Institute of Biostatistics and Analyses

PRIVACY POLICY

Issued / vydáno dne: **2018-05-29**

Written by / vypracoval: **Mgr. Michaela Škrabalová**

Revised by / revidoval: **---**

Approved by / schválil: **Ing. Petr Brabec**

Version/verze: **QA.10.18.01**

Supersedes/nahrazuje: **---**

Valid from / platné od: **2019-05-29**

Document length / počet stran: **6**

Signature / elektronický podpis

Ing. Petr Brabec, Ph.D.

Digitálně podepsal Ing. Petr Brabec, Ph.D.
Datum: 2018.05.29 06:20:43 +02'00'

Registered e-document

Obsah

Zkratky

GDPR	Obecné nařízení o ochraně osobních údajů
IBA	Institut biostatistiky a anlýz
ICT	Informační a komunikační technologie
IS	Interní směrnice
OÚ	Osobní údaj
SÚ	Subjekt údajů
ÚOOÚ	Úřad pro ochranu osobních údajů

1. PRIVACY POLICY

Společnost Institut biostatistiky a analýz, s.r.o., se sídlem Poštovská 68/3, 602 00, Brno, IČO: 02784114, (dále jen "***IBA***") vnímá problematiku ochrany práv a svobod fyzických osob jako velmi zásadní a v dnešní době nezbytnou součást každodenního života jak v profesním, tak v soukromém životě.

Předmětem podnikání společnosti IBA je:

1) Provozování zdravotnických registrů.
2) Kompletní řízení a vedení NIS, včetně technického zázemí, data managementu a analýzy dat v rámci projektů v České Republice i v zahraničí.
3) Poskytování online služeb v podobě uložení dat na serverech IBA a jejich dalšího statistického zpracování dle požadavků zákazníka.

V rámci poskytování výše zmíněných služeb může docházet ke zpracování OÚ zaměstnanců, lékařů (investigátorů), klientů, ale i ke zpracování osobních a zvláštní kategorie (dále jen „citlivých") údajů pacientů.

Na základě nařízení 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 (General Data Protection Regulation = Obecné nařízení o ochraně osobních údajů) se vedení společnosti, zavazuje nakládat s osobními údaji svých zaměstnanců, obchodních partnerů i pacientů v důsledném souladu s tímto nařízením tak, aby nemohla být způsobena subjektům údajů žádná újma (nebo alespoň v maximální možné míře bylo omezeno riziko jejího vzniku) z hlediska zneužití, poškození, krádeže OÚ nebo jiného neoprávněného nakládání s nimi, způsobená při aktivitách souvisejících s výkonem pracovních činností ve společnosti, a učinit takové, kroky, aby ochrana osobních údajů na této úrovni byla důsledně dodržována v celé společnosti.

Společnost se zavazuje dodržovat základní principy GDPR ve vztahu k nakládání s osobními údaji, kterými jsou mj.:

- **Důvěrnost**
- **Dostupnost**
- **Integrita**
- **Odolnost**

Aby bylo možné zajistit důvěrnost, dostupnost, integritu a odolnost zpracovávaných osobních údajů, společnost zavádí a definuje veškeré procesy, při kterých ke zpracování dochází, formou interních směrnic. Všichni zaměstnanci, včetně externích dodavatelů služeb, podílejících se na zpracování OÚ musí být s těmito (pro ně relevantními) procesy prokazatelně seznámeni.

Kromě interních směrnic společnost disponuje také bezpečným systémem pro sběr dat CLADE IS, jehož zabezpečení se stále rozvíjí v souladu s požadavky mezinárodní normy ISO 27 001 Systém řízení bezpečnosti informací.

Vedení společnosti se dále zavazuje pravidelně kontrolovat dodržování stanovených zásad a procesů zaměstnanci. Pravidelné porušování a nedodržování zásad a pravidel stanovených v interních směrnicích týkajících se ochrany osobních údajů, nebo hrubé porušení či nedodržení těchto zásad a pravidel, může být vyhodnoceno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci zvlášť hrubým způsobem nebo jako závažné porušení, jež může vést k ukončení pracovněprávního vztahu příslušného zaměstnance. Zaměstnanci jsou seznámeni s tím, že společnost klade na důvěrnost, dostupnost, integritu a ochranu osobních údajů velký důraz a jsou poučeni o následcích nedodržování zásad a pravidel stanovených pro udržování vysoké úrovně ochrany osobních údajů.

Vedení společnosti se dále zavazuje do procesu zpracování OÚ zapojit pouze ověřené zpracovatele prokazující soulad s požadavky GDPR a současně tyto zpracovatele pravidelně kontrolovat, že jsou tyto požadavky a podmínky definované článkem 28 GDPR na zpracovatele dodržovány. V případě nedodržování podmínek sjednaných v rámci smlouvy o zpracování OÚ, či požadavků definovaných relevantními právními předpisy, bude spolupráce s takovými zpracovateli bezprostředně ukončena.

Vedení společnosti se zavazuje zajišťovat, a každý její zaměstnanec je povinen při výkonu práce nebo v souvislosti s ní respektovat, že při zpracovávání OÚ společností budou dodržovány zejména následující podmínky:

- Zpracování bude probíhat korektním, transparentním a zákonným způsobem.
- Zpracování bude prováděno pouze pro určité, výslovně vyjádřené a legitimní účely.
- Zpracování OÚ bude přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování.
- Zpracování OÚ bude probíhat jenom po dobu nezbytně nutnou, po uplynutí této doby budou OÚ zlikvidovány.
- Budou přijata taková technická a organizační opatření, aby nemohlo dojít ke zneužití, odcizení či poškození OÚ.

Vedení společnosti přijímá svou odpovědnost za zpracování osobních údajů. Stejně tak každý zaměstnanec společnosti je odpovědný za bezpečnost jím zpracovaných (zpracovávaných) OÚ.

Pro zajištění maximální bezpečnosti zpracovávaných informací je nutné identifikovat všechny kategorie a oblasti zpracovávaných OÚ a současně veškerých prostředků, které se na zpracování podílí. Tyto informace jsou předmětem dokumentu **Záznamy o činnostech zpracování OÚ**.

Pro zajištění maximální bezpečnosti OÚ je dále nezbytné identifikovat a ohodnotit rizika narušení bezpečnosti osobních údajů. K hodnocení rizik slouží **Analýza rizik**. Na základě výsledků analýzy rizik jsou přijata vhodná organizační a technická opatření s cílem snížit potenciální riziko na minimum. Proces řízení rizik je popsán v interní směrnici **Řízení rizik.**

Pro zajištění bezpečnosti je důležitá především:

- účinná prevence,
- včasná detekce,
- rychlá reakce.

Prevence je zajištěna nastavením systému a procesů při nichž ke zpracování OÚ dochází a proškolením všech zainteresovaných zaměstnanců/zpracovatelů na tyto postupy. Preventivní opatření vychází především z výsledků analýzy rizik.

Detekce – každý zaměstnanec podílející se na zpracování OÚ je seznámen s interní směrnicí **Řízení incidentů**. Jakmile získá zaměstnanec podezření na bezpečnostní událost/incident je dle této směrnice povinen tuto okolnost bezprostředně nahlásit odpovědné osobě.

Reakce – jakákoliv bezpečnostní událost/incident musí být bezprostředně po zjištění prošetřena a příčina incidentu musí být odstraněna tak, aby nemohlo dojít k dalším škodám. Veškeré relevantní informace týkající se bezpečnostní události/incidentu musí být náležitě zdokumentovány.

Podle výše uplatněného rizika na ochranu práv a svobod subjektu údajů a při dodržení podmínek stanovených relevantními právními předpisy (zejména GDPR) musí být o incidentu notifikován Úřad pro ochranu osobních údajů, popř. subjekt údajů.

Základní pravidla pro nakládání s osobními údaji včetně jejich procesování jsou uvedena v dokumentu **Směrnice o zpracování osobních údajů**. Interní směrnice obsahuje informace o základních zpracováních u společnosti, ale také práva subjektu údajů a jejich uplatnění.

Základní pravidla pro zajištění bezpečného prostředí jak fyzického, tak i kybernetického jsou popsána v dokumentu **Provozní řád**. Všichni zaměstnanci společnosti jsou povinni se těmito pravidly řídit, neboť právě lidské chyby jsou nejčastějším zdrojem bezpečnostních incidentů.

Přístup k OÚ uložených na firemních ICT zařízeních je řízen takovým způsobem, že každý zaměstnanec se může přihlásit do sítě pouze pod svým účtem. Přístup k OÚ je umožněn zaměstnancům pouze v takové míře, kterou potřebují k plnění svých pracovních povinností.

Změny týkající se procesních nebo technických prvků s vlivem na zpracování OÚ musí být vždy řádně zváženy a vyhodnoceny před tím, než je změna provedena. Je nezbytné zvážit profit a současně vyhodnotit možná rizika, včetně dopadu rizika na subjekt údajů. Konečné rozhodnutí o provedení změny vydává vedení společnosti. Celý proces včetně uskutečněné analýzy rizik s vyhodnocením potencionálního dopadu rizika na práva a svobody subjektu údajů musí být řádně zdokumentován.

Tato interní směrnice je pro jednotlivé zaměstnance společnosti závazná od okamžiku, kdy s ní byli seznámeni a své seznámení stvrdili podpisem.

1.1. Zpracování OÚ zaměstnanců

Osobní údaje zaměstnanců jsou zpracovány v souladu s interní směrnicí, přičemž všichni zaměstnanci jsou o rozsahu zpracování svých OÚ řádně informováni.

1.2. Zpracování OÚ pacientů

V rámci provozování zdravotnických registrů a studií na IBA může docházet ke zpracování osobních a citlivých údajů. Dle článku 9 GDPR je možné tyto údaje zpracovávat pouze za omezených podmínek.
OÚ o zdravotním stavu mohou být zpracovány na základě:

- plnění právních povinností zpracovatele vyplývajících zejména ze zákona č.372/2011 Sb., zákon o zdravotních službách, ustanovení § 2647 a násl. zákona č. 89/2012 Sb., občanský zákoník atd.…;
- poskytování pracovního a preventivního lékařství;
- výslovného informovaného souhlasu.

Pro účely vědeckého a statistického hodnocení v rámci studií/registrů je jedinou zákonnou možností zpracování osobních a citlivých údajů na základě **Výslovného informovaného souhlasu subjektu hodnocení.** Do registru tak nemůže být zapojen žádný pacient, který k tomuto neudělil výslovný souhlas.

Společnost IBA provozuje 3 typy registrů

1) **Registry obsahující čistě anonymní údaje** – osobní a citlivé údaje jsou v registru v plně anonymizované podobě pod unikátním číselným kódem (ID), kdy není možné pacienta v registru identifikovat.
2) **Registry s obsahem pseudonymních údajů** – pacienti jsou opět v registrech vedeni pod unikátním číselným kódem, a pacienty není možné v registru bez dodatečných informací jednoznačně identifikovat. K identifikaci je potřeba dodatečných informací. Na pseudonymní údaje se z hlediska GDPR pohlíží jako na údaje osobní.
3) **Registry s obsahem osobních údajů** – Rozsah zpracovávaných osobních údajů umožňuje jednoznačnou identifikaci pacienta.

Při zpracování OÚ vznikají dvě základní role:

1) Správce OÚ - určuje účel a prostředky zpracování
2) Zpracovatel OÚ - zpracovává OÚ na základě pokynů správce

V rámci provozování registrů je správcem OÚ pacientů primárně zadavatel studie tedy farmakologická společnost, odborná společnost, popř. IBA dle preferencí zadavatele.

Investigátoři/poskytovatelé zdravotnických služeb jsou v rámci registru zpracovatelé OÚ, vykonávající svou činnost na základě pokynů udělených správcem.

1.3. Zpracování OÚ investigátorů

V rámci provozování zdravotnických registrů dochází ke zpracování OÚ investigátorů, tedy spolupracujících lékařů, zadávajících data do registrů. OÚ investigátorů jsou zpracovávány v rozsahu nezbytném pro účely uzavření smlouvy, naplnění podmínek smlouvy a zřízení a vedení přístupů do elektronického systému dat.

Všichni spolupracující lékaři musí být o zpracování svých OÚ IBA řádně informováni.

1.4. Pověřenec pro ochranu osobních údajů

Společnost IBA zavádí roli Pověřence pro ochranu osobních údajů. Pravomoci a odpovědnosti pověřence jsou následující:

- poskytování informací a poradenství v oblasti ochrany osobních údajů zaměstnancům, kteří se na zpracování OÚ podílí;
- monitorování souladu s tímto nařízením a dalšími předpisy Unie nebo členských států v oblasti ochrany údajů;
- zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracovávání;
- poskytování poradenství na požádání;
- spolupráce a komunikace s dozorovým úřadem ÚOOÚ;
- komunikace a poskytování informací v oblasti ochrany osobních údajů spolupracujícím subjektům (uživatelé registrů, klienti, externí zpracovatelé OÚ) na mailové adrese **gdpr@biostatistika.cz**;
- příprava a aktualizace relevantní dokumentace, vedení záznamů;
- participace na řešení bezpečnostních incidentů a jejich hlášení dotčeným SÚ a ÚOOÚ.