

VNITROPODNIKOVÁ SMĚRNICE

K OCHRANĚ OSOBNÍCH ÚDAJŮ V SOULADU S GDPR (Nařízení Evropského parlamentu a rady EU 2016/679)

NÁZEV PODNIKU:

ČÍSLO SMĚRNICE:

ÚČINNOST SMĚRNICE OD:

VYPRACOVAL:

I. Obecné pojmy

Vysvětlení pojmů je součástí přílohy číslo I. Směrnice/Kodex Steerty ochrany osobních údajů

II. Zpracování osobních údajů

Zpracování se řídí dle přílohy číslo I. Směrnice/Kodex Steerty ochrany osobních údajů s ohledem na doplněné kapitoly:

- | | |
|---|----------------|
| • Úvodní analýza stavu ochrany osobních údajů | strana 10 - 14 |
| • Závěry na základě analýzy | strana 15 - 17 |
| • Záznamy o činnostech zpracování | strana 18 - 23 |
| • Posouzení vlivu na ochranu osobních údajů | strana 24 |
| • Zpracovávané osobní údaje | strana 74 - 76 |
| • Zásady zpracování osobních údajů | strana 79 |
| • Poučení o zpracování osobních údajů | strana 93 - 94 |
| • Povinnost mlčenlivosti zaměstnance | strana 95 |

V:

DNE:

PODPIS:

© 2006 The Authors



Směrnice / Kodex Steerty ochrany osobních údajů

Steerty USA, Inc.

Email: network@steerty.com

Website: www.steerty.com

Tel: +420 723 940 666

Mostní 747, Kralupy nad Vltavou

Česká Republika, 278 01



[illegible]

OBSAH

Revize dokumentu	2
Vlastnosti dokumentu	2
Účel dokumentu	2
Úvod	7
Zásady práce pro zpracování osobních údajů	7
Nařízení	7
Příklad	8
Přípravná fáze	8
Doporučení	8
Pravidla	8
Opakované preventivní kontroly	9
Analýza stávající ochrany osobních údajů v podniku	10
Shromažďované údaje	10
Oznamovací povinnost	12
Zabezpečení	12
Personální a mzdová dokumentace zaměstnanců	13
Evidence pracovních úrazů zaměstnanců	13
Prezentace podniku	14
Kamerový systém	14
Závěry a doporučení dle analýzy stávajícího stavu v podniku	15
Záznamy o činnostech zpracování osobních údajů	18
Posouzení vlivu na ochranu osobních údajů	24
Hodnocení dopadů programového vybavení Steerty	25
míra monitorování subjektu údajů	25
shromažďované údaje o subjektu údajů	25
míra zranitelnosti subjektu údajů	25
dostupnost osobních údajů	25
rozsah zpracovávaných osobních údajů	25
zasažené území z hlediska subjektu údajů	25
uplatnění práv subjektu	26
přístupnost osobních údajů	26

soustavnost zpracování osobních údajů	26
předávání osobních údajů	26
k působnosti správce	26
k rozložení správce na území	26
ke složitosti systému zpracování	26
vazby na jiné subjekty	26
inovativnost řešení	26
Registrace uživatele	27
Registrace partnera, poskytovatele služeb nebo dodavatele zboží	32
Vytvoření objednávky zákazníka	37
Vytvoření objednávky partnera	42
Správa kartotéky, administrace obchodního případu	47
Administrace profilu uživatele	52
Komunikace pomocí API	57
Archivace dat	62
Smazání dat	67
Vysvětlení pojmů	72
Správce osobních údajů	72
Společný správce	72
Zpracovatel osobních údajů	72
Podnik	72
Subjekt údajů	72
Vedení podniku	72
Zpracování zvláštní kategorie (citlivých) údajů	73
Zpracovávané osobní údaje	74
Osobní údaje zpracovávané na základě oprávněného zájmu	75
Osobní údaje zpracovávané vzhledem k povinnosti vůči veřejné moci	75
Osobní údaje zpracovávané na základě informovaného souhlasu	75
Osobní údaje povinně zpracovávané podle zvláštních zákonů a nařízení	75
Informace o ochraně osobních údajů	77
Právo na přístup k osobním údajům	77
Právo na opravu osobních údajů	78
Právo vznést námitku proti zpracování osobních údajů	78

Právo na výmaz osobních údajů _____	78
Zásady zpracování osobních údajů _____	79
“zákonnost, korektnost a transparentnost” _____	79
“účelové omezení” _____	79
“minimalizace údajů” _____	79
“přesnost” _____	79
“omezení uložení” _____	79
“integrita a důvěrnost” _____	79
Organizační a technická opatření k zabezpečení osobních údajů v podniku _	80
Spisový a skartační řád _____	80
Skartační plán _____	82
Provozní pokyny / řád _____	85
Organizační pokyny / řád _____	85
Kartotéka, evidence záznamů v podniku _____	85
Webové stránky a použití audiovizuálních děl na sociálních sítích _____	85
Mimopracovní aktivity _____	86
Firemní stravování _____	86
Smlouvy _____	86
Výpočetní technika _____	87
Kamerový systém _____	87
Pracovní náplně _____	88
Odpovědnost podniku jako správce osobních údajů _____	90
Odpovědnost zpracovatele osobních údajů _____	90
Ohlašování případů porušení zabezpečení osobních údajů _____	91
Jmenování pověřence pro ochranu osobních údajů _____	91
Poplatky za poskytnuté informace _____	92
Poučení o zpracování osobních údajů _____	93
Povinnost mlčenlivosti _____	95
Seznam příloh _____	96
Dokumenty určené k doplnění _____	96
Obecné _____	96
Volitelné _____	96
Informovaný souhlas _____	97

Žádost o informaci o zpracovávaných osobních údajích	98
Hlášení bezpečnostního incidentu	99
Smlouva o poskytování služeb DPO	100
1. Smluvní strany	100
2. Předmět smlouvy	100
3. Práva a povinnosti pověřence	101
4. Cena a platební podmínky	101
5. Ukončení smlouvy	101
6. Závěrečná ustanovení	102
Dotazník na kontrolu aktuálnosti evidovaných osobních údajů	103
Sazebník úhrad za poskytování informací na vyžádání	104
Pořízení kopií a tisků vč. skenování	104
Média pro přenos informací	104
Harmonogram provádění kontrol	105

ÚVOD

Závazný pokyn vedení podniku pro zajištění odpovídající ochrany osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

Zásady práce pro zpracování osobních údajů

Osobní údaje může podnik zpracovávat pouze na základě právního předpisu, v případě prokázání oprávněného zájmu nebo na základě souhlasu subjektu údajů (řidič, zákazník, zástupce třetí strany, zaměstnanec, brigádník...). Zpracování osobních údajů může být také na základě veřejného zájmu a při výkonu veřejné moci.

Souhlas subjektu údajů musí být informovaný, konkrétní a písemný a správce osobních údajů je povinen ho získat ještě předtím, než zpracování osobních údajů zahájí, a také je povinen po celou dobu zpracování prokázat souhlas se zpracováním osobních údajů Subjektu údajů nebo jeho oprávněného zástupce. V případě, že dochází pouze ke schraňování osobních údajů, bez dalšího zpracování a možnosti systematického vyhledávání, řazení informací atp., nejde o zpracování. Vedení podniku důsledně zakazuje předávání osobních údajů třetím osobám pro komerční nebo soukromé využití, pokud nejde o přímý požadavek Subjektu údajů. Obdobně se postupuje i u osobních údajů zaměstnanců podniku.

Nařízení

Vedení podniku se rozhodlo řídit tímto dokumentem vč. vlastních příloh a přijmout interní směrnici, která je součástí tohoto dokumentu, s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. Cílem je aplikovat ucelený soubor pravidel na ochranu osobních údajů v podniku, aby byla zajištěna ochrana proti neoprávněnému zacházení s daty.

“Informovaný souhlas nemusí správce získat pouze v případě zákonného zpracování a při doložení oprávněného zájmu.”

PŘÍKLAD

Servis má několik zaměstnanců, kteří přijímají objednávky osobně, po telefonu nebo pomocí internetových stránek a dalšími způsoby (email, skype, facebook). Objednávky se zaznamenávají do kalendáře rezervací klientů v papírové a elektronické podobě, mimo služby auto/pneu servisu, které se poskytují bez rezervace (na počkání).

Přípravná fáze

Základ je připravit si seznam způsobů, jak podnik přichází do styku osobními údaji, jak s nimi dále nakládá, kde a jak dlouho je eviduje a komu je dále předává. Analýzou se zjistilo, že osobní údaje zákazníků jsou evidované v objednávkovém a fakturačním nástroji (v sešitu a na PC). S osobními údaji zákazníků pracují zaměstnanci pověřeni realizací jednotlivých zakázek a po jejich skončení jsou informace uloženy v počítači i papírové podobě. Podnik využívá online inzerci, při které nedochází k propojování informací o zákaznících. Osobní údaje zaměstnanců i uchazečů o zaměstnání jsou v šanonu v kanceláři, odkud se neaktuální dokumenty přesouvají do archivu a následně zničí v prostorách podniku nebo smluvně. Údaje se předávají externí firmě pro zpracování mzdové a účetní evidence, pojištění, stravenek a orgánům státní správy (daňové, důchodové, nemocenské, zdravotní, inspektorát práce).

Doporučení

Po zvážení situace vyplynulo několik oblastí na které je třeba se zaměřit.

- zajistit aby k osobním údajům měl přístup jen povolený okruh zaměstnanců
- s externími dodavateli zajistit v případě potřeby dodatek o způsobu zpracování
- zabezpečit přístup k osobním údajům z počítače jen oprávněnými osobami
- doklady v areálu uchovávat pod zámkem, zamčené kanceláři nebo v zamykatelné skříni
- zavést povinnost zaměstnanců o mlčenlivosti a dodržování ochrany osobních údajů
- připravit plán na archivaci informací po splnění účelu a důvodu jejich schraňování
- zveřejnit v provozovně a na internetových stránkách pravidla pro ochranu osobních údajů

Pravidla

- zaměstnanci, kteří se podílejí na realizaci zakázky v areálu podniku a nepřicházejí do kontaktu se zákazníkem budou mít přístup pouze k technickým informacím, bez osobních údajů zákazníka (např. zakázkový list bez kontaktních údajů)

- přístup do programu nebo pc bude přístupný pouze pod uživatelským jménem a heslem, jen pro oprávněnou osobu, stejně tak bude zajištěn přístup do elektronické pošty.
- pokud dochází k předávání osobních údajů třetí straně, zajistit smluvně jejich ochranu včetně předávání prostředky elektronické komunikace v zaheslované nebo v šifrované podobě a zajistit předávání bezpečnostních incidentů, pokud k nim dojde u druhé smluvní strany, včetně spolupráce při řešení požadavků subjektu údajů ke zpracování údajů
- vytvořit pro jednotlivé pracovníky oddělené přístupy k výpočetní technice (profily, přihlašovací účty pracovníků) s hesly, která znají jen oni, případně určit vlastní zařízení.
- zajistit, aby kancelář, kde jsou uloženy osobní údaje v listinné podobě byla v nepřítomnosti oprávněných osob vždy zamčena
- projít spisy a poté dokumenty s osobními údaji umístit do uzamykatelného prostoru / skříně
- seznámit (a proškolit nové) zaměstnance s pokyny pro nakládání s osobními údaji v podniku a upozornit na sankce při neplnění pracovních povinností, včetně mlčenlivosti
- spolu s roční inventurou majetku/zásob, provádět inventarizaci osobních dat o zaměstnancích, uchazečích o zaměstnání, zákaznících i potencionálních klientech a stanovit si lhůtu pro vymazání údajů u nedokončených obchodních případů bez fakturace
- vyvěsit v provozovně pravidla ochrany osobních údajů a přidat je i na internetové stránky

Opakované preventivní kontroly

- po několika měsících od zavedení nových pravidel firma vyhodnotila situaci s dodržováním práv subjektů údajů a doladila postupy, když došlo ke zjištění, že ne vždy se všichni zaměstnanci chovali v souladu s nařízením. Např. posílání dat v mailu bez hesla, předávání osobních údajů mezi pracovníky, kteří je nepotřebují k plnění úkolů.
- z toho důvodu se rozhodlo pořádat čtvrtletní proškolení zaměstnanců o nakládání s osobními údaji v podniku, zvláště s ohledem na plánované zavedení nových nástrojů a postupů, kdy musí dojít znovu k analýze celého procesu zpracování a seznámení zaměstnanců s vlivem na jejich pracovní náplň

VYSVĚTLENÍ POJMŮ

Správce osobních údajů

I když mizí povinnost registrovat se u úřadu pro ochranu osobních údajů jako správce resp. zpracovatel osobních údajů, nové nařízení se týká plošně všech subjektů, které s osobními údaji mohou přijít do styku. Každý podnikatel je tak správcem osobních údajů, bez povinnosti se nahlásit úřadu. Správce osobních údajů je pro účely této směrnice podnik, člen sítě Steerty.



Společný správce

Podnik zapojený do Steerty, který využívá řešení Steerty jako svou Kartotéku pro účely vedení obchodní administrativy v servisu, je společný správce spolu s poskytovatelem platformy, který je zároveň i jedním ze zpracovatelů osobních údajů pro podnik v souladu s nařízením GDPR.

Zpracovatel osobních údajů

Správce může být i zpracovatelem osobních údajů. Zpracovatelem pro podnik je například účetní, daňový poradce, podnikový lékař nebo poskytovatelé pojištění a dalších služeb, kteří pro podnik vykonávají činnosti s přístupem k osobním údajům zaměstnanců a klientů.

Podnik

Podnikem se rozumí správce osobních údajů stejně jako areál podniku tohoto správce.

Subjekt údajů

Je soukromá osoba, klient, zákazník, řidič i zodpovědná nebo kontaktní osoba, která je zástupce třetí strany.

Vedení podniku

Odpovědná právnická nebo fyzická osoba, případně kolektivní zástupce, který je oprávněn vydat / přijmou tuto směrnici v rámci podniku, resp. přistoupit k dodržování Kodexu Steerty.

SEZNAM PŘÍLOH

Dokumenty určené k doplnění

- Analýza současného stavu (strana 10 - 14)
- Závěry analýzy (strana 15 - 17)
- Záznamy o činnostech zpracování osobních údajů (strana 18 - 23)
- Poučení o zpracování osobních údajů (strana 93)

Obecné

- Informovaný souhlas (Příloha I.)
- Žádost o informaci o zpracovávaných osobních údajích (Příloha II.)
- Formulář pro hlášení bezpečnostního incidentu (Příloha III.)
- Smlouva o poskytování služeb Steerty DPO (Příloha IV.)
- Dotazník na kontrolu aktuality osobních údajů (Příloha V.)
- Sazebník úhrad za poskytování informací na vyžádání (Příloha VI.)
- Harmonogram prováděných kontrol (Příloha VII.)

Volitelné

- Směrnice pro evidenci úschov a zastupování zákazníků
- Pracovní náplně vedení, administrativních, technických, odborných a dalších pracovníků
- Spisový a skartační řád
- Provozní řád
- Organizační řád
- Vytýkáci dopis - porušení povinnosti mlčenlivosti

SMLOUVA O POSKYTOVÁNÍ SLUŽEB DPO

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, v platném znění

Smlouva o poskytování služby: Ochrana osobních údajů v podniku dle 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.

1. Smluvní strany

1.1 Člen sítě Steerty (dále jen „podnik“)

1.2 Externě spolupracující právnická osoba Steerty USA, Inc. (dále jen „DPO“)

2. Předmět smlouvy

DPO se zavazuje vykonávat pro podnik zajišťovat službu funkce pověřence pro ochranu osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016, článek 37 až 39.

Jedná se zejména o tyto činnosti:

- monitorovat soulad zpracování osobních údajů s povinnostmi vyplývajícími z nařízení EU,
- sledovat vývoj související legislativy,
- poskytovat poradenství správcům, zpracovatelům a jejich zaměstnancům,
- provádět interní audity na ochranu osobních údajů v podniku,
- školit zaměstnance k problematice ochrany osobních údajů,
- zajišťovat kontakt mezi podnikem a dozorovým orgánem,
- zajišťovat kontakt mezi podnikem a subjektem údajů v oblasti ochrany osobních údajů,
- vést potřebné záznamy (listinné nebo elektronické záznamy) o činnostech zpracování,
- navrhnout organizační a technická opatření k zabezpečení osobních údajů v podniku,
- pravidelně informovat zaměstnance a další strany o ochraně osobních údajů (GDPR),
- ve spolupráci s vedením podniku pravidelně kontrolovat dodržování opatření podniku,
- ve spolupráci s vedením podniku vyřizovat žádosti o informace od subjektu údajů, pokud k tomu není možné využít online aplikace Steerty nebo některou z jejich součástí,
- podílet se na ochraně osobních údajů získávaných z kamerového systému a konzultovat směrnici k provozování kamerového systému s dozorovým orgánem (Úřad na ochranu osobních údajů).

3. Práva a povinnosti pověřence

- Pověřenec je nápomocnou osobou podniku při práci s osobními údaji.
- Pověřenec je přímo podřízen vedení podniku.
- Pověřenec má přístup ke všem dokumentům a informacím, potřebným pro plnění úkolů.
- Pověřenec spolupracuje s dozorovým úřadem (Úřad pro ochranu osobních údajů) a je kontaktní osobou pro tento dozorový úřad a subjekty údajů, kteří se na něho mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv a povinností..
- Pověřenec plní své povinnosti a úkoly nezávislým způsobem, není v konfliktu zájmů.
- Pověřenci nejsou udíleny žádné pokyny týkající se plnění jeho úkolů podle nařízení, pro plnění svých úkolů nesmí být nijak postihován za nezávislý způsob výkonu povinností.
- Pověřenec je dostupný pomocí prostředků elektronické komunikace nebo osobně.

Pověřenec nenese osobní odpovědnost za nedodržování GDPR, právní soulad v oblasti ochrany dat je odpovědností správce nebo zpracovatele. Podnik pro svoji odpovědnost není vázán radou nebo stanoviskem pověřence při ochraně osobních údajů. Pověřencem je vždy jmenována konkrétní fyzická osoba, která zastupuje DPO a je dostatečně znalá k výkonu funkce.

4. Cena a platební podmínky

Podnik se zavazuje platit pověřenci měsíčně cenu za objednané služby DPO. ve výši odpovídajícího čerpání služeb za uplynulý měsíc. Úhrada ceny za vykonané činnosti bude prováděna na základě faktur, které budou vystaveny pověřencem vždy 1x za měsíc s datem zdanitelného plnění poslední pracovní den v daném období, ve kterém byly činnosti provedeny.

5. Ukončení smlouvy

- Zahájení plnění smlouvy je dnem podpisu této smlouvy.
- Ukončení plnění smlouvy je možné na základě písemné dohody smluvních stran.
- Podnik může odstoupit z této smlouvy v případě, že dojde k podstatnému porušení smluvních povinností nebo nevykonáváním činností, jež jsou předmětem této smlouvy, řádně, včas a s odbornou péčí.
- Pověřenec je oprávněn odstoupit od této smlouvy, nebudou-li mu umožněny podmínky ze strany podniku k plnění smluvních povinností nebo pokud dojde k prodlení s úhradou faktury za poskytnuté služby delší než 30 dní.
- Odstoupení od smlouvy oznámí oprávněná strana druhé straně doporučeným dopisem nebo jiným způsobem, kdy je strana schopna doložit doručení dokumentu. Smlouvy zaniká ke dni doručení dopisu obsahujícího oznámení o odstoupení. Odstoupením od smlouvy zanikají po úhradě fakturovaných služeb všechna práva a povinnosti smluvních stran.

6. Závěrečná ustanovení

Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu. Tuto smlouvu lze uzavřít výhradně písemně v listinné nebo elektronické podobě. Tuto smlouvu je možné měnit, doplňovat nebo rušit pouze písemnou formou. Pro právní vztahy z této smlouvy vyplývající platí příslušná ustanovení zákona č. 89/2012 Sb., občanského zákoníku a dalších obecně závazných právních předpisů České republiky. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s plněním této smlouvy budou řešit přednostně dohodou.

Tato smlouva je vyhodnocena ve dvou výtiscích s platností originálu, z nichž podnik obdrží jedno a pověřenec druhé vyhotovení této smlouvy.

PODNIK

V:

DNE:

PODPIS:

DPO

V:

DNE:

PODPIS: