základě:

- prokazatelného a informovaného souhlasu dotčených osob (zákonných zástupců):
  - s uvedením konkrétního účelu zpracování OÚ,
  - s možností kdykoli souhlas odvolat.
- pokud je zpracování nezbytné:
  - pro splnění právní povinnosti,
  - pro plnění úkolu veřejného zájmu,
  - pro plnění smlouvy,
  - pro ochranu životně důležitých zájmů SOÚ nebo jiné osoby,
  - pro účely oprávněných zájmů správce OÚ nebo třetí strany (pokud před nimi nemají přednost zájmy či základní práva a svobody SOÚ).
- zpracovávání osobních údajů pro jiný účel je možné pouze pokud:
  - existuje slučitelnost původního účelu s jiným účelem,
  - existuje vztah mezi původním a jiným účelem,
  - existují přiměřené okolnosti shromáždění osobních údajů,
  - jsou zváženy přiměřené důsledky zamýšleného zpracování,
  - je poskytnut systém vhodných záruk (šifrování nebo pseudonymizace).

8.3 V rámci evidence důvodů zpracování OÚ se důvody pro zpracování OÚ nekombinují, platí vždy závažnější důvod v pořadí: legislativní, nezbytné pro Jabok, souhlas SOÚ.

8.4 Posouzení důvodu zpracování OÚ je provedeno vždy při změně rozsahu zpracování nebo změně příslušných systémů zpracování OÚ nebo smluvně zajištěného zpracovatele.

8.5 Za posouzení odpovídá správce.

8.6 Systémy pro evidenci a zpracování OÚ mají zajištěno (organizačně nebo technicky) zaznamenávání práce s OÚ:
- zaznamenávání operací s osobními údaji včetně vyhledávání, čtení, editace, exportu do záznamu (u IT nástrojů - transakčního logu),
- zajištění vedení evidence případných souhlasů se zpracováním OÚ.

8.7 Technické záznamy o činnostech uživatele a využívání IT nástrojů a IS (logy) jsou zachovány po nezbytnou dobu z provozních, případně archivních důvodů dle technologie zálohování daného IT prostředí nebo příslušné části IS.

9 Oblast smluvních vztahů

9.1 S externími zpracovateli OÚ pro Jabok je ze strany Jaboku uzavřena smlouva o ochraně osobních údajů.

9.2 Smluvní dokumenty, případně jejich části, jsou zpracovávány a pravidelně prověřovány.

9.3 Osoby, které pracují se smluvními dokumenty, mají podepsánu dohodu o mlčenlivosti (NDA).

10 Knihovna na Jaboku

10.1 Knihovna Jaboku v Knihovním řádu Knihovny Jabok v článku IV přesně uvádí jaké OÚ zpracovává, za jakým účelem je zpracovává, kde je uchovává a po jakou dobu: https://knihovna.jabok.cz/cs/o-knihovne/knihovni-rad/uplne-zneni-knihovniho-radu.

11 Procesy v oblasti ochrany osobních údajů

11.1 Procesy v oblasti OÚ vycházejí z práv SOÚ:

- právo na přístup k OÚ
- právo na opravu OÚ
- právo na výmaz (právo být zapomenut)
- právo na omezení zpracování OÚ
- právo na přenositelnost OÚ
- právo vznést námitku

11.2 Povinné procesy, včetně interakce s dozorovým úřadem, jsou popsány v ***Příloze 2*** tohoto dokumentu.

11.3 Písemné žádosti SOÚ jsou přijímány sekretariátem Jaboku na adresu Salmovská 8, Praha 2, 12000. Následně jsou předány DPO k záznamu, ke kontrole a rozhodnutí a ke koordinaci přípravy odpovědi.

11.4 SOÚ musí být nejpozději do 30 dní informován o výsledku jeho žádosti nebo musí být informován o prodloužení lhůty o další 2 měsíce (60 dní). V případě prodloužení doby reakce musí být informován o dané skutečnosti s uvedením důvodů prodloužení i dozorový orgán.

11.5 V případě komunikace zpráv s osobními údaji elektronickou poštou lze tento komunikační kanál využít při poslání zašifrované zprávy (např. zip s heslem) a heslo je předáno jinou cestou (např. SMS).

11.6 Odpověď SOÚ i případnou informaci dozorovému úřadu zajišťuje DPO, podepisuje správce OÚ – ředitel Jaboku.

12 Zajištění bezpečného zpracování a ukládání osobních údajů

12.1 Papírové dokumenty, smlouvy a další dokumenty nesoucí OÚ, jsou uchovávány v zabezpečeném prostoru (kancelář, příruční spisovna a spisovna) s řízeným přístupem.

12.2 Bezpečné zpracování dat, zálohování dat i správa elektronických nosičů dat podléhají standardním postupům informační bezpečnosti viz ***Příloha č.3***.

13 Archivní data

13.1 Životní cyklus dokumentů a záznamů na Jaboku se řídí vnitřním předpisem „***Spisový řád***“.

13.2 Evidence OÚ v informačních systémech i písemných záznamech, které byly vytvořeny / přesunuty do jiného prostoru, včetně IT úložiště, za účelem archivace a dále se již nezpracovávají, nejsou zahrnuty do oblasti, kde lze realizovat případný výmaz dat nebo poskytovat výstupy pro SOÚ dle požadavků GDPR a ZZOÚ.

13.3 Archivní záznamy musí být označeny jako „archivní“ a slouží pro prokazování či dohledávání historicky proběhlých skutečností, ne již ke zpracování dat.

13.4 Zálohovaní provozních IT systémů musí být prováděno v režimu obnovy záložních médií tak, aby došlo k přemazání údajů na záložních médiích vždy nejpozději do 30 dní.

13.5 Zálohy osobních a pracovních souborů na uživatelských PC/NB jsou určeny pro účely daného zaměstnance, nejsou součástí zpracování OÚ na Jaboku a podléhají standardním postupům ochrany dat viz ***Příloha č.3***.

14 Školení k ochraně osobních údajů

14.1 Periodické školení pracovníků a zaškolení nových zaměstnanců a studentů k ochraně OÚ zajišťuje DPO. Pravidelná proškolení jsou s periodou 1x za 2 roky. Osnova školení k ochraně osobních údajů je v ***Příloze č. 4.***

14.2 Evidence školení je uložena na sekretariátu Jaboku. Součástí proškolení zaměstnanců je i opakované seznámení s dokumentací k ochraně OÚ.

15 Kontrola a audit

15.1 Procesy, jejich nastavení, řízení a dodržování jsou ověřovány DPO pravidelnými audity a to minimálně 1x ročně. Plán auditů připravuje DPO ve spolupráci s ředitelem Jaboku.

15.2 Na základě závěrů auditu a výstupů z analýzy rizik projedná DPO s vedením Jaboku odstranění případných nedostatků.

16 Přílohy

Číslo	Název
Příloha č. 1	Obecné požadavky zásad ochrany osobních údajů
Příloha č. 2	Procesy v oblasti ochrany osobních údajů
Příloha č. 3	Stručné požadavky zajištění informační bezpečnosti
Příloha č. 4	Osnova školení k ochraně osobních údajů

17 Související dokumenty

Označení	Název
Interní	
1	Organizační řád
2	Spisový řád
3	Pracovní řád
Externí	
Zákon č. 262/2006 Sb.	Zákoník práce ve znění pozdějších předpisů
Školský zákon 561/2004 Sb. a vyhl. 72/2005 přílohy 1-4	Školský zákon
Nařízení EU 2016/679	GDPR (General Data Protection Regulation) - o ochraně osobních údajů
Zákon č. 418/2011 Sb.	O trestní odpovědnosti právnických osob a řízení proti nim ve znění pozdějších předpisů

Zákon č.110/2019 Sb.	Zákon o zpracování osobních údajů

Příloha 1

Stručně obecné požadavky zásad ochrany osobních údajů

Ochrana osobních údajů

fyzické osoby mají právo:

- právo na přístup ke svým OÚ
- právo na opravu OÚ
- právo na výmaz (právo být zapomenut)
- právo na omezení zpracování OÚ
- právo na přenositelnost OÚ
- právo vznést námitku

Opatření a oznamování

Jabok musí:

- vést dokumentaci ke shromažďovaným, evidovaným a zpracovávaným osobním údajům
- chránit osobní údaje pomocí adekvátních bezpečnostních opatření
- uchovávat záznamy o aktivitách týkajících se zpracovávání dat
- ohlašovat dozorovému úřadu případy porušení zabezpečení osobních údajů
- dle potřeby získat souhlas se zpracováváním osobních údajů a zajistit jeho evidenci

Transparentnost

Jabok musí zavést pravidla, která:

- jasně upozorňují na shromažďování údajů
- vysvětlují, proč a kdy jsou zpracovávány osobní údaje
- definují pravidla uchovávání a mazání údajů

IT a školení

Jabok musí:

- zaškolit zaměstnance v oblasti ochrany a zabezpečení osobních údajů
- auditovat a aktualizovat svoje pravidla týkající se údajů
- zavést roli DPO (v případě citlivých údajů)
- spravovat své smlouvy v souladu s požadavky ochrany OÚ

Příloha 2

Procesy v oblasti ochrany osobních údajů

1. Procesy navázané na práva subjektů osobních údajů

1.1. Právo na přístup k OÚ

Právo získat od správce potvrzení, zda o SOÚ v roli žadatele zpracovává OÚ,

a pokud jsou zpracovávány, zajistit žadateli výpis OÚ s doplněnými informacemi:

- účely zpracování;
- kategorie dotčených OÚ;
- příjemci nebo kategorie příjemců, kterým OÚ byly nebo budou zpřístupněny;
- plánovaná doba, po kterou budou OÚ uloženy/případně určit kritéria ke stanovení této doby;
- veškeré dostupné informace o zdroji OÚ, pokud nejsou získány od SOÚ;
- že dochází k automatizovanému rozhodování, včetně profilování.

1.2. Právo na opravu osobních údajů

SOÚ má právo na to, aby správce bez zbytečného odkladu opravil nepřesné OÚ, které se ho týkají. S přihlédnutím k účelům zpracování má SOÚ právo na doplnění.

1.3. Právo na výmaz (právo být zapomenut)

SOÚ má právo na to, aby správce bez zbytečného odkladu vymazal OÚ, které se daného SOÚ týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

- OÚ již nejsou potřebné pro účely, pro které byly shromážděny nebo zpracovány;
- SOÚ odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
- SOÚ vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
- OÚ byly zpracovány protiprávně;
- OÚ musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo Členského státu, které se na správce vztahuje;
- OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Výše uvedené se neuplatní, pokud je zpracování nezbytné:

- pro splnění **právní povinnosti**;
- pro účely **archivace ve veřejném zájmu**, pro účely vědeckého či historického výzkumu či pro statistické účely;
- pro **určení, výkon nebo obhajobu právních nároků**.

1.4. Právo na omezení zpracování

Omezené zpracování se týká případů:

- SOÚ **popírá přesnost OÚ**, omezení zpracování je na dobu potřebnou k tomu, aby správce mohl přesnost OÚ ověřit;

- **protiprávní zpracování** a SOÚ odmítá výmaz OÚ a žádá místo toho o omezení jejich použití;
- správce již OÚ nepotřebuje pro účely zpracování, ale **SOÚ je požaduje pro určení, výkon nebo obhajobu právních nároků**;
- **SOÚ vznesl námitku proti zpracování**, omezení zpracování je po dobu, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody SOÚ.

Pokud bylo zpracování omezeno, mohou být tyto OÚ, s výjimkou jejich uložení, zpracovány pouze se souhlasem SOÚ nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu.

SOÚ, který dosáhl omezení zpracování dle bodů výše, je správcem předem upozorněn na to, že bude omezení zpracování zrušeno.

Omezení zpracování OÚ musí být zajištěno technickými prostředky tak, aby se na OÚ nevztahovaly žádné další operace zpracování a aby nemohly být změněny. Tato skutečnost, musí být jasně vyznačena (například označená oddělená záloha dat).

1.5. Právo na přenositelnost údajů

SOÚ má právo získat OÚ, které se ho týkají, ve **strukturovaném, běžně používaném a strojově čitelném formátu**, a právo předat tyto údaje **jinému správci**, aniž by tomu správce, kterému byly OÚ poskytnuty, bránil, a to v případě, že:

- týká se dat poskytnutých SOÚ ke zpracování Jaboku na základě souhlasu nebo na základě smlouvy;
- zpracování dotčených dat se provádí na Jaboku automatizovaně.

Právem uvedeným v předchozím odstavci nesmí být nepříznivě dotčena práva a svobody jiných osob.

1.6. Právo vznést námitku

SOÚ má právo kdykoliv vznést námitku proti zpracování OÚ, vč. profilování. Správce OÚ dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami SOÚ nebo pro určení, výkon nebo obhajobu právních nároků.

Pokud se OÚ zpracovávají pro **účely přímého marketingu (například i pozvánky na nějakou aktivitu)**, má SOÚ právo vznést kdykoli námitku proti zpracování OÚ, které se ho týkají, pro tento marketing (i profilování v rámci marketingu). Pokud SOÚ vznese námitku, nebudou již OÚ pro tyto účely zpracovávány.

Pokud SOÚ vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

SOÚ musí být na právo uvedené v předchozích odstavcích výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se SOÚ.

Jsou-li osobní údaje zpracovávány pro účely vědeckého či historického výzkumu či pro statistické účely, má SOÚ, z důvodů týkajících se jeho konkrétní situace, právo vznést námitku proti zpracování osobních údajů, které se ho týkají, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.

2. Ohlašování porušení zabezpečení OÚ

Jakékoli porušení zabezpečení OÚ **DPO bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl**, ohlásí **Dozorovému úřadu**. Pokud není ohlášení Dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Ohlášení musí přinejmenším obsahovat:

- popis povahy daného případu porušení zabezpečení OÚ včetně, pokud je to možné, kategorií a přibližného počtu dotčených SOÚ a kategorií a přibližného množství dotčených záznamů OÚ;
- jméno a kontaktní údaje DPO nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení OÚ
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení OÚ, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytovány postupně bez dalšího zbytečného odkladu.

Správce OÚ (CD-IS) dokumentuje veškeré případy porušení zabezpečení OÚ v nástrojích SD obdobně jako ostatní incident, přitom zadává kategorii informační bezpečnost. Při zadání incidentu se uvádí skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí Dozorovému úřadu umožnit ověření souladu.

2.1. Ohlašování porušení zabezpečení OÚ SOÚ

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek **riziko pro práva a svobody fyzických osob**, oznámí DPO toto porušení bez zbytečného odkladu i dotčenému SOÚ.

V oznámení určeném SOÚ se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení OÚ a uvedou se v něm přinejmenším informace:

- jméno a kontaktní údaje DPO nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení OÚ,

- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení OÚ, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

3. Interakce s dozorovým úřadem

Dozorový úřad je pověřen monitorováním uplatňování nařízení EU a ZZOÚ s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich OÚ.

3.1. Pravomoci dozorového úřadu

- nařídit správci a zpracovateli OÚ, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů;
- provádět vyšetřování formou auditů ochrany údajů;
- provádět přezkum;
- ohlásit správci nebo zpracovateli údajné porušení tohoto nařízení;
- získat od správce a zpracovatele přístup ke všem osobním údajům a ke všem informacím, které potřebuje k výkonu svých úkolů;
- získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů.

3.2. Nápravné pravomoci dozorového úřadu

- upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;
- udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;
- nařídit správci nebo zpracovateli, aby vyhověli žádostem SOÚ o výkon jeho práv podle tohoto nařízení;
- nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
- nařídit správci, aby SOÚ oznámil případy porušení zabezpečení osobních údajů;
- uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;
- nařídit opravu či výmaz OÚ nebo omezení zpracování a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny;
- uložit správní pokutu a nápravná opatření, podle okolností každého jednotlivého případu;
- nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

Příloha 3

Stručné požadavky pro ochranu OÚ

Z hlediska zajištění ochrany osobních údajů je nezbytné zajistit oblasti:

- Prokazatelné pověření pracovníků organizace do příslušných rolí – jmenovité určení zodpovědností za jednotlivé oblasti ochrany dat.

- Fyzickou a personální bezpečnost – zamezit neautorizovaném přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací a nastavení kroků ke snížení rizik vzniku lidské chyby, krádeže, podvodu nebo zneužití.

- Řízení přístupu k listinným dokumentům – zamezit neautorizovaném přístupu k listinným dokumentům ve stanoveném umístění (kancelář, archiv, kartotéka), vedení záznamu o převzetí dokumentu ke zpracování a o prováděných zásazích/doplnění do spisu.

- Řízení komunikací a řízení provozu – stanovit odpovědnosti, postupy pro řízení a správu IS, smluvní zajištění podpory provozu IT, zálohování, monitorování, správu sítě, bezpečnost médií a výměnu informací, ochranu před škodlivými kódy.

  Pravidla pro provoz a ukládání dat v uživatelských PC/NB.

- Řízení přístupu – zavedení autentizace a autorizace, rolí a práv k informačním systémům, zařízením a datům, správu certifikátů, politika hesel.

  Nastavení pravidel pro práci z domova.

- Řízení rizik a postup zvládání incidentů – nastavení postupů pro eliminaci rizik.

- Pravidelné kontroly – připravit plán kontrol dodržování nastavených pravidel a jejich souladu s legislativou.

Příloha 4

Osnova školení k ochraně osobních údajů na Jaboku

Ochrana osobních údajů

Typové osobní údaje

Citlivé osobní údaje

Podmínky shromažďování a zpracovávání osobních údajů

Správce osobních údajů

Správce osobních údajů – zodpovědnost

Zpracovatel osobních údajů

Externí zpracovatel osobních údajů

Pověřenec k ochraně osobních údajů (DPO)

Technická opatření na Jaboku k ochraně OÚ

Práva subjektů osobních údajů

OÚ při rozvázání pracovního poměru

Interní a externí legislativa k ochraně OÚ

Periodické školení pracovníků a zaškolení nových zaměstnanců k ochraně OÚ zajišťuje dle uvedené osnovy s přihlédnutím k dalším vnitřním řídícím dokumentům Jaboku DPO. Pravidelná proškolení jsou s periodou 1x za 2 roky.

Studenti jsou proškoleni při zahájení školního roku v rozsahu nezbytném pro jejich činnost dle uvedené osnovy. Školení zajišťuje DPO.