Informativní dokument

Přístup a zásady k ochraně osobních údajů v BorsodChem MCHZ, s.r.o.

Tento dokument prezentuje ochranu osobních údajů fyzických osob, práva a povinnosti při zpracování těchto údajů v souladu s nařízením EP a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen Nařízení EP) a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

I. Obecná vymezení

I. Zaměstnavatel je ve smyslu čl. 4 bodu 7) nařízení GDPR správcem osobních údajů.

II. Tento dokument upravuje zpracování a ochranu osobních údajů, které zaměstnavatel jako správce zpracovává o svých zaměstnancích a osobách, které se o zaměstnání ucházejí, fyzických osobách, které vstupují a pohybují se v areálu zaměstnavatele a fyzických osobách, které mohou vstoupit do obchodního vztahu.

Pro účely tohoto nařízení se rozumí:

I. „**osobními údaji“** veškeré informace o identifikované nebo identifikovatelné fyzické osobě (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;

II. „**zpracováním**“ jakákoliv 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;

III. „**omezením zpracování**“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

IV. **profilováním“** jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

V. **„pseudonymizací“** zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

VI. **„evidencí“** jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

VII. **„správcem“** fyzická nebo právnická osoba, který sama nebo spolu s jinými určuje účel, způsoby a prostředky zpracování osobních údajů;

VIII. **„zpracovatelem“** fyzická nebo právnická osoba, která zpracovává data jménem správce;

IX. **„příjemcem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

X. **„třetí stranou“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;

XI. **„souhlasem“** subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

XII. „**porušením zabezpečení osobních údajů“** porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

XIII. **„genetickými údaji“** osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

XIV. **„biometrickými údaji“** osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

XV. **„údaji o zdravotním stavu“** osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

XVI. **„závaznými podnikovými pravidly“** koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel sídlící na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.

II. Specifikace údajů a pojmů:

I. Osobním údajem je jakýkoliv údaj vztahující se k identifikované nebo identifikovatelné fyzické osobě. Takovými údaji jsou veškeré informace obrazové, slovní, rentgenové snímky, IP adresa, ve vztahu k danému obsahu (například jméno, adresa, pracovní pozice) nebo k identifikované či identifikovatelné osobě (specifické charakteristiky, nepřímá identifikace s přihlédnutím ke všem prostředkům - určitelnost, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu).

II. **Osobní údaje obecné** jsou: jméno, pohlaví, věk a datum narození, rodné číslo, osobní stav, občanství, IP adresa, fotografický údaj. Osobní údaje organizační jsou: pracovní nebo osobní adresa, pracovní nebo osobní telefonní číslo, pracovní nebo osobní email, ověřovací identifikační údaje, identifikační čísla vydaná státem.

III. **Citlivé osobní údaje** jsou údaje vypovídající o rasovém či etnickém původu, politickém postoji, náboženském nebo filozofickém vyznání, členství v odborových organizacích, zdravotním stavu a sexuální orientaci, trestních deliktech či pravomocném odsouzení. Patří zde rovněž genetické a biometrické údaje a osobní údaje dětí. Genetické údaje se vztahují ke zděděným nebo získaným genetickým charakteristikám, poskytující jedinečné informace o fyziologii nebo zdraví, nebo vyplývající z analýzy biologického vzorku. Biometrické údaje se vztahují k osobním údajům vyplývajícím z konkrétního technického zpracování, vztahující se k fyzickým, fyziologickým nebo behaviorálním charakteristikám, k těm, které dovolují nebo potvrzují jedinečnou identifikaci (například snímky obličeje nebo daktyloskopické údaje)

IV. Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.

V. BorsodChem MCHZ, s.r.o. (dále jen BC MCHZ) je správcem i zpracovatelem osobních údajů a je za ně odpovědný.

VI. Zveřejněným osobním údajem je osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

III. Zásady zpracování osobních údajů

I. Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem - **„zákonnost, korektnost a transparentnost“;**

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely - **„účelové omezení“;**

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány - **„minimalizace údajů“;**

d) 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 - **„přesnost“;**

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů - **„omezení uložení“;**

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením - **„integrita a důvěrnost“**;

2. Správce odpovídá za dodržení souladu s výše uvedeným.

IV. Zákonnost zpracování osobních údajů

1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek:

a) subjekt údajů udělil **souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů. Souhlas není nutný pro zpracování údajů na základě smlouvy, pro ochranu životně důležitých zájmů subjektu, pro splnění povinnosti správce nebo pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci (např. soukromé pojišťovny, zdravotnická zařízení)

b) zpracování je nezbytné pro splnění **předsmluvní fáze** a případné **smlouvy**, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění **právní povinnosti**, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve **veřejném zájmu** nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely **oprávněných zájmů příslušného správce**. Oprávněné zájmy správce nesmí převažovat nad zájmy nebo právy a svobodami subjektu údajů - **"rovnováha".**

2. **Zpracování citlivých dat (zvláštní kategorie osobních údajů)**

a) Je zakázáno zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

b) zpracování citlivých dat je možné pouze za předpokladu že:

- je udělen výslovný souhlas subjektu údajů,
- zpracování je nezbytné v oblasti pracovního práva, sociálního zabezpečení a sociální ochrany,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu, v případě, že subjekt není fyzicky nebo právně schopen souhlas udělit
- zpracování sleduje politické, filozofické, náboženské nebo odborové cíle - nadace, sdružení neziskové organizace,
- zpracování se týká údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro obhajobu právních nároků nebo v rámci soudního řízení,
- důvodného veřejného zájmu na základě EU nebo národního práva,
- pro účely preventivního lékařství, posouzení pracovní schopnosti zaměstnance, veřejného zájmu v oblasti veřejného zdraví,
- zpracování pro účely vědeckého, historického výzkumu nebo statistické účely.

V. Bezpečnost zpracování osobních údajů a jejich ochrana, porušení ochrany dat

1. Správce i zpracovatel je odpovědný za nastavení vhodných technických a organizačních opatření v úrovni zabezpečení, které odpovídá danému riziku, včetně

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti, zajištění, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

2. Z**áměrná a standardní ochrana osobních údajů**

a) Spočívá v zavedení jak v době určení prostředků pro zpracování, tak v době zpracování samostatných a vhodných technických a organizačních opatření, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.

b) Spočívá v zavedení vhodných technických a organizačních opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné (týká se množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti). Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

3. **Zabezpečení zpracování**

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

4. **Porušení ochrany osobních dat**

Porušením ochrany osobních dat se rozumí porušení bezpečnosti vedoucímu k náhodnému nebo nezákonnému zničení, ztrátě, změně, nepovolenému odhalení nebo přístupu. Porušení ochrany dat musí být oznámeno příslušnému Úřadu na ochranu osobních údajů do 72 hodin a také postiženým subjektům dat v případě vysokého rizika. V případě méně závažného porušení ochrany osobních dat rozhodne správce o způsobu přijetí opatření k nápravě a následnému zamezení podobného porušení a o takovém porušení vede písemný záznam. Zodpovědnou osobou pro podání oznámení Úřadu na ochranu osobních údajů a postiženému subjektu dat je výhradně interní auditor BC MCHZ (dále jen interní auditor).

4.1 **Náležitosti ohlášení úřadu**

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

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

4.2 **Náležitosti ohlášení správci**

a) popis povahy daného případu porušení zabezpečení osobních údajů;

b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, musí pověřená osoba interní auditor oznámit toto porušení bez zbytečného odkladu subjektu údajů.

V oznámení určeném subjektu údajů se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření stejně jako když se ohlašuje dozorovému úřadu

5. **Způsob a pravidla oznamování a ohlašování porušení ochrany dat**

Jakmile dojde k porušení ochrany osobních údajů, tedy k jakémukoliv bezpečnostnímu incidentu v této oblasti, činnosti nebo situaci v rozporu s touto směrnicí, je ten, kdo takové porušení zjistil nebo způsobil, povinen bezodkladně informovat správce (Interní audit nebo personální manažerka), který posoudí míru rizika a dopadu pro práva a svobody fyzických osob v souladu s Nařízení EP a rozhodne o způsobu řešení a opatřeních k nápravě a následnému zamezení podobného porušení. O veškerých takových porušeních vede písemný záznam.

6. **Chování a přístup k ochraně osobních údajů je zpracován s ohledem na**

a) spravedlivé a transparentní zpracování;

b) oprávněné zájmy správce;

c) shromažďování osobních údajů;

d) pseudonymizaci osobních údajů;

e) informace poskytované veřejnosti a subjektů údajů;

f) výkon práv subjektů údajů;

g) opatření a postupy týkající se odpovědnosti správce, ochrany osobních údajů a opatření k zajištění bezpečnosti zpracování;

h) ohlašování případů porušení zabezpečení osobních údajů dozorovým úřadům a oznamování těchto případů porušení subjektům údajů;

i) předávání osobních údajů do třetích zemí nebo mezinárodním organizacím; nebo

j) mimosoudní vyrovnání a jiné postupy pro řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním, aniž by byla dotčena práva subjektů údajů.

VI. Určení zpracovávaných osobních údajů

1. Ve vztahu ke svým zaměstnancům zpracovává zaměstnavatel osobní údaje, kterými jsou:

- jméno a příjmení (i rodné),
- datum a místo narození a rodné číslo,
- místo trvalého bydliště, případně jiné místo, kde zaměstnanec pobývá,
- číslo občanského průkazu nebo průkazu o povolení k pobytu,
- dosažené vzdělání a kvalifikace,
- státní příslušnost,
- počet nezletilých dětí a údaje o nich v souvislosti s uplatnění daňových slev a příspěvků na dětskou rekreaci,
- údaje o zdravotní pojišťovně,

- údaje o invaliditě (I. - III. stupeň),
- kontaktní údaje (email, telefon)
- a další údaje specifikované v bodě II. 2.

2. Ve vztahu k fyzickým osobám, které se ucházejí o zaměstnání, zpracovává zaměstnavatel osobní údaje, jimiž jsou:
   - jméno a příjmení,
   - dosažené vzdělání a kvalifikace,
   - kontaktní údaje (telefonní číslo nebo e-mailová adresa),
   - předchozí pracovní zkušenosti,
   - dosažené vzdělání.
3. Ve vztahu k fyzickým osobám, které vstupují a pohybují se v areálu zaměstnavatele
   - jméno a příjmení,
   - číslo pracovního, případně občanského průkazu nebo jiného dokladu totožnosti,
   - ročník narození.
4. Ve vztahu k fyzickým osobám, které mohou vstoupit se společností do obchodního vztahu
   - jméno a příjmení,
   - doklad totožnosti,
   - kontaktní údaje (telefonní číslo nebo e-mailová adresa),
   - místo trvalého bydliště, případně jiné místo, kde fyzická osoba pobývá
   - identifikační údaje společnosti.

VII. Práva subjektů údajů (zaměstnanec BC MCHZ nebo jiný subjekt údajů)

1. Subjekt údajů má **právo na poskytnutí** informací, které jsou o něm vedeny stručným, **transparentním**, **srozumitelným a snadno přístupným způsobem** za použití jasných a jednoduchých jazykových prostředků. Správce informace poskytne písemně nebo jinými prostředky, ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

2. Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má **právo** získat **přístup** (nahlédnutí) k těmto osobním údajům a k následujícím informacím:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovaná doba, po kterou budou osobní údaje uloženy,

e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) skutečnost, že dochází k automatizovanému zpracování, včetně profilování.

Správce poskytne kopii zpracovávaných osobních údajů ve formě, kterou je žádost podána, včetně elektronické. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů.

3. Subjekt údajů má **právo na opravu,** tzn. aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají.

4. Subjekt údajů má **právo na výmaz ("právo být zapomenut")**, tzn. aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;

c) subjekt údajů vznese námitky proti zpracování a neexistují žádné oprávněné důvody pro zpracování

5. Subjekt údajů **má právo na omezení** zpracování, tzn. aby správce omezil zpracování, v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

6. Subjekt údajů **má právo na přenositelnost** údajů, tzn. získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:

a) zpracování je založeno na základě souhlasu nebo na smlouvě

b) zpracování se provádí automatizovaně.

Při výkonu svého práva na přenositelnost údajů má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

7. Subjekt údajů má z důvodů týkajících se jeho konkrétní situace **právo** kdykoli **vznést námitku** proti zpracování osobních údajů, které se jej týkají. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody

pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu.

8. **Uplatnění práv subjektu údajů**

8.1 Každý subjekt údajů má právo, na základě písemné žádosti, *jednou za kalendářní rok bezplatně, jinak kdykoli za úhradu částky ve výši 200,- Kč,*na poskytnutí informace o osobních údajích o něm zpracovávaných nebo na uplatnění kteréhokoliv výše uvedeného práva subjektu údajů. O svých právech musí být subjekt správcem informován. Písemná žádost musí být doručena Lidským zdrojům a komunikace přímo písemně nebo elektronicky. Útvar Lidských zdrojů a komunikace (dále LZK) poskytne informace o osobních údajích žadateli nejpozději do 30 kalendářních dnů od doručení žádosti. O podaných a vyřízených žádostech subjektů údajů vede LZK potřebnou evidenci. V případě, že informace je poskytována za úhradu, provede se tato úhrada v hotovosti v pokladně BC MCHZ.

VIII. Zpracování osobních údajů

1. Manuální způsob zpracování osobních údajů

1. Osobní údaje zpracovává zaměstnavatel v listinné podobě v osobních spisech, záznamech o uchazečích o zaměstnání, záznamech o vstupech a pohybu v areálu, či uzavřených smlouvách, které zaměstnavatel ve vztahu ke svým zaměstnancům, uchazečům o zaměstnání, fyzickým osobám vstupujících a pohybujících se v areálu, či fyzickým osobám vstupujících do obchodního vztahu vede.

2. Automatizovaný způsob zpracování osobních údajů

1. Osobní údaje zpracovává zaměstnavatel v elektronické podobě v příslušných SW, databázích a souborech, které zaměstnavatel vede ve vztahu ke svým zaměstnancům, uchazečům o zaměstnání, fyzickým osobám, které vstupují a pohybují se v areálu zaměstnavatele nebo které s ním í do obchodního vztahu vstupují.
2. Ochrana a likvidace osobních údajů automaticky zpracovávaných je uvedena v části 5. této směrnice.

3. Kamerové systémy

1. Provoz kamerových systémů upravuje provozní norma H202-S002 Kamerové systémy v BC MCHZ, která popisuje kamerový systém používaný v BC MCHZ a to z důvodu dohledu nad technologickými výrobními celky, prevence závažných havárií a za účelem ochrany majetku a osob. Popisuje počet, umístění instalovaných kamer a sledovaný prostor v areálu BC MCHZ a na přilehlých parkovištích. Popisuje způsob snímaného záznamu, provozní dobu kamer, určuje jeho uložení a definuje osoby, které mají k záznamům přístup.
2. Tento kamerový systém podle tohoto nařízení již nepodléhá dříve povinné registraci. V souladu s tímto nařízením jsou vedeny příslušné záznamy o zpracování.

4. Technická a organizační opatření k zajištění ochrany osobních údajů

1. **Osobní údaje**

a) uchovávané v listinné podobě jsou zabezpečeny uzamčením na určeném místě (uzamčená kancelář, skříň, trezor - s omezeným přístupem)

b) uchovávané v elektronické podobě jsou zabezpečeny prostřednictvím výpočetní techniky s příslušnou SW a HW ochranou definovanou ve směrnici Používání prostředků výpočetní techniky.

1.1. K osobním údajům zpracovávaným zaměstnavatelem mají **přístup** pouze zaměstnanci, u kterých je tento přístup nezbytný vzhledem k povinnostem, jež plní v pracovněprávním vztahu k zaměstnavateli, a zaměstnanci, kteří mají podle zákoníku práce právo nahlížet do osobních spisů zaměstnanců. Jedná se o zaměstnance na pozicích:

- zaměstnanci útvaru Lidských zdrojů a komunikace
- jednatelé a manažeři – přístup k osobním údajům všech subjektů řízeného útvaru
- vedoucí zaměstnanci včetně mistrů - přístup k vymezeným osobním údajům zaměstnanců řízeného útvaru a k údajům příslušných subjektů dle působnosti útvaru; těmito údaji se rozumí jméno a příjmení, datum narození, údaje o kvalifikaci, odborné a zdravotní způsobilosti, pracovní a mzdové zařazení zaměstnanců
- určení zaměstnanci - přístup k vymezeným osobním údajům pouze určených subjektů, se kterými pracují (pracovníci zajišťující agendu, související se vstupem a pohybem subjektů v areálu BC MCHZ, a pracovníci zajišťující agendu související s uzavřením smluvního vztahu s fyzickými osobami, dále vybraní zaměstnanci útvaru Kvality, ekologie a bezpečnosti). Těmito údaji se rozumí jméno a příjmení, číslo pracovního případně občanského průkazu nebo jiného dokladu totožnosti, kontaktní údaje (telefonní číslo nebo e-mailová adresa), místo trvalého bydliště, případně jiné místo, kde fyzická osoba pobývá.

1.2. Zaměstnanci, kteří mají přístup k osobním údajům, jsou povinni o obsahu těchto údajů zachovávat mlčenlivost, a to i po skončení jejich pracovního poměru nebo dohody konané mimo pracovní poměr.

1.3. Zaměstnanci, kteří se podílí na zabezpečení osobních údajů, jsou povinni o bezpečnostních opatřeních přijatých za účelem zajištění ochrany osobních údajů zachovávat mlčenlivost, a to i po skončení jejich pracovního poměru nebo dohody konané mimo pracovní poměr.

1.4. Každý zaměstnanec, který je vázán mlčenlivostí o osobních údajích nebo bezpečnostních opatřeních, musí být na tuto svou povinnost zaměstnavatelem individuálně upozorněn a musí být rovněž poučen o právních souvislostech ochrany osobních údajů.

2. **Možná technická a organizační opatření na ochranu osobních údajů**

a) Technická opatření

- Zabezpečení heslem
- Automatické uzamčení nepoužívaných terminálů

- Omezení přístupových práv na USB paměťové médium a jiné datové nosiče
- Software pro kontrolu virů a brány firewall
- Přístupová práva na základě rolí
- Zajištění prostor, v nichž se nacházejí systémy pro ukládání údajů a vstupní systému pro přístup do těchto prostor
- Šifrování zařízení, která opouštějí prostory organizací (např. notebooky)
- Zajištění bezpečnosti lokálních sítí
- Použití technologií, které zvyšují ochranu údajů, jako je pseudonymizace a anonymizace

b) Organizační opatření

- Identifikace a použití mezinárodních bezpečnostních standardů relevantní z pohledu společnosti
- Školení na různých úrovních organizace
- Opatření, která zohledňují spolehlivost zaměstnanců (například žádost o reference)
- Začlenění povinnosti ochrany údajů do pracovních smluv
- Identifikace odpovědných osob a vyvození odpovědnosti v případě porušení zabezpečení osobních údajů
- Monitorování zaměstnanců z hlediska dodržování bezpečnostních předpisů
- Omezení fyzického přístupu k elektronickým i papírovým záznamům
- Zavedení zásady čistého stolu
- Ukládání papírových dokumentů do uzamykatelných protipožárních skříní
- Omezení používání přenosných elektronických zařízení mimo pracoviště
- Omezení používání vlastních zařízení zaměstnance na pracovišti
- Zavedení předpisů o použití hesel
- Pravidelné vytváření bezpečnostních kopií a ukládání médií na jiné pracoviště / mimo podnik.
- Uložení smluvních závazků předepisujících příslušná bezpečnostní opatření straně, která údaje importuje v případě jejich přenosu do třetí země

3. Zabezpečení osobních údajů

1. Každý zpracovatel - uživatel a vedoucí útvaru (vlastník údajů), ve kterém jsou uživatelé osobních údajů, je povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Písemná nebo tištěná data s údaji subjektů údajů musí být uložena v příručních trezorech nebo uzamykatelných registrech s omezeným, kontrolovaným a definovaným přístupem. V útvarech hlavního zpracovatele (LZK) navíc v elektronicky zabezpečeném objektu a zabezpečené místnosti se zamezením volného přístupu osob. Tato povinnost platí i po ukončení zpracování osobních údajů.

2. Zabezpečení centrálního automatizovaného systému zpracování, systém uživatelských identifikací, oprávnění apod. (včetně systému MARK), se řídí směrnicí Používání prostředků výpočetní techniky.
3. Zabezpečení programového systému MARK sestává z funkčních modulů "zaměstnanci" a "zpracování mzdy", podporujících činnosti útvaru Lidské zdroje a komunikace. Každý uživatel je v systému jednoznačně identifikován svým jménem a přístupovým heslem, jsou mu přiřazena přístupová práva, dle jeho funkčního zařazení. Aktuální seznam uživatelů MARK a rozsah jejich oprávnění (kategorií) vede mzdový ekonom LZK, definováno ve směrnici o Používání výpočetní techniky
4. Všechny podnikové procesy musí být posuzovány rovněž z hlediska ochrany osobních údajů ve smyslu Nařízení EP a tato povinnost musí být stanovena v příslušné interní dokumentaci, která je pro příslušný proces určující.

4. Likvidace osobních údajů

1. Zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů. Likvidaci písemné dokumentace a automatizovaného zpracování určují směrnice.
2. Výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení stanoví zvláštní zákon.

5. Předávání osobních údajů do třetích zemí

1. Do třetích zemí mohou být osobní údaje předány za podmínek odpovídajícím požadavkům stanoveným Nařízením EP:

a) na základě rozhodnutí o odpovídající ochraně.

Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit, jestliže Komise EP rozhodla, že tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi, nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany. Takovéto předání nevyžaduje žádné zvláštní povolení.

b) na základě vhodných záruk;
Jestliže neexistuje rozhodnutí podle čl. a) správce nebo zpracovatel mohou předat osobní údaje do třetí země nebo mezinárodní organizaci, pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

2. Do třetích zemí smí za stanovených podmínek předat osobní údaje výhradně jen centrální zpracovatel LZK, případně další útvar pouze s jeho souhlasem po provedeném posouzení.

IX. Všeobecné zásady týkající se sdílení údajů

Následující zásady se uplatňují bez ohledu na směr sdílení údajů (přenos nebo příjem údajů). Tyto obecné zásady je třeba vykládat pro vnitropodnikovou komunikaci a také

pro komunikaci mezi jednotlivými právními subjekty, a to nezávisle na tom, zda je strana účastnící se sdílení údajů členem skupiny nebo zastupuje třetí stranu.

Nestanoví-li předpisy společnosti jinak, je distribuce osobních údajů primárně právem a odpovědností vlastníka údajů. Vlastník údajů je nezávisle na směru sdílení údajů oprávněn vydávat vnitřní nařízení týkající se sdílení příslušných údajů.
Při sdílení údajů musí vlastník údajů dodržovat platné interní předpisy společnosti.
V zásadě se sdílení údajů může uskutečnit pouze s vědomím vlastníka údajů. Není-li stanoveno jinak, informování vlastníka údajů o jejich sdílení není nutné, pokud je sdílení údajů stanoveno zákonem nebo vnitřním předpisem společnosti nebo je poskytování údajů upraveno smlouvou a vlastník údajů se podílel na jejím uzavření.

Distribuovat osobní údaje lze výhradně spolu se zásadami zpracování údajů podobně jako u jiných operací zpracování údajů (viz kapitola 7) mimo jiné se zvláštním zřetelem na omezení účelu a minimalizaci údajů.

1. Zásady sdílení údajů

Sdílením údajů se rozumí sdílení osobních údajů členem skupiny, umožnění nahlížení a zajištění přístupu k nim, pokud je přijímající stranou třetí osoba (obvykle sdílení údajů s externími partnery nebo mezi členy skupiny).

Rozsah sdílených údajů a osob oprávněných k nahlížení je omezen na minimum nezbytné k dosažení účelu zpracování údajů. Osobní údaje lze sdílet s fyzickou a právnickou osobou, která je oprávněna se s nimi seznámit. Toto pravidlo se použije i v případě blízkých příbuzných subjektu údajů.

2. Zajištění zákonného zpracování údajů v případě sdílení údajů v rámci společnosti

V případě sdílení údajů v rámci člena skupiny, jsou-li zákonem stanoveny dobře definované zásady a postupy související se zpracováním osobních údajů, za jejichž dodržování odpovídají i přijímající strany, zajistí vlastník údajů seznámení přijímajících stran s těmito zákonnými povinnostmi. Příjemci mohou být informováni ad hoc, vydáním interního nařízení nebo upozorněním na platné předpisy. Odborník na ochranu údajů a koordinátor ochrany údajů mohou v případě potřeby zajistit podporu při poskytování informací.

3. Zvláštní ustanovení pro sdílení údajů se třetí stranou

Příjemce musí být ve všech případech upozorněn, že sdílené údaje nesmí být použity k jinému účelu.

Je-li to nezbytně nutné, snaží se členové skupiny se v rámci možností podílet na sdílení údajů. V případě žádosti o údaje od třetí strany se třetí strana, pokud je to možné, sama snaží získat osobní údaje od subjektu údajů, jsou-li tyto údaje u subjektu údajů rovněž k dispozici. Členové skupiny provádějí nepovinné zpracování údajů a sdílení údajů, které úzce nesouvisí s obchodním jednáním, pouze tehdy, pokud to jednoznačně přináší přidanou hodnotu pro člena skupiny nebo subjekty údajů.

Pokud jde o sdílení údajů, musí být dodržována práva subjektů údajů se zvláštním ohledem na právo být informován.
Tyto subjekty údajů, bez ohledu na to, zda se jedná o zaměstnance nebo externí osobu, musí být informovány o tom, že člen skupiny sdílí jejich osobní údaje s třetí stranou. K informování zpravidla dojde před sdílením údajů. Pokud je zde pouze obecná možnost sdílení údajů a není jisté, zda k němu skutečně dojde, musí být poskytnuty informace o možnosti předání údajů.
Zpracovávané údaje původně shromážděné pro jiný účel lze sdílet s jinou osobou, pouze tehdy, pokud byly subjekty údajů informovány o rozšíření účelů zpracování údajů a před sdílením údajů bylo provedeno posouzení v souladu s nařízením GDPR. Pokud jsou údaje zpracovávány na základě souhlasu, musí být ke sdílení osobních údajů v zásadě získán souhlas subjektu údajů. V případě neposkytnutí souhlasu není možné údaje sdílet, pokud to není nezbytné z důvodu právní povinnosti správce údajů, životně důležitého zájmu jakékoli osoby nebo jiných relevantních právních důvodů. I v těchto případech je nutné subjekt údajů o sdílení údajů informovat.

V případě jiných právních důvodů souvisejících se zpracováním údajů není ke sdílení údajů vyžadován souhlas subjektu údajů.

4. **Smlouvy upravující sdílení údajů**

V případě sdílení údajů se třetí stranou je třeba vynaložit veškeré úsilí, aby podrobnosti o sdílení údajů byly upraveny ve smlouvě (uzavření zvláštní smlouvy není nutně vyžadováno). Smluvní regulace je rozumná zejména tehdy, pokud

- existuje vysoký počet subjektů údajů, nebo
- dochází k pravidelnému sdílení údajů, nebo
- se jedná o různé osobní údaje, nebo
- sdílené údaje spadají do zvláštní kategorie osobních údajů, nebo
- subjektem údajů je dítě, nebo
- k poskytování údajů dochází v rámci využívání služby, jejímž předmětem a klíčovým prvkem je výslovně zpracování osobních údajů.

Uzavření smlouvy je povinné, pokud jde o společnou kontrolu údajů a činnost zpracování údajů.

Smlouvu není nutné uzavírat, pokud k dodání údajů dochází z důvodu plnění zákonné povinnosti, zejména v případě žádostí o údaje ze strany veřejných orgánu.

Vlastník údajů musí zajistit, aby smlouva zahrnovala alespoň následující oblasti:

- Účel zpracování údajů;
- Role smluvních stran při zpracování údajů (nezávislý správce údajů, společní správci údajů, zpracovatel údajů);
- Úlohu a odpovědnost smluvních stran při výkonu práv subjektů údajů;
- Prohlášení, že poskytování údajů probíhá v souladu se zákonem;
- Kontaktní údaje zástupce smluvních stran pro ochranu osobních údajů;
- Závazek, že poskytnuté údaje nebudou použity pro jiné účely;
- Povinnosti strany přijímající údaje v oblasti ochrany údajů, zejména pokud je sdílení údajů pravidelné, jsou sdíleny zvláštní údaje nebo údaje dětí a údaje jsou dodávány v rámci využívání takové služby, jejímž předmětem a podstatnou součástí je výslovně zpracování osobních údajů.

Odborník na ochranu údajů se podílí na přípravě smluv týkajících se sdílení údajů. Je vhodné, aby členové skupiny vypracovali vzory smluv, všeobecné smluvní podmínky a standardní smluvní doložky s ohledem na výše uvedené zásady. Na přípravě těchto předpisů se podílí odborník na ochranu údajů. Při uplatňování těchto právních předpisů se další pokyny odborníka na ochranu údajů nevyžadují, pokud jsou tyto předpisy používány v nezměněné podobě tak, jak jsou obvykle zamýšleny.

5. **Příjem osobních údajů od třetí strany**

O přijetí osobních údajů hovoříme, pokud některý člen skupiny obdrží osobní údaje od třetí strany (obvykle od právnické osoby).

6. **Obecné zásady přijímání údajů**

Před přijetím údajů je třeba se ujistit, že osobní údaje jsou dostatečné a vhodné pro splnění účelu zpracování údajů. Veškeré údaje, které nejsou nezbytné pro dosažení účelu zpracování údajů, budou vymazány.
Nevyžádané údaje, které nesouvisejí s žádným účelem zpracování údajů, budou pokud možno okamžitě vymazány.

V případě osobních údajů přijatých ze třetí země si vlastník údajů od strany, která údaje sdílí, vyžádá informace o tom, zda je v souvislosti s dodanými osobními údaji třeba zohlednit přeshraniční právní předpisy o ochraně údajů. Pokud tomu tak je, informuje o tom vlastník údajů odborníka na ochranu osobních údajů, který se zapojí do výkladu zákona a zajištění zákonného přijetí údajů, nestanoví-li jiný předpis společnosti jinak.
Strana, která poskytuje osobní údaje členovi skupiny, ručí za přesnost dodaných údajů a je-li to možné, je povinna zajistit aktuálnost osobních údajů.

Minimální úroveň sdělování údajů nezbytná pro výkon práva na informace

V případě sběru dat od subjektu údajů	**V případě sběru dat jinak než od subjektu údajů**
Při získávání osobních údajů poskytne správce údajů tyto informace:	**Správce údajů poskytne následující informace** a) **nejpozději do jednoho měsíce;** b) **při první příležitosti kontaktovat subjekt údajů nebo** c) **nejpozději při prvním zpřístupnění příjemci, jsou-li údaje poskytování jiným příjemcům:**
Správce údajů (zástupce) a jeho kontaktní údaje	Správce údajů (zástupce) a jeho kontaktní údaje
Kontaktní údaje pověřence/odborníka pro ochranu osobních údajů	Kontaktní údaje pověřence/odborníka pro ochranu osobních údajů
Objektivní a právní důvod zpracování údajů	Objektivní a právní důvod zpracování údajů
Důvody pro zpracování osobních údajů (např. povinné zpracování, plnění smluvního závazku, předpoklad smlouvy)	-
-	Kategorie zpracovaných osobních údajů

Doba uchování údajů nebo aspekty stanovení doby uchování	Doba uchování údajů nebo aspekty stanovení doby uchování
Příjemci osobních údajů	Příjemci osobních údajů
Záměr přenosu údajů do třetí země, uvedení záruk	Záměr přenosu údajů do třetí země, uvedení záruk
Použití automatizovaného rozhodování a informace související s aplikovanou logikou, jakož i význam a důsledky zpracování údajů.	Použití automatizovaného rozhodování a informace související s aplikovanou logikou, jakož i význam a důsledky zpracování údajů.
Práva subjektu údajů (přístup, oprava, výmaz, omezení zpracování, námitky a právo na přenositelnost údajů).	Práva subjektu údajů (přístup, oprava, výmaz, omezení zpracování, námitky a právo na přenositelnost údajů).
Právo na odvolání souhlasu	Právo na odvolání souhlasu
Právo na stížnost vnitrostátnímu orgánu pro ochranu osobních údajů a svobodu informací (nebo místně příslušnému dozorovému úřadu)	Právo na stížnost vnitrostátnímu orgánu pro ochranu osobních údajů a svobodu informací (nebo místně příslušnému dozorovému úřadu)
-	Zdroj osobních údajů
Je subjekt údajů povinen údaje poskytnout	-
Možné důsledky neposkytnutí údajů	-