**Příloha č. 2 - Technická a organizační opatření ochrany dat**

**Obsah**

[I. Rozsah aplikace](#_Toc509913773)

[II. Kontrola vstupu](#_Toc509913774)

[III. Řízení přístupu](#_Toc509913775)

[IV. Kontrola přístupu](#_Toc509913776)

[V. Kontrola přenosu](#_Toc509913777)

[VI. Kontrola vstupu](#_Toc509913778)

[VII. Smluvní kontrola](#_Toc509913779)

[VIII. Kontrola dostupnosti](#_Toc509913780)

[IX. Pravidlo oddělení](#_Toc509913781)

# Rozsah aplikace

## Podle nařízení o ochraně osobních údajů (GDPR) je jakýkoli subjekt, který sám nebo jménem jiného shromažďuje, zpracovává nebo používá osobní údaje, povinen přijmout taková technické a organizační opatření, která jsou nezbytná k zajištění provádění zákonných pravidel ochrany údajů. Tento dokument stanoví záruky, které byly zavedeny podle článku 28 GDPR.

# Kontrola vstupu

## Řízení vstupu slouží k tomu, aby se neoprávněným osobám zabránilo získat přístup k technickému vybavení, kterým jsou zpracovávány nebo používány osobní údaje a do prostor, kde jsou tyto údaje zpracovávány nebo používány.

### *Vstupní kontrola v provozních prostorách Zpracovatele*

### Vstup do budov společnosti skupiny Zpracovatele je omezen vstupními kontrolami. Pro pracovníky Zpracovatele se jedná především o elektronické klíče, které umožňují vstup do provozních prostor podle míry oprávnění k přístupu stanovené pro každý klíč. Práva přístupu jsou sladěna s pravomocemi přiznanými zaměstnancům jak časově (podle povoleného užití v určitých pracovních dnech a v určitých časech), tak i místně (podle konkrétních částí provozních prostor). Pro osoby mimo skupinu společností Zpracovatele je vstupní kontrola zajištěna centrální recepční halou nebo vrátnicí, která zaznamenává návštěvníky a vydává návštěvníkům průkazy návštěvníků platné po dobu jejich návštěv.

### *Řízení vstupu do počítačového centra Zpracovatele*

### IT systémy společností skupiny Zpracovatele jsou provozovány pro Zpracovatele různými datovými centry. Datová centra jsou navržena jako uzavřené bezpečnostní prostory. Existuje jak stavební, tak technická kontrola vstupu. Datová centra jsou zabezpečena elektronicky a návštěvníci mají přístup pouze v doprovodu a nejsou ponecháni bez dozoru. Požadované vstupní karty jsou vydávány pouze po předchozím oznámení a za přísných podmínek. Jejich používání je zaznamenáváno. Datová centra jsou monitorována videem na místě samém, stejně tak jako klíčové vnitřní prostory budovy jsou průběžně kontrolovány bezpečnostní agenturou.

# Řízení přístupu

## Řízení přístupu zahrnuje opatření, kterými je zabráněno použití systémů zpracování údajů neoprávněnými osobami (logická bezpečnost).

### *Kontrola vstupu do provozoven skupiny Zpracovatele*

### Administrativní práce prováděné Zpracovatelem nebo provozovatelem datových center provádějí pouze někteří zaměstnanci, kteří podepsali zvláštní dohodu o mlčenlivosti a byli prověřeni předtím, než zaměstnání získali. Dohoda o mlčenlivosti obsahuje závazek k utajení údajů. Tam, kde se administrativní práce provádí prostřednictvím externího přístupu, jsou tzv. připojení VPN šifrována pomocí nejnovějších technologií a vyžaduje se další autentizace. Identifikace pomocí uživatelských jmen a bezpečnostních hesel je povinná. Informační systém Zpracovatele je také chráněn před vnějšími útoky technologií brány firewall.

### *Řízení přístupu u operátora datového centra*

### Aby bylo zajištěno, že systém Zpracovatele je bezpečný, operátor datového centra nainstaloval další sofistikovanou bránu firewall v rámci síťové vrstvy a produktů regulujících přístup.

# Kontrola přístupu

## Kontrola přístupu zahrnuje opatření, aby se zajistilo, že osoby oprávněné k používání systému zpracování údajů mohou získat přístup pouze k údajům, ke kterým mají oprávnění k přístupu, a že osobní údaje nelze v průběhu zpracování nebo používání číst, kopírovat, měnit nebo smazat bez povolení poté, co jsou uloženy.

### *Kontrola přístupu v provozních prostorách Zpracovatele*

### Skupina společností Zpracovatele definovala a zdokumentovala vnitřní standardy pro správu oprávnění. Ty upravují práva, která mají administrátoři nad systémem pro klienty. Tato pravidla stanovují například požadavky týkající se bezpečných hesel.

### *Řízení přístupu u operátora datového centra*

### Pokud je provozovatel datového centra smluvně pověřen Zpracovatelem převzít vkládání uživatelů a oprávnění na aplikační vrstvě, bude v zásadě vázán stejnými bezpečnostními standardy, jaké platí pro samotné provozní prostory Zpracovatele. Odchylky jsou přípustné pouze v případě, že je Zpracovatel písemně umožní. Definice pokynů o tom, jak mají být operátorem datového centra navrženy koncepty autorizací specifické pro aplikaci, je určena Zpracovatelem.

# Kontrola přenosu

## Kontrola přenosu zahrnuje opatření, která zajišťují, že osobní údaje nemohou být čteny, kopírovány, měněny nebo vymazány bez povolení během elektronického přenosu, při přepravě nebo při uložení na nosičích dat a že je možné ověřit a zjistit, kde mají být osobní údaje předávány prostředky datové komunikace.

### *Kontrola přenosu v provozních prostorách Zpracovatele*

### Pokud jde o obecné zpracování údajů Zpracovatelem (údaje o zaměstnancích, údaje dodavatele, údaje o zákaznících), řízení přenosu (kontrola přenosu, kontrola přepravy, kontrola komunikace), vše je zajištěno pomocí vhodných technických postupů (opatření). Mezi ně patří firewall, ochrana proti virům, VPN tunel, šifrování dat (zejména prostřednictvím protokolu https / SSL nebo VPN tunelu) a ochrana heslem pro jednotlivé dokumenty. Jedinými paměťovými médii používanými pro elektronický přenos důvěrných dat jsou ty, které umožňují šifrování dat. Pouze vhodní poskytovatelé služeb jsou vybráni pro logistickou přepravu dat.

### Co se týče komerčního zpracování údajů Zpracovatelem, zejména získávání a poskytování dat klientů v podnikání Zpracovatele, je řízení přenosu zajištěno přihlášením všech fází zpracování dat. Pokud je to s klientem dohodnuto, jsou údaje klasifikované jako zvlášť důvěrné zašifrovány pro účely přenosu přes veřejné sítě.

### *Kontrola přenosu u operátora datového centra*

### Provozovatel datového centra je vázán stejnými povinnostmi týkajícími se řízení přenosu jako Zpracovatel. U provozně nezbytných kopií (zálohování), zejména v souvislosti s bezpečností základních dat, se používají pouze standardizované a zdokumentované postupy. Vytvoření všech záloh je zaznamenáno.

# Kontrola vstupu

## Řízení vstupu zahrnuje opatření, aby se zajistilo, že je možné následně ověřit a zjistit, zda a kým byly osobní údaje v systémech zpracování údajů zadány, změněny nebo odstraněny.

## Zadávání dat může provádět pouze personál, který má přístup k datům (viz ustanovení o řízení přístupu v kapitole III).

## Jsou také automaticky vytvářeny záznamy o „určitých procesních krocích“ na systémech. Zaznamenávání „určitých procesních kroků“ se týká procesů, které slouží k zajištění kontinuity provozu, které slouží účetním účelům a splnění zákonných požadavků na uchovávání dat.

# Smluvní kontrola

## Smluvní kontrola zahrnuje opatření, která zajišťují, že osobní údaje zpracovávané na základě smlouvy mohou být zpracovány pouze podle pokynů klienta.

## Tam, kde Zpracovatel zpracovává osobní údaje na základě smlouvy, se vždy uzavírá písemná dohoda o zpracování údajů se zákonným obsahem požadovaným podle GDPR. Zpracovatel má také pro tuto variantu vlastní vzorové smlouvy, které jsou k dispozici a které může klient k tomuto účelu použít. Smluvní závazky zajišťují, že Zpracovatel zpracovává pouze údaje o klientech podle jejich pokynů, že je zajištěna důvěrnost údajů a zejména, že při neexistenci výslovných odlišných pokynů klienta nejsou údaje klienta začleněny do obecné databáze společnosti skupiny Zpracovatele.

## Navíc podrobnosti o technicko-organizační bezpečnosti Zpracovatele a opatřeních Zpracovatele na místě samém tvoří součást každé smlouvy o zpracování údajů se Zpracovatelem v důsledku toho, že tento dokument je dohodnutou přílohou k takové smlouvě o zpracování osobních údajů.

# Kontrola dostupnosti

## Kontrola dostupnosti zahrnuje opatření, která zaručují, že osobní údaje budou chráněny před náhodnou ztrátou nebo zničením.

## Základem kontroly dostupnosti je outsourcing provozu IT vybavení do dobře chráněného datového centra operátora datového centra. Ten má zejména záložní napájecí systémy s nepřerušitelným zdrojem napájení a nouzovým generátorem (například s dieselovými generátory). Datové centrum je propojeno s provozními prostory společnosti skupiny Zpracovatel prostřednictvím přímého připojení na úrovni středního napětí prostřednictvím vlastní transformační stanice nebo podobného připojení. V datových centrech jsou instalovány také systémy včasného detekce požáru, které automaticky spouštějí hasicí proces.

## Dostupnost dat, zejména ochrana před ztrátou dat způsobenou technickou nefunkčností nebo náhodným smazáním, je rovněž zajištěna prostřednictvím pravidelných záloh dat a zálohování všech příslušných databází a systémů, takže v případě poruchy je možné je obnovit nejméně jednou měsíčně.

# Pravidlo oddělení

## Pravidla oddělení zahrnují opatření, která zajišťují, že data shromážděná pro různé účely mohou být zpracovávána samostatně.

### *Pravidlo oddělení v provozních prostorách Zpracovatel*

### Pokud jde o obecné zpracování údajů Zpracovatelem (data personálu, dodavatelská data, údaje o zákaznících), pravidlo oddělení se provádí například fyzickým oddělením a ukládáním v samostatných systémech nebo na samostatných nosičích dat, oddělení výrobních, testovacích a vývojových prostředí pro naše aplikace a systémy IT, vhodné koncepty autorizace a také databázová práva. Dále na straně softwaru je implementován logistický systém pro oddělování klientů.

### Co se týče komerčního zpracování údajů Zpracovatelem, zejména získávání a poskytování dat klientů v oboru informačních obchodů Zpracovatelem, je separace při ochraně dat zásadně dosaženo na základě žádosti. Všechny dodané datové balíčky jsou zpracovány zcela odděleně, takže je vyloučena možnost překrývání dat klienta. Byla zde přijata příslušná opatření (hardware a software).

### *Pravidlo oddělení operátora datového centra*

### Provozovatel datového centra odděluje všechna data fyzicky i logicky na úrovni klienta. Pokud je vrstva Zpracovatele převedena na externího operátora datového centra, obvykle existují další samostatná rozhraní založená na systému nebo databázi.