SMĚRNICE O OCHRANĚ OSOBNÍCH ÚDAJŮ

ČÁST první
Úvod

Tato směrnice je vydávána k zajištění postupu při zpracování a ochraně osobních údajů zaměstnanců i dalších osob a za účelem konkretizace povinností v Psychologickém ústavu AV ČR, v. v. i. (dále jen „PSÚ“) v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „GDPR“).

ČÁST druhá
Základní pojmy

1. Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě – subjektu údajů - zaměstnanci (dále jen Subjekt údajů).
   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.
2. Osobními údaji tak budou zejména:

   a) jméno, příjmení, adresa, datum narození/věk, pohlaví, rodné číslo, IČO, DIČ, číslo dokladu (OP, pas, řidičský průkaz), telefonní číslo, e-mailová adresa, státní příslušnost, SPZ;
   b) bankovní spojení, údaje z platební karty, údaje o externí lustraci (registr dlužníků apod.), číslo exekučního příkazu, číslo/údaje věrnostní karty;
   c) uživatelské jméno a heslo, IP adresa, geolokační údaje, data pro Internet tracking (cookies, local shared objects, web beacons, data pro device fingerprinting, atd.);
   d) vzdělání, rodinný stav, údaje o rodinných příslušnících (manžel, děti apod.);
   e) povolání, číslo zaměstnance;
   f) fotografie, zvukové, obrazové záznamy (např. tel. hovory, videonahrávky, záběry z kamer).
3. Podskupinou osobních údajů jsou **zvláštní kategorie osobních údajů** dle článku 9 GDPR (kam spadají například údaje o zdravotním stavu) a údaje o trestných činech dle článku 10 GDPR. Bližší informace o zvláštních kategoriích osobních údajů jsou obsaženy v části šesté tohoto interního předpisu.
4. **Za anonymní údaj** lze považovat takový údaj, který nelze přiřadit k identifikovatelné osobě, nebo jej nelze vztáhnout k žádnému subjektu údajů.
5. **Zpracováním osobních údajů** se rozumí 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.
6. **Subjektem osobních údajů (dále jen Subjekt údajů nebo zaměstnanec)** je každá fyzická osoba, jejíž osobní údaje jsou předmětem zpracování (GDPR se vztahuje pouze na osobní údaje fyzických osob, nikoliv právnických. GDPR se nevztahuje na osobní údaje zesnulých fyzických osob).

7. **Správcem osobních údajů (dále jen Správce nebo zaměstnavatel)** 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 (tj. osoba, která provádí operace zpracování osobních údajů). Odpovídá za zpracování osobních údajů. Správce musí mít řádný právní důvod pro zpracování osobních údajů, se kterými musí disponovat.
8. **Zpracovatelem** je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt (pověřený zaměstnanec), který zpracovává osobní údaje pro správce (správce jej pověří zpracováním osobních údajů pro něj). Zpracovatel sám může určit prostředky, avšak nikoliv účel zpracování.

ČÁST třetí
Základní zásady zpracování osobních údajů

Článek I.
Zásady zpracování

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

1. Osobní údaje musí být zpracovávány vždy korektně, zákonným způsobem a transparentním způsobem (zásada korektnosti, zákonnosti a transparentnosti).
2. Osobní údaje mohou být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely (zásada účelového omezení) a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný, (účelové omezení).
3. Osobní údaje musí být zpracovávány pouze přiměřeně a omezeně na nezbytný rozsah ve vztahu k účelu zpracování (zásada minimalizace).
4. 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 (zásada přesnosti).
5. Osobní údaje lze uložit ve formě umožňující identifikaci subjektu údajů pouze po nezbytně nutnou dobu pro účely, pro které jsou zpracovávány (zásada omezenosti uložení).
6. Při zpracování osobních údajů je nutno vždy náležitě zajistit zabezpečení osobních údajů pomocí technických a organizačních opatření tak, aby se zabránilo neoprávněnému či protiprávnímu zpracování, ztrátě, zničení nebo poškození osobních údajů (zásada integrity a důvěrnosti).

Článek II.
Odpovědnost za dodržování zásad zpracování

1. Vedoucí zaměstnanci a zaměstnanci pověření zpracováním osobních údajů jsou v souladu s GDPR odpovědni ve své působnosti za dodržování zásad zpracování osobních údajů uvedených v předchozím článku a jsou povinni kdykoliv toto dodržování souladu na vyžádání nadřízeného zaměstnance, nebo dozorového úřadu doložit.

ČÁST čtvrtá
Zákonnost zpracování

Článek I.
Přehled právních titulů pro zpracování

1. Aby zpracování osobních údajů bylo zákonné, je možné tyto údaje zpracovávat pouze na základě šesti právních titulů (právních základů zpracování) dle článku 6 GDPR:

    a) souhlas,
    b) splnění smlouvy,
    c) splnění právní povinnosti (např. zákona),
    d) pokud je to nezbytné pro ochranu životně důležitých zájmů,
    e) pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
    f) oprávněný zájem správce nebo třetí strany.

Ad a) 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 pozdější ho doložení souhlasu. Správce musí být po celou dobu zpracování údajů schopen doložit, že subjekt údajů souhlas udělil. 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.

Ad b) 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 kategorii subjektu údajů patří, zda jde o dospělého, či dítě, zaměstnance, či studenta, pacienta, či další třetí osobu, smluvní stranu apod.

Ad c) 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.

Ad f) 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.

ČÁST čtvrtá
Přehled o rozsahu a struktuře zpracovávaných osobních údajů

1. Přehled o rozsahu a struktuře osobních údajů zpracovávaných v rámci PSÚ je obsažen v samostatném interním dokumentu PSÚ – „Nařízení GDPR ve mzdové účtárně a personální oblasti“.
   Tento dokument je členěn podle jednotlivých agend, v jejichž rámci jsou zpracovávány osobní údaje.
2. 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 důvodech, pro které může zaměstnavatel provádět zpracování osobních údajů, informace o době uložení těchto údajů a informace o tom zda údaje ne/podléhají souhlasu zaměstnance z důvodu plnění povinností stanovených právním předpisem nebo oprávněných zájmů zaměstnavatele.
3. V případě, že vznikne potřeba zpracování dalších osobních údajů neuvedených v „Nařízení GDPR ve mzdové účtárně a personální oblasti“, je třeba neprodleně soupis doplnit.
4. Při zpracování osobních údajů používají příslušní pracovníci PSÚ vzory souhlasů a dalších dokumentů, které byly vypracovány pro vnitřní potřebu.

ČÁST pátá
Práva subjektu údajů

Článek I.
Žádosti subjektu

1. 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.
2. 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.
3. Pro účely žádostí subjektu 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 PSÚ.
4. Správce nemá povinnost přijmout opatření, o které subjekt údajů požádal, 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.

5. 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 činnosti 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.
6. Pokud organizace nemá pověřence, je třeba, aby tyto žádosti a uplatňování práv subjektů údajů vyřizovali zaměstnanci pověření konkrétním zpracováním osobních údajů a jejich vedoucí zaměstnanci, a to ve lhůtách uvedených výše.

Článek II.

1. Dle GDPR je každý subjekt údajů oprávněn uplatňovat u správce svá práva týkající se ochrany jeho osobních údajů. Správce je povinen výkon těchto práv subjektu údajů umožnit.
2. Jedná se o následující práva:
   a) právo na přístup k osobním údajům;
   b) právo na opravu osobních údajů;
   c) právo na výmaz osobních údajů,
   d) právo na omezení zpracování osobních údajů;
   e) právo vznést námitku proti zpracování
   f) právo na přenositelnost osobních údajů
   g) právo nebýt předmětem automatizovaného rozhodování, včetně profilování
   h) případně též právo odvolat souhlas se zpracováním osobních údajů.

Ad a) 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.

Ad b) Právo na opravu osobních údajů

Zaměstnanec má právo na opravu nepřesných osobních údajů, které se ho týkají. Pokud se subjekt údajů domnívá, že zaměstnavatel zpracovává nepřesné údaje, upozorní jej na to a zaměstnavatel je povinen opravu provést.

Ad c) 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.

Ad d) Právo na omezení zpracování

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 plný 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).

Ad e) 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.

Ad f) 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.

ČÁST šestá
Zpracování zvláštních kategorií osobních údajů

1. Dle článku 9 GDPR se obecně zakazuje zpracovávat zvláštní kategorie osobních údajů (dle zákona č. 101/2000 Sb., o ochraně osobních údajů, též citlivé údaje). Jedná se osobní údaje, které vypovídají o:
    a) rasovém či etnickém původu,
    b) politických názorech,

c) náboženském vyznání,
d) filozofickém přesvědčení,
e) členství v odborech,
f) genetických a biometrických údajích za účelem jedinečné identifikace fyzické osoby,
g) údajů o zdravotním stavu,
h) údajů o sexuálním životě nebo sexuální orientaci fyzické osoby.

GDPR nepovažuje národnost jako údaj, který spadá do této kategorie.

2. 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 udělený souhlas - např. vlastnoručně či elektronickým podpisem podepsaný souhlas, potvrzovací email propojený s SMS zprávou, apod.
3. Zákaz zpracování zvláštních kategorií osobních údajů se nepoužije v těchto případech (jinými slovy tyto údaje lze zpracovávat pouze v těchto případech):
   a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;
   b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
   c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
   d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
   e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
   f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí;
   g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;
   h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;
   i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých

přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

ČÁST sedmá
Záznamy o činnostech zpracování

1. Každý zaměstnavatel vede záznamy o činnostech zpracování, za něž odpovídá.
2. Záznam obsahuje tyto informace:
   a) Identifikace zaměstnavatele / Správce
   b) Účel zpracování
   c) Popis kategorií subjektů údajů (zaměstnanců) a kategorie osobních údajů
   d) Kategorie pověřených pracovníků (příjemců), kterým budou informace zpřístupněny
   e) Informace o předání osobních údajů do třetí země nebo mezinárodních organizacích
   f) Je-li to možné plánované lhůty pro výmaz jednotlivých kategorií údajů
   g) Je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.
3. Záznamy se vyhotovují písemně, včetně elektronické formy.
4. Zaměstnavatel poskytne záznamy na požádání dozorového úřadu (Úřad na ochranu osobních údajů).

ČÁST osmá
Odpovědnost správce

Článek I.

1. Obecná odpovědnost Správce osobních údajů nese odpovědnost za to, že zpracovává osobní údaje člověka v souladu s Nařízením. Tuto odpovědnost nelze přenést na někoho jiného.
2. 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 „Nařízení GDPR ve mzdové účtárně a personální oblasti“ (Samostatný interní dokument).
3. 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.
4. 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.

5. V příloze č. 2 této směrnice jsou uvedena konkrétní ustanovení týkající se zpracování osobních údajů, která musí být uvedena ve všech uzavíraných smlouvách, na základě kterých dochází ke zpracování osobních údajů.
6. 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.
7. Správce je vždy povinen pokusit se o co nejkomplexnější 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.

Článek II.
Jak postupovat v případě porušení zabezpečení

1. Postup správce v těchto případech upravují články 33 a 34 GDPR. Zaměstnanci mají povinnost neprodleně (tj. ihned) oznámit jakékoliv podezření či zjištění o porušení bezpečnosti svému nadřízenému a v případě, že je v organizaci jmenován pověřenec, též tomuto pověřenci
2. Správce - organizace musí ohlásit všechny tyto incidenty Úřadu na ochranu osobních údajů (dále jen „ÚOOÚ“) bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl. Pokud správce nestihne ohlášení ve lhůtě 72 hodin, při ohlášení uvede důvody zpoždění.
3. V případě e-mailové komunikace zaměstnanci oznamují porušení zabezpečení prostřednictvím zvláštního formuláře v Excelu – viz Příloha č. 3.
4. Zaměstnanec nebo zaměstnanci, kterým bylo porušení zabezpečení oznámeno, případně též pověřenec, prošetří oznámený incident a provedou jeho vyhodnocení.
5. Na základě posouzení incidentu zajistí zaměstnanci ohlášení porušení bezpečnosti dozorovému orgánu (dále jen „ÚOOÚ“) a v případě, kdy to bude dle GDPR potřeba, rovněž subjektu údajů. V případě, že se bude jednat o takové porušení zabezpečení, u kterého nevzniká povinnost jej ohlašovat nebo oznamovat, je povinností takový incident zaznamenat pro případ kontroly.
6. Příslušní zaměstnanci dále reagují na vyjádření ÚOOÚ a případně uvědomí postižené subjekty osobních údajů v případě, že to vyžaduje toto riziko nebo dozorový úřad. Rovněž zajišťují komunikaci s ÚOOÚ do uzavření incidentu. Všechny kroky a závěry je potřeba zdokumentovat.
7. Pověřený zaměstnanec v organizaci nebo pověřenec, je-li ustanoven, má povinnost vést záznamy o všech jemu oznámených bezpečnostních incidentech, ve kterých vedle skutečností požadovaných GDPR, zaznamenává také totožnost oznamovatele a skutečnost, zda bylo porušení zabezpečení oznámeno ÚOOÚ, subjektu údajů či nebylo oznámeno a z jakého důvodu. O těchto skutečnost podá zaměstnanci – oznamovateli a jeho nadřízenému zprávu.

8. Nesplnění povinnosti řádně porušení oznámit může vést až k uložení správní pokuty správci v souladu s článkem 83 GDPR.

Článek III.
Posouzení vlivu na ochranu osobních údajů

1. 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.
2. 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.
3. Posouzení provede zodpovědná osoba ve spolupráci se svým nad řízeným a pořídí o něm protokol.

Závěrečná ustanovení

1. Všichni zaměstnanci organizace, kteří zpracovávají osobní údaje, mají povinnost seznámit se s tímto interním předpisem. Seznámení těchto zaměstnanců zajišťují jejich vedoucí zaměstnanci. Pokud jde o seznámení se s postupy při zpracování a ochraně osobních údajů v organizaci, toto je zajišťováno pomocí školení. V případě, že je v organizaci jmenován pověřenec na ochranu osobních údajů, je toto zajišťováno tímto pověřencem, zejména formou školení a konzultací.
2. Zaměstnanci jsou povinni před schválením procesů, které by mohly mít vztah ke zpracování osobních údajů, před zahájením nového zpracování osobních údajů a při pochybnostech při uplatňování práv a povinností při zpracování a ochraně osobních údajů si vyžádat stanovisko osoby pověřené v organizaci ochranou osobních údajů.
3. Tento interní předpis nabývá účinnosti dnem 25. 5.2018.

prof. PhDr. Tomáš Urbánek, Ph.D.
ředitel Psychologického ústavu AV ČR, v. v. i.

Přílohy:
Příloha č. 1 -Vzor žádosti subjektu osobních údajů (výmaz, omezení zpracování, přenesení, námitka) a odvolání souhlasu ke zpracování osobních údajů
Příloha č. 2 - Podstatné náležitosti smlouvy v oblast i zpracování osobních údajů
Příloha č. 3 - Ohlášení porušení zabezpečení osobních údajů (OÚ)
a
Nařízení GDPR ve mzdové účtárně a personální oblasti“ (Samostatný interní dokument) s přílohami

Příloha č. 1

Žádost subjektu osobních údajů (výmaz, omezení zpracování, přenesení, námitka) a odvolání souhlasu ke zpracování osobních údajů

Správce osobních údajů:
Psychologický ústav AV ČR, v. v. i.
se sídlem Veveří 97, 602 00 Brno
IČ 68081740 (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 námitku** proti zpracovávání svých osobních údajů

specifikace osobních údajů, důvodu zpracování a odůvodnění námitky:
……
……

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

specifikace souhlasu (kdy a jak udělený), osobních údaj ů a důvodu zpracování:
……
……

V …….. dne ……..

……..

Příloha č. 2

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 jednáním 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 sídlu 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 výhodný, 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.

Ohlášení porušení zabezpečení osobních údajů (OÚ)

I. Informace o oznamovateli

Jméno a příjmení zaměstnance	
Divize	
Název útvaru/úseku/odboru	
Kontakt (e-mail, telefon)	
Jméno a příjmení nadřízeného zaměstnance	

II. Povaha incidentu

Čas a datum vzniku události:	
Čas a datum zjištění události:	
Typ porušení zabezpečení, vyberte: Krádež OÚ zaměstnancem, Krádež OÚ jinou osobou; Kybernetické narušení ochrany OÚ; Neoprávněné použití/zpřístupnění OÚ; Nedostupnost OÚ; Poškození/ztráta v úložišti OÚ; Ztráta nosiče s OÚ (papír, přenosné elektronické médium, mobilní zařízení)	
Stručný popis incidentu:	
Kategorie OÚ (vyberte): Běžné kategorie OÚ nebo Zvláštní kategorie OÚ (údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetika, biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci).	
O jaké jde osobní údaje (např. jména a příjmení, hesla, e-mailové adresy, údaje o mzdě nebo platu, o zdravotním stavu apod.)	
Množství OÚ:	
Kategorie dotčených subjektů údajů:	
(Přibližný) počet dotčených subjektů údajů:	
Jsou data čitelná neoprávněnými osobami? ANO/NE	
Specifikujte případně opatření, která byla přijata k ochraně dat:	
Případné důvody pro pozdní ohlášení:	