Institute of Biostatistics and Analyses

PRIVACY POLICY

Issued / vydáno dne: **2019-08-20**

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

Revised by / revidoval: **Ing. Karla Henčlová**

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

Version/verze: **QA.10.19.03**

Supersedes/nahrazuje: **QA.10.18.02**

Valid from / platné od: **2019-08-27**

Document length / počet stran: **12**

Petr Brabec

Digitálně podepsal Petr Brabec
Datum: 2019.08.19 14:22:39 +02'00'

Signature / elektronický podpis

Registered e-document

Content/Obsah

Abbreviations

DS	Data Subject
GDPR	General Data Protection Regulation
IBA	Institute Biostatistics and Analyses
ICT	Information Communication Technologies
IEC	International Electrotechnical Commission
IS	Information System
ISO	International Organization for Standardization
NIS	Non-interventional Study
OPDP	Office for Personal Data Protection
PD	Personal Data

Zkratky

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

1. PRIVACY POLICY

The Institute of Biostatistics and Analyses Ltd. company, with headquarters in Poštovská 68/3, 602 00, Brno, ID: 02784114, (hereinafter referred to as '***IBA***') perceives the issue of protection of rights and freedoms of natural persons as greatly fundamental and as an essential part of everyday life today, both in professional and private life.

The scope of business of the IBA company entails:

1) Operation of medical registers.
2) Complete management and conduct of NIS, including technical structure, data management, and data analysis within the framework of projects in the Czech Republic and abroad.
3) Provision of online services in the form of data storage on IBA servers and its further statistical processing according to the customer's requirements.

In the framework of the provision of the above-mentioned services, processing of PD of employees, physicians (investigators), clients may occur, as well as the processing of personal data and the special category of data (hereinafter referred to as 'sensitive') of the patients.

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the management of the company undertakes to handle the personal data of its employees, business partners, and patients consistently in accordance with this Regulation in such a way that no damage is caused to the data subjects (or at least to limit the risk of its occurrence to the maximum extent possible) in terms of abuse, damage, theft of PD, or any other unauthorised treatment, caused by activities related to the performance of work activities in the company, and to take steps to ensure that the protection of personal data at this level is consistently observed throughout the company.

The company undertakes to comply with the basic GDPR principles in relation to manipulation with personal data, which are, among others:

- **Confidentiality**
- **Availability**
- **Integrity**
- **Resilience**

In order to ensure confidentiality, availability, integrity, and resilience of the processed personal data, the company introduces and defines all processes, during which processing takes place, through internal

directives. All employees, including external providers of services, involved in the processing of PD must be demonstrably familiar with these (to them relevant) processes.

In addition to internal directives, the company also has the CLADE IS secure system for data collection, the security of which is still being developed in accordance with the requirements of international standard ISO/IEC 27 001 Information Security Management System.

The management of the company further undertakes to regularly control the compliance with the set-out principles and processes by the employees. Regular violations and non-compliance with the principles and rules set out in in the internal directives related to personal data protection, or gross breach or non-compliance with these principles and rules, may be evaluated as a gross breach of the obligation resulting from employment-specific legislation or as a serious violation, which may lead to the termination of the employment relationship of the employee concerned. Employees are aware that the company places great emphasis on confidentiality, availability, integrity, and the protection of personal data, and they are advised on the consequences of non-compliance with the principles and rules set out for the sustenance of a high level of personal data protection.

The management of the company further undertakes to only engage certified processors into the process of PD processing who demonstrate compliance with the GDPR requirements, and at the same time, to regularly check these processors on the compliance with the requirements and conditions defined by Article 28 of GDPR. In the event of non-compliance with the conditions negotiated in the framework of the agreement on the processing of PD, or the requirements defined by relevant legal regulations, the cooperation with such processors will be immediately terminated.

The management of the company undertakes to ensure, and each employee is obligated to respect upon the conduct of work or in relation to it, that the following conditions are respected during the processing of PD by the company:

- Processing will be done in a correct, transparent, and lawful manner.
- Processing will be done only for specific, explicit, and legitimate purposes.
- Processing of PD will be reasonable, relevant, and limited to the extent necessary in relation to the purpose of the processing.
- Processing of PD will take place only for the time necessary, after which the PD will be disposed of.
- Such technical and organisational measures will be taken in order to avoid abuse, theft, or damage of PD.

The management of the company takes on its responsibility for the processing of personal data. Similarly, every employee of the company is responsible for the security of the PD processed (being processed) by him/her.

In order to ensure maximum security of the processed information, it is necessary to identify all categories and fields of the processed PD, and at the same time, of all the resources involved in the processing. This information is the subject of the document on **Records of PD Processing Activities**.

In order to ensure maximum security of PD, it is further necessary to identify and evaluate the risks of personal data security breaches. **Risk Analysis** is used to evaluate the risks. Based on the results of the risk analysis, appropriate organisational and technical measures are adopted to minimise the potential risk to a minimum. The risk management process is described in the internal **Risk Management** directive.

The following is especially important in terms of ensuring security:

- Effective prevention,
- Early detection,
- Fast response.

Prevention is ensured through the setting of a system and processes during which the processing of PD takes place and through the training of all engaged employees/processors on these procedures. Preventive measures are mainly based on the results of the risk analysis.

Detection – every employee involved in the processing of PD is familiar with the internal directive on **Incident Management**. Once an employee has a suspicion of a security event/incident, he/she is required under this directive to immediately report the matter to the person responsible.

Reaction – any security event/incident must be investigated immediately upon detection and the cause of the incident must be removed so that no further damage can occur. All relevant information regarding a security event/incident must be duly documented.

Depending on the level of the risk involved regarding the protection of rights and freedoms of the data subject and upon compliance with the conditions set out by the relevant legal regulations (GDPR in particular), the Office for Personal Data Protection, or the data subject, must be notified about the incident.

The basic rules on the handling of personal data, including its processing, are set out in the **Directive on Personal Data Processing** document. The internal directive contains information on basic processing at the company, but also the rights of the data subjects and their application.

Basic rules for ensuring a secure environment, both physical and cybernetic, are described in the **Rules of Operation** document. All employees of the company are obligated to follow these rules, since human errors are the most common source of security incidents.

Access to PD stored on corporate ICT devices is managed in such a way that each employee can only log into the network under his/her account. Access to the PD is only available to employees to the extent they need to fulfil their work responsibilities.

Changes concerning process or technical elements influencing the processing of PD must always be duly considered and evaluated before the change is made. It is necessary to consider the profit, and at the same time, to evaluate the possible risks, including the impact of the risk on the data subject. The final decision on the change is issued by the management of the company. The whole process, including the carried-out risk analysis along with an assessment of the potential impact of the risk on the rights and freedoms of the data subject, must be duly documented.

This internal directive is binding for the individual employees of the company from the time of their familiarisation and upon the confirmation of their familiarisation with their signature.

1.1. Processing of Employees' PD

The personal data of employees is processed in accordance with the internal directive, and all employees are properly informed of the extent of the processing of their PD.

1.2. Processing of Patients' PD

In the framework of operating medical registers and studies at IBA, the processing of personal and sensitive data may occur. Pursuant to Article 9 of GDPR, it is possible to process such data only under limited conditions.

PD about the health condition may be processed on the basis of:

- The fulfilment of legal obligations of the processor arising, in particular, from Act No. 372/2011 Coll., Act on Health Services, Provisions of Section 2647 et seq. Act No. 89/2012 Coll., the Civil Code, etc.;
- The provision of work and preventive medicine;
- Explicit informed consent.

For the purposes of scientific and statistical evaluation in the framework of studies/registers, the only legitimate possibility of processing personal and sensitive data is on the basis of an **Explicit Informed Consent of the Evaluation Subject**. Therefore, no patient may be involved in the register, who did not expressly consent to this.

The IBA company operates 3 types of registers

1) **Registers containing purely anonymous data** – personal and sensitive data are in the register in a fully anonymised form under a unique numeric code (ID), wherein it is not possible to identify the patient in the register.
2) **Registers containing pseudonymous data** – again, patients are kept in the register under a unique numeric code, and it is not possible to unambiguously identify the patients in the register without sufficient information. Additional information is required for identification. Pseudonymous data is considered as personal data in terms of GDPR.
3) **Registers containing personal data** – the extent of processed personal data allows for unambiguous patient identification.

There are two basic roles in the processing of PD:

4) PD Administrator – determines the purpose and means of processing

5) PD Processor – processes PD on the basis of the administrator's instructions

In the framework of operating registers, the sponsor of the study, i.e. the pharmacological company, professional company, or IBA according to the preferences of the sponsor, is primarily the administrator of the patient PD.

In the framework of the register, investigators/providers of medical services are the processors of PD, carrying out their activity on the basis of instructions given out by the administrator.

1.3. Processing of Investigators' PD

In the framework of operating medical registers, the processing of PD of investigators, i.e. cooperating physicians entering data into registers, takes place. The investigators' PD is processed in the extent necessary for the purposes of concluding an agreement, meeting the terms and conditions of an agreement, and establishing and maintaining access to the electronic data system.

All cooperating physicians must be properly informed on the processing of their PD by IBA.

1.4. Data Protection Officer

The IBA company introduces the role of the Data Protection Officer. The authority and responsibilities are as follows:

- Providing information and counselling in the field of personal data protection to employees who are involved in the processing of PD;
- Monitoring of the compliance with this regulation and other regulations of the Union or Member State in the field of data protection;
- Increasing awareness and professional training of workers involved in processing operations;
- Providing counselling upon request;
- Cooperation and communication with the OPDP supervisory authority;
- Communication and provision of information in the field of personal data protection to cooperating subjects (users of the register, clients, external PD processors) at the **gdpr@biostatistika.cz** e-mail address;
- Preparation and updates of relevant documentation, keeping of records;
- Participation in solving security incidents and their reporting to the DS and OPDP concerned.

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/IEC 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.