



KOVOLIT ČESKÁ

Název dokumentu:

SMĚRNICE O OCHRANĚ OSOBNÍCH ÚDAJŮ

společnosti KOVOLIT Česká, spol. s r.o.

Základní pravidla a povinnosti

I. Definice

1. **GDPR** – Nařízení Evropského parlamentu a Rady (EU) č. 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.
2. **Osobní údaj** - 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.
3. **Dozorový úřad** – Úřad pro ochranu osobních údajů, pokud prováděcí předpis nestanoví jinak.
4. **Správce** – společnost KOVOLIT Česká, spol. s r.o.
5. **Subjekt údajů** – každá fyzická osoba, včetně osob samostatně výdělečně činných.
6. **Oprávněná osoba** – je každá osoba, včetně právnických osob, která pro správce vykonává takovou činnost, při které přichází do styku s osobními údaji subjektů, včetně zaměstnanců správce, event. členů jeho orgánů.
7. **Pověřená osoba** – je oprávněná osoba pověřená správcem ke specifickým činnostem souvisejícím se zpracováním osobních údajů, zejména prevencí incidentů, zabezpečením zpracování osobních údajů, řešením stížností a žádostí, správou systémů a dalšími činnostmi. Seznam pověřených osob včetně označení jejich pověření je přílohou této směrnice.
8. **Zaměstnanec** – fyzická osoba v pracovněprávním či jiném obdobném vztahu ke správci jako zaměstnavateli.
9. **Klient/zákazník** (dále jen klient) – osoba v právním vztahu se správcem, vůči níž má správce v postavení dlužníka povinnost splnit dluh.
10. **Dodavatel** – osoba v právním vztahu se správcem, vůči níž má správce v postavení věřitele právo na určité plnění (pohledávku).
11. **Zpracování osobních údajů** – 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.

II. Účel

1. Účelem této směrnice, jako jednoho z organizačních opatření ve smyslu čl. 32 NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 (dále také GDPR), je stanovit pravidla zpracování osobních údajů správcem a zásady ochrany těchto údajů uplatňované na všechny informace týkající se identifikovaného nebo identifikovatelného subjektu údajů.
2. Tato směrnice dále upravuje postupy v případě porušení zabezpečení osobních údajů ve smyslu článku 33 a 34 GDPR a zároveň práva subjektu údajů na přístup k osobním údajům ve smyslu článku 15 GDPR.

III.

Zásady zpracování osobních údajů

1. Tato směrnice se vztahuje na každou oprávněnou osobu při plnění jejích povinností. Jakékoli zpracování osobních údajů musí být prováděno zákonným, spravedlivým a transparentním způsobem.
2. Každá oprávněná osoba musí být s touto směrnicí seznámena a na důkaz toho, že ji řádně pochopila a nemá k ní doplňující dotazy, připojí svůj podpis k dokumentu „Nakládání s osobními údaji dle zásad GDPR“.
3. Správce vede záznam o činnostech zpracování osobních údajů.
4. Správce provádí kontrolu přesnosti, úplnosti a aktuálnosti osobních údajů minimálně 1 x za dva roky u klientů a dodavatelů a každý rok u zaměstnanců.
5. Správce bude zpracovávat osobní údaje po dobu trvání smlouvy, nebo po dobu nezbytnou k plnění archivačních povinností správce podle platných právních předpisů, zejména zákona č. 563/1991 Sb., o účetnictví, zákona č. 235/2004 Sb., o dani z přidané hodnoty, zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, zákona č. 499/2004 Sb., o archivnictví a spisové službě, zákona č. 262/2006 Sb., zákoník práce.
6. Správce zpracovává osobní údaje jak v elektronické, tak analogové formě.
7. Správce zajistí pravidelná školení oprávněných osob na zásady dodržování ochrany osobních údajů ve smyslu GDPR každých 24 měsíců.

IV.

Povinnosti oprávněné osoby

1. Oprávněná osoba je povinna zpracovávat osobní údaje ve vztahu k subjektu údajů korektně a zákonným způsobem. Oprávněná osoba nesmí získané informace bez pokynu správce předat žádné další třetí osobě, a to ani v České republice a ani do zahraničí, tj. má povinnost mlčenlivosti.
2. Oprávněná osoba je povinna při získání osobních údajů od subjektu údajů informovat o tom pověřenou osobu, která subjektu údajů předá informační doložku dle GDPR, jejíž vzor je přílohou této směrnice, a zajistí její podpis.
3. Každá oprávněná osoba smí zpracovávat osobní údaje pouze za správcem určeným účelem, a to pouze správcem určenými prostředky.
4. Oprávněná osoba je oprávněna zpracovávat osobní údaje pouze v souladu s pokyny správce. Oprávněná osoba smí zpracovávat pouze osobní údaje nezbytné pro plnění svých povinností vůči správci. Správce za tímto účelem zřizuje oprávněným osobám přístup výlučně k nutným evidencím osobních údajů.
5. Zjistí-li oprávněná osoba, že jsou osobní údaje jakéhokoliv subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to správci.
6. Zjistí-li oprávněná osoba, že jsou osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to bezprostředně přímému nadřízenému a nedojde-li k nápravě bez zbytečného prodlení, pověřené osobě, příp. správci.
7. Oprávněná osoba pracující s osobními údaji v analogové formě je povinna tyto vždy před odchodem z pracoviště uzamknout tak, aby k nim neměla přístup žádná neoprávněná osoba.

8. Oprávněná osoba pracující s osobními údaji na PC musí vždy zajistit, aby v době její nepřítomnosti bylo nezbytné pro přístup k nim zadat přístupové heslo, které nesmí prozradit třetí osobě. Zároveň se zavazuje přístupové heslo minimálně 1 x za 6 měsíců měnit.

V.

Práva subjektů údajů

1. Oprávněná osoba, která obdržela v jakékoliv formě (písemně, telefonicky, osobně) žádost či stížnost fyzické osoby, která se týká nebo by se mohla týkat ochrany osobních údajů, zejména žádosti ve smyslu čl. 15 - 22 GDPR, oznámí tuto skutečnost příslušné pověřené osobě.
2. Příslušná pověřená osoba vyřizuje požadavky subjektů údajů v souladu s obecnými pokyny společnosti, vždy však tak, aby žádosti subjektu údajů bylo vyhověno bez zbytečného odkladu nejpozději do 1 měsíce ode dne obdržení žádosti, a aby mu byly k vyřízení jeho žádosti poskytnuty veškeré informace a v případě, že žádosti nebylo vyhověno, aby byly sděleny důvody tohoto rozhodnutí.
3. Pověřená osoba je povinna před odpovědí na požadavek ověřit identitu žádajícího subjektu údajů, a provést tak vždy přiměřeným způsobem, který zaručí dostatečnou identifikaci subjektu údajů s ohledem na formu podání, využitý komunikační prostředek a obsah žádosti subjektu údajů.
4. V případě žádosti subjektu údajů o přístup k osobním údajům poskytne příslušná pověřená osoba subjektu údajů minimálně informaci, zda osobní údaje, které se subjektu údajů týkají, jsou či nejsou zpracovávány a poskytne mu Informační doložku dle GDPR, jejíž vzor je přílohou této směrnice.
5. Informace podle tohoto článku poskytuje společnost subjektu údajů ve stejné formě, v jaké o informace subjekt údajů požádal.
6. Vzor odpovědi na žádost subjektu údajů je přílohou této směrnice.

VI.

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Může se jednat zejména o krádež nebo zničení analogově vedených informací, krádež nebo zničení elektronických medií včetně PC nebo hackerský útok.
2. Oprávněná osoba, která zjistí, že došlo k porušení zabezpečení osobních údajů je o tom povinna neprodleně informovat pověřenou osobu, a to bez ohledu na denní dobu.
3. Jakékoli porušení zabezpečení osobních údajů je správce povinen bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
4. Ohlášení dozorovému úřadu provede správce prostřednictvím datové schránky.
5. Ohlášení dozorovému úřadu podle tohoto článku musí přinejmenším obsahovat:
 - 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.

Není-li možné poskytnout veškeré tyto informace současně, mohou být poskytnuty postupně bez zbytečného odkladu.

6. Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí pověřená osoba toto porušení bez zbytečného odkladu subjektu údajů.
7. Správce prostřednictvím pověřené osoby dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

VII.

KONTROLA DODRŽOVÁNÍ SMĚRNICE

1. Dohled nad dodržováním této směrnice a obecně závazných právních předpisů souvisejících s GDPR vykonává správce.
2. Statutární orgán společnosti slouží jako kontaktní osoba oprávněné osoby v otázkách bezpečnosti a ochrany osobních údajů. V případě jakýchkoli pochybností o výkladu této směrnice či rozsahu a obsahu zákonných povinností poskytuje statutární orgán závazný výklad, kterým jsou oprávněné osoby povinny se řídit.
3. Statutární orgán odpovídá za aktualizaci této směrnice.

PŘÍLOHY

Nedílnou součástí této směrnice jsou tyto přílohy:

1. Nakládání s osobními údaji dle zásad GDPR
2. Zpracování osobních údajů dle požadavků GDPR – KOVOLIT Česká, spol. s r.o.
3. Přehled zaměstnanců určených k nakládání s osobními údaji
4. Vzor odpovědi na žádost subjektu údajů

Tato směrnice je účinná ode dne 25. 5. 2018

V České dne 14. 05. 2018

KOVOLIT Česká, spol. s r.o.
ČESKÁ 16
664 31 Lelekovice
DIČ: CZ4404 1861
tel.: 541 232 421 Fax: 541 232 114

.....
Správce