

Směrnice č. ORG/21

## Zpracování osobních údajů a pravidla jejich ochrany v souvislosti s evropským nařízením „GDPR“

Směrnice na zpracování a ochranu osobních údajů aplikuje v praxi nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (v textu dále jako „GDPR“).

DEBRA ČR, z.ú. je správcem a jedním ze zpracovatelů osobních údajů několika různých okruhů fyzických osob, níže rozepsaných a specifikovaných, a to na základě různých právních titulů, specifikovaných dále a v jednotlivých přílohách směrnice. Výjimku tvoří oblast osobních údajů zpracovávaných na základě informovaného souhlasu subjektu osobních údajů.

### Vymezení pojmů:

**Osobní údaje** (dále OÚ) - jsou definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě. Mezi obecné OÚ patří jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresa a fotografie.

**Citlivé údaje** (dále CÚ) - údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení. Do kategorie citlivých údajů nařízení nově zahrnuje genetické, biometrické údaje a osobní údaje dětí.

Úprava nařízení GDPR chrání pouze osobní údaje žijících fyzických osob a nevztahují se na údaje právnických osob, nebo údaje fyzických osob spojené s výkonem jejich funkce nebo zaměstnání. Nařízení GDPR se také nevztahuje na osobní údaje zesnulých osob, nicméně ochranu vyžadují také údaje zesnulých, který by mohly vypovídat také o žijících osobách (např. údaje o dědičné nemoci) nebo údaje, které jsou chráněny jinými právními předpisy (např. zdravotnická dokumentace).

**Správce OÚ** - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.

**Zpracovatel OÚ** - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

### Další zpracovatelé osobních údajů pro DEBRA ČR:

- Zásilkovna s.r.o. (spolupráce na zasílání objednávek charitativního e-shopu)
- Česká pošta s.p.
- Účetní software POHODA

- Program NUTRI DATA
- Instructor
- Revizor GINKGO účetnictví s.r.o.
- Auditor 22HLAV
- Administrátoři webu, DEBRA evidence, úložiště dat v organizaci
- Kontrolní orgány na základě zákonného pověření (např. MPSV, ČSSZ,...)

### Obecné zásady práce s osobními údaji

**Zákonnost** – konkrétní činnost je založená na právním titulu zpracování

**Korektnost a transparentnost** – informovat subjekty OÚ o způsobu zpracování

**Účelové omezení** – používat OÚ jen za účelem, za kterým byly získány

**Minimalizace údajů** – pouze omezeně nezbytný rozsah OÚ

**Přesnost** – povinnost zpracovávat přesné a aktualizované OÚ

**Omezení uložení** – po dobu nezbytně nutnou s ohledem na účel zpracování

**Integrita a důvěrnost** – zabezpečení před neoprávněným či protiprávním zpracováním (únikem) a před náhodnou ztrátou, zničením či poškozením

**Odpovědnost správce** – správce OÚ nese odpovědnost za celkový soulad s GDPR

### Stanovení pověření na ochranu osobních údajů

Zavedení pověření na ochranu osobních údajů dopadá na vymezené skupiny správců a zpracovatelů (viz. čl 37 a násl. GDPR). DEBRA ČR v této chvíli **nemá vymezeného pověření na ochranu osobních údajů**, a to do doby, než bude v ČR přijat adaptační zákon, který tuto povinnost blíže upraví. Nyní vycházíme z Doporučeného postupu č. 02/2018 vydaného Ministerstvem práce a sociálních věcí pro poskytovatele sociálních služeb.

### SOUHLAS SUBJEKTU SE ZPRACOVÁNÍM OÚ

Souhlas subjektu údajů se zpracováním OÚ je nezbytný v případě, neexistuje-li právní důvod zpracování osobních či citlivých údajů. V případě, kdy je nutno udělit souhlas subjektu OÚ (viz. příloha č. 1 – Katalog osobních údajů) souhlas musí být:

1. **svobodný a aktivní** – není akceptována volba předvyplněným tlačítkem
2. **konkrétní a jednoznačný** – pro jednotlivé účely či úkony zpracování musí být souhlas udělen jednotlivě;
3. **informovaný** – srozumitelná formulace souhlasu s uvedením vyžadovaných údajů o zpracování a s náležitým poučením o právech subjektu údajů
4. **„viditelný“ a „odlišitelný“** – pokud souhlas není udělován na samostatném dokumentu, měl by být dostatečně graficky oddělený, a tak odlišitelný od zbytku textu
5. **snadno odvolatelný** – odvolání souhlasu by mělo být stejně snadné, jako jeho udělení
6. **oddělitelný** – nesmí být spojován s jinými požadavky

V případě zpracování osobních údajů dětí ze strany správce, které vyžaduje souhlas se zpracováním osobních údajů, je pro určení osoby, která by souhlas měla udělit, rozhodující zejména úprava občanského zákoníku. Doporučuje se získat souhlas zákonného zástupce (rodiče, opatrovníka nebo pověřené osoby), a je-li dítě starší 15 let tak zároveň i souhlas dítěte, aby byly dostatečně ošetřené i jeho práva a zájmy coby dotčeného subjektu údajů.

DEBRA ČR využívá pro zpracování souhlasů GOOGLE Forms v rámci firemního účtu DEBRA ČR. Souhlasy jsou archivovány v zabezpečeném úložišti dat DEBRA ČR.

### **PROŠKOLENÍ PRACOVNÍKŮ DEBRA ČR V OBLASTI ZABEZPEČENÍ DAT**

Pracovníci DEBRA ČR byli podrobně seznámeni se směrnicí na ochranu osobních údajů, poučeni o způsobu zabezpečení jednotlivých OÚ. Jsou seznámeni s pravidly bezpečného užívání internetu, bezpečného stanovování hesel, bezpečného používání kancelářské počítačové techniky, e-mailového klienta, úložiště dat DEBRA ČR. Jsou si vědomi povinnosti nevynášet data žádnými způsoby, a to např. na externích discích, ústně, v tištěné podobě a nepřeposílat si data na soukromé e-mailové adresy či do soukromých telefonů. Pracovníci byli dále poučeni o způsobu archivace a ochrany tištěných fyzických dat v uzamykatelných schránkách a skříních. Pracovníci DEBRA ČR jsou tedy přímo odpovědní za dodržování ochrany osobních údajů všech dotčených subjektů OÚ, se kterými ti konkrétní pracovníci přicházejí do styku.

### **ANALÝZA RIZIK a JEJICH OŠETŘENÍ v RÁMCI ZPRACOVÁNÍ OÚ a CÚ**

Analýza rizik osobních údajů a nápravná opatření (příloha č. 2) přímo navazuje na vytvoření katalogu osobních údajů (příloha č. 3). Analýza rizik bude revidována minimálně 1x ½ roku. V okamžiku výskytu rizika a ohrožení OÚ je nutné vyhodnotit bezpečnostní incident a případně ohlásit porušení bezpečnosti či ohrožení osobních údajů.

### **HLÁŠENÍ PORUŠENÍ BEZPEČNOSTI či OHROŽENÍ OSOBNÍCH ÚDAJŮ**

V případě porušení bezpečnosti či ohrožení osobních údajů je nezbytné tuto skutečnost okamžitě nahlásit řediteli/ředitelce organizace. Vedení organizace musí respektovat oznamovací povinnost dle nařízení „GDPR“ a hlásit tuto skutečnost na předepsaných formulářích (příloha č. 3 a 4) nejpozději do 72 hodin Dozorovému úřadu (Úřadu na ochranu osobních údajů).

### **PRAVIDLA PRO NÁKLÁDÁNÍ S OSOBNÍMI ÚDAJI v ORGANIZACI**

#### **1) Nakládání a zpracování osobních údajů klientů/uživatelů sociální služby**

Tato pravidla se vztahují na zájemce o službu i klienty/uživatele sociální služby. Cílovou skupinou sociální služby jsou osoby s nemocí motýlích křídel a jejich rodinní příslušníci.

#### **Právní titul zpracování**

Osobní a případně citlivé údaje klientů je nutné zjišťovat a evidovat z důvodu poskytování sociální služby dle zákona č. 108/2006 Sb. a prováděcí vyhlášky č.

505/2006 Sb., z důvodu dlouhodobé koncepční a kvalitní práce s klienty, ale také např. jako prevence zdravotních rizik v případě náhlého zhoršení zdravotního stavu klienta.

### Elektronická data a jejich zabezpečení

Osobní údaje uživatelů služeb jsou evidovány v evidenčním programu „DEBRA evidence“, do kterého mají přístup pouze pracovníci přímé péče DEBRA ČR a ředitel DEBRA ČR (případná kontrolní funkce). Pro ukládání dat o uživatelích/klientech je využit Microsoft-SQL server poskytovaný platformou AZURE. Je vybráno umístění dat v EU. A) connection string je v aplikaci šifrovaný. Přístup k datům je možný pouze pomocí webové aplikace debra-evidence a to jen přihlášeným uživatelům.

### Zabezpečení přihlášených uživatelů je docíleno pomocí Microsoft Identity

Nový uživatel musí být zadán již aktivním uživatelem systému debra-evidence. Není tedy možné se libovolně přihlásit. K ověření identity je využito Google OAuth2 provider. Uživatelé jsou tedy vázáni na vlastnění účtu u GOOGLE, který organizaci spravuje e-mailovou komunikaci a není třeba dalších opatření. Přístup k účtu Azure organizace DEBRA má pouze ředitelka organizace.

### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba. Pořizování fotografií Obecně je možné pořizovat fotografie, na kterých nelze osoby identifikovat, v opačném případě je nutné získat souhlas osob i uchování a používání takových fotografií pro potřeby organizace DEBRA ČR. V souhlasu jsou jasně specifikovány jednotlivé účely využití fotografií. Klient/uživatel má možnost vybrat z nabízených možností jen ty, se kterými souhlasí. Souhlas je tedy konkrétní s výčtem všech možností prezentace fotografií, které mohou nastat. Souhlas je odvolatelný, o čemž je klient/uživatel pracovníky DEBRA ČR informován.

## 2) Nakládání a zpracování osobních údajů zaměstnanců DEBRA ČR

### Právní titul zpracování

Zákon č. 563/1991 Sb., o účetnictví  
Zákon práce č. 262/2006 Sb.

### Elektronická data a jejich zabezpečení

Osobní údaje zaměstnanců jsou vedeny v účetním software POHODA, do kterého má přístup účetní/administrativní pracovníci a dále na sdíleném disku v organizaci.

### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží

se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

#### Pořizování fotografií

Pořizování fotografií zaměstnanců je prováděno s jejich souhlasem, jedná se o fotografie z akcí s klienty, z benefičních akcí a také fotografie zveřejněné na webu DEBRA ČR v kontaktních údajích. V souhlasu jsou specifikovány jednotlivé účely využití fotografií. Pracovník má možnost vybrat z nabízených možností jen ty, se kterými souhlasí. Souhlas je tedy konkrétní s výčtem všech možností prezentace fotografií, které mohou nastat. Souhlas je odvolatelný, o čemž je každý pracovník DEBRA ČR informován.

### 3) Nakládání a zpracování osobních údajů uchazečů o zaměstnání v DEBRA ČR

#### Právní titul zpracování

Oprávněný zájem – v případě sporů se zájemcem o zaměstnání. Data jsou archivována po dobu 1 roku od ukončeného výběrového řízení.

#### Elektronická data a jejich zabezpečení

Sdílený zabezpečený disk v organizaci, e-mailový klient pověřeného pracovníka, případně ředitele organizace.

#### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

### 4) Nakládání a zpracování osobních údajů dobrovolníků a praktikantů

#### Právní titul zpracování

Zákon o dobrovolnické službě č.198/2002 Sb.

Občanský zákoník č.89/2012 Sb.

Školský zákon č. 561/2004 Sb.

#### Elektronická data a jejich zabezpečení

Osobní údaje dobrovolníků a praktikantů jsou vedeny na sdíleném zabezpečeném disku a v emailovém klientovi koordinátorky praxí a dobrovolníků.

#### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

### Pořizování fotografií

Pořizování fotografií dobrovolníků a praktikantů je prováděno s jejich souhlasem, jedná se o fotografie z akcí s klienty, z benefičních akcí apod. V souhlasu jsou specifikovány jednotlivé účely využití fotografií. Subjekt OÚ má možnost vybrat z nabízených možností jen ty, se kterými souhlasí. Souhlas je tedy konkrétní s výčtem všech možností prezentace fotografií, které mohou nastat. Souhlas je odvolatelný, o čemž je každý subjekt OÚ informován.

### 5) Nakládání a zpracování osobních údajů individuálních dárců

#### Právní titul zpracování

Zákon č. 563/1991 Sb., o účetnictví

Zákon č. 586/1992 Sb., o dani z příjmu

Občanský zákoník č. 89/2012 Sb.

#### Elektronická data a jejich zabezpečení

Osobní údaje individuálních dárců jsou vedeny v účetním software POHODA a na sdílených zabezpečených discích organizace, případně v e-mailovém klientovi ředitelky organizace či účetní/administrativní pracovnice.

#### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

### 6) Nakládání a zpracování osobních údajů účastníků benefičních akcí

#### Právní titul zpracování

Nabídky benefičních akcí jsou rozesílány osobám na e-mailovou adresu pouze na základě souhlasu uděleného speciálně pro tento účel. K udělení souhlasu byl využit GOOGLE Form.

Zveřejnění fotografií z akce je činěno na základě oprávněného zájmu, a to dokladování realizace akce pro zúčastněné a využití finančních prostředků, výše výtěžku. Jedná se o hromadné fotografie z akcí, na které není souhlas potřebný.

Cílené detailní fotografie - na základě souhlasu osoby uvedeno jméno a fotografie osoby předávající případný šek s vybranou částkou z akce.

#### Elektronická data a jejich zabezpečení

Fotografie z benefičních akcí i databáze kontaktů a souhlasů k nim jsou uloženy na sdíleném zabezpečeném disku.

### 7) Nakládání a zpracování osobních údajů členů orgánů DEBRA ČR, z.ú.

#### Právní titul zpracování



Občanský zákoník č.89/2012 Sb.

Zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob

### Elektronická data a jejich zabezpečení

Osobní údaje členů orgánů DEBRA ČR (zakladatelé, členové správní rady (včetně bývalých), statutární zástupce) jsou vedeny na sdíleném zabezpečeném disku a v e-mailovém klientovi ředitele organizace.

### Zabezpečení dat v písemné podobě

Všechny shromážděné údaje v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

## 8) Nakládání a zpracování osobních údajů na akcích DEBRA ČR (výroční konference, Galavečer DEBRA ČR, ozdravné pobyty)

### Právní titul zpracování

Oprávněný zájem – fotografie a prezenční listiny z akcí DEBRA ČR podpořených dotacemi či granty, které je nutné vyúčtovat a doložit konkrétní účast.

### Elektronická data a jejich zabezpečení

Fotografie z akcí jsou uloženy na zabezpečeném sdíleném disku organizace. S výjimkou klientů DEBRA ČR se jedná o hromadné fotografie bez nutnosti souhlasu. U klientů sociální služby řešeno samostatně souhlasem (blíže viz. bod. 1).

Prezenční listiny jsou uloženy v elektronické podobě na sdíleném zabezpečeném disku organizace.

### Zabezpečení dat v písemné podobě

Prezenční listiny z akcí v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

## 9) Nakládání a zpracování osobních údajů nakupujících na e-shopu DEBRA ČR

### Právní titul zpracování

Zákon č. 563/1991 Sb., o účetnictví Zákon č. 586/1992 Sb., o dani z příjmu  
Občanský zákoník č. 89/2012 Sb.

### Elektronická data a jejich zabezpečení

Data jsou evidována v účetním software POHODA a na zabezpečeném webu e-shopu DEBRA ČR. Data jsou zde uložena v databázi MySQL v hostingovém centru Wedos. Data nejsou nijak šifrována na disku, ale přístup k datům je možný pouze přes webové

rozhraní s protokolem HTTPS. Přístup má pouze správce e-shopu, účetní a administrativní pracovníci.

### Zabezpečení dat v písemné podobě

Stejnopisy faktur v písemné podobě jsou uschovány v uzamykatelné skříni v kanceláři DEBRA ČR. Kancelář je v době, kdy v ní pracovníci nejsou, zabezpečena mříží se dvěma zámky. Do areálu FN Brno, ve kterém se kancelář nachází, je vjezd/vstup prostřednictvím vrátnice, kde je zajištěna 24-hodinová služba.

