

Název:	Směrnice GDPR o ochraně osobních údajů
--------	---

Vazba na legislativu:	zákon č. 101/2000 Sb. o ochraně osobních údajů, evropská právní úprava Nařízením Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů, dále též jen „GDPR“
Závazné pro:	LESCUS Cetkovice, s.r.o.
Účinnost od:	25. 5. 2018
Účinnost do:	Neomezena

Úvod

Firma s ohledem na jí ukládané povinnosti, a to jak českou právní úpravou (zákonem č. 101/2000 Sb. o ochraně osobních údajů), tak i evropskou právní úpravou (Nařízením Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů, dále též jen „GDPR“) tímto přijímá tuto směrnici, která stanoví pravidla pro všechny pracovníky firmy.

Účelem této směrnice je zajištění ochrany osobních údajů fyzických osob, s nimiž přijdou pracovníci firmy do styku, jakožto i naplnění dalších zákonných požadavků kladených na firmu. Veškerá ustanovení této směrnice musí být vykládána v souladu s výše uvedeným účelem směrnice, když veškerá ustanovení musí být vyložena ve prospěch zajištění maximálního naplnění účelu této směrnice.

Každý z pracovníků firmy je oprávněn a zároveň povinen upozornit svého nadřízeného, případně přímo vedení firmy, na nesoulad této směrnice s faktickým, popřípadě právním stavem, a za účelem odstranění tohoto nežádoucího stavu navrhnout přijetí vhodných opatření. Pokud tato směrnice vymezuje konkrétní pojmy, skutečnosti, nebo vlastnosti úžeji, než vyplývá z rozhodných právních předpisů, pak toto zúžení nezakládá odlišný obsah pojmu, skutečnosti nebo vlastnosti, ale má sloužit pouze k jednoduššímu vysvětlení obsahu pojmu, skutečnosti nebo vlastnosti, a to pro účely této směrnice.

OBSAH

PREAMBULE	1
OBSAH.....	1
ČLÁNEK 1 – ÚVODNÍ USTANOVENÍ.....	2
ČLÁNEK 2 – ZÁKLADNÍ ZÁSADY NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI	2
ČLÁNEK 3 – PRÁVA A POVINNOSTI PRACOVNÍKŮ JAKO SUBJEKTU ÚDAJŮ	3
ČLÁNEK 4 – INFORMOVÁNÍ SUBJEKTU ÚDAJŮ.....	4
ČLÁNEK 5 – NĚKTERÁ TECHNICKÁ OPATŘENÍ.....	5
ČLÁNEK 6 – ZÁVĚREČNÁ USTANOVENÍ.....	5

ČLÁNEK 1 – ÚVODNÍ USTANOVENÍ

1. Osobními údaji jsou veškeré informace o fyzické osobě, na jejichž základě je možné tuto osobu přímo nebo nepřímo identifikovat. Za takovýto osobní údaj se považuje kromě typicky identifikačních údajů (datum narození, jméno, příjmení, rodné číslo, apod.) taktéž údaj o její funkci v konkrétní právnické osobě, lokační nebo komunikační údaje, nebo jeden či více prvků fyzické, fyziologické, ekonomické, nebo společenské identity osoby.
2. Zpracováním osobních údajů je jejich jakékoliv zobrazení, užití, archivace, popřípadě prosté uvedení do databáze firmy.
3. K zpracování osobních údajů bude docházet výlučně u firmy s tím, že pokud by tato chtěla pověřit zpracováním osobních údajů externího zpracovatele (např. externí účetní, apod.), pak takovýto subjekt musí nakládat s osobními údaji v souladu se shora uvedenými právními předpisy.
4. Případný externí zpracovatel musí být smluvně zavázán k tomu, aby poskytoval firmě součinnost při výkonu práv subjektů údajů, oznamoval bezpečnostní incidenty ve smyslu ustanovení čl. 33 a 34 GDPR, a tyto řešil, a dále umožnil provádět firmě audity pro ni zpracovávaných údajů, včetně umožnění provádění inspekcí. Za tímto účelem bude do smluv s externími zpracovateli vkládána doložka, která bude znít následovně: *„Zpracovatel je povinen firmě poskytovat součinnost při výkonu práv subjektů údajů, písemně oznamovat bezpečnostní incidenty ve smyslu ustanovení čl. 33 a 34 GDPR, a tyto řešit, a umožnit firmě provádět audity pro ni zpracovávaných údajů, včetně umožnění provádění inspekcí u zpracovatele. Zpracovatel je taktéž povinen plnit veškeré povinnosti vyplývající přímo zpracovateli z rozhodných právních předpisů, tak také povinnosti ukládané firmě, která tyto povinnosti bude plnit prostřednictvím zpracovatele.“*

ČLÁNEK 2 – ZÁKLADNÍ ZÁSADY NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

1. Osobní údaje mohou být firmou zpracovávány pouze na základě zákonného důvodu, typicky z důvodu nezbytnosti plnění smlouvy, popřípadě zákonné povinnosti, nebo subjekt poskytne firmě souhlas se zpracováním svých osobních údajů.
2. Osobní údaje mohou být zpracovány pouze pro účely sledování legitimního cíle – tedy zejména naplnění smluvních povinností, zákonných archivačních, účetních nebo daňových povinností, ostrahy a ochrany majetku. Pokud by osobní údaje měly být zpracovány i nad rámec důvodů uvedených výše, pak k tomuto zpracování musí firma získat souhlas konkrétní osoby.
3. Osobní údaje musí být zpracovávány přiměřeně, relevantně a omezeně s ohledem na účel jejich zpracování, tedy firma nebude zpracovávat větší objem osobních údajů, než je pro účely jejich zpracování nezbytné.
4. Pracovníci firmy budou i s ohledem na práva subjektu údajů ověřovat aktuálnost, a tedy přesnost zpracovávaných osobních údajů.
5. Osobní údaje budou ukládány u firmy v nezbytně nutném rozsahu k naplnění účelu jejich zpracování, a to při respektování skutečnosti, že k daným osobním údajům budou mít přístup pouze pracovníci, u nichž je dána potřeba zajištění přístupu k těmto osobním údajům.
6. Pracovníci firmy jsou povinni zajistit, aby osobní údaje jak obchodních partnerů, tak případně pracovníků firmy i dalších osob, byly konkrétní osobou zpracovávány s maximálním důrazem na zachování jejich ochrany.

ČLÁNEK 3 – PRÁVA A POVINNOSTI PRACOVNÍKŮ JAKO SUBJEKTU ÚDAJŮ

1. Pracovníci firmy jsou povinni při každé změně svých osobních údajů, které o nich firma zpracovává, tuto změnu oznámit firmě. Firma zpracovává o pracovnících osobní údaje zahrnující:
 - a) identifikační údaje – jméno, příjmení, datum narození, rodné číslo, bydliště,
 - b) zdravotní údaje – zdravotní údaje jsou shromažďovány v rozsahu zdravotní způsobilosti a dále případných zdravotních omezení; firma nezpracovává jiné údaje o zdravotním stavu pracovníků vyjma údajů nezbytných pro plnění povinností zaměstnavatele,
 - c) registrační údaje pro účely odvodů – zdravotní pojišťovna, daňově uplatnitelné odpočty, slevy, apod.,
 - d) další údaje, pokud jejich zpracování je nezbytné pro účely plnění dalších povinností zaměstnavatele (např. držení řidičského oprávnění, apod.).
2. Pracovníci firmy berou na vědomí, že firma zpracovává jejich osobní údaje, a to i citlivé osobní údaje, a to pro účely daňové, sociální, účetní, apod. Zpracování těchto osobních údajů je nezbytné pro plnění povinností vyplývajících z dotčených právních předpisů, a to jak povinností vyplývajících pro firmu jakožto zaměstnavatele, tak i pro plnění povinností jednotlivých pracovníků. V případě nesdělení daných údajů nebude moci firma plnit předmětné povinnosti.
3. Pracovníci firmy jsou povinni sdělovat firmě změny svých údajů, a to za účelem zajištění správnosti, úplnosti a autenticity údajů zpracovávaných firmou, zároveň se jedná o právo jednotlivých pracovníků požadovat opravu jednotlivých evidovaných údajů. Za účelem ověření správnosti a autenticity údajů je firma povinna vyhovět žádosti pracovníka o sdělení údajů, které o něm jsou zpracovávány, a to ve formě potvrzení o tom, jaké osobní údaje jsou zpracovávány v jakém rozsahu, za jakým účelem, apod.
4. Firma zpracovává mzdovou a personální agendu.
5. Všichni pracovníci firmy jsou oprávněni se obrátit na dozorový orgán.
6. Jakmile odpadne důvod pro zpracování osobních údajů, kdy pracovník byl s firmou ve smluvním (zejména pracovněprávním vztahu), je firma povinna vymazat osobní údaje pracovníka.
7. Firma není oprávněna činit jakékoliv rozhodování v záležitostech pracovníka pouze na základě automatizovaného zpracování jeho osobních údajů, ani provádět jakékoliv jeho profilování, a to vyjma zařazování pracovníka k výkonu těch prací, ke kterým má zdravotní způsobilost.
8. Firma nezpracovává osobní údaje pracovníka z titulu jeho souhlasu, ale pouze z titulu plnění zákonných povinností. Firma osobní údaje získává primárně od pracovníka, čímž však není dotčeno, aby firma mohla získat osobní údaje i z jiných veřejně dostupných zdrojů nebo databází subjektů, ve vztahu ke kterým plní právní povinnosti.
9. Firma je povinna informovat pracovníka o jakémkoliv ohrožení jeho osobních údajů.
10. V případě, že firma zřídí pověřence pro ochranu osobních údajů, pak je povinna pracovníkům tuto skutečnost sdělit, a to včetně náležité identifikace tohoto pověřence.
11. V případě, že kterýkoliv pracovník zjistí, že u firmy dochází k rozsáhlému pravidelnému a systematickému monitorování subjektů údajů, je na toto povinen písemně upozornit firmu, aby zajistila pověřence pro ochranu osobních údajů.
12. Každý pracovník je povinen informovat firmu o jakémkoliv jím zjištěném ohrožení osobních údajů jeho i třetích osob.
13. Žádosti subjektu údajů ohledně uplatnění práva na:
 - a) přenositelnost,
 - b) omezení zpracování (žádost o dočasný přesun do jiného systému nebo znepřístupnění),
 - c) vydání potvrzení o zpracovávání údajů o něm,
 - d) opravu,

- e) vymazání,
- f) informace o přijatých opatřeních,
vyřídí bez zbytečného odkladu, nejpozději však do 30 dnů pověřený pracovník, který předem písemně informuje svého nadřízeného a po odsouhlasení nadřízeným pracovníkem zašle subjektu údajů zprávu o způsobu a termínu vyřešení jeho žádosti.

ČLÁNEK 4 – INFORMOVÁNÍ SUBJEKTU ÚDAJŮ

1. Firma informuje své obchodní partnery o skutečnosti, že o nich zpracovávají osobní údaje a o veškerých právech, které jim z rozhodných právních předpisů vyplývají. Tyto údaje jsou následující:

- a) *identifikační údaje – jméno, příjmení, datum narození, bydliště/sídlo, identifikační číslo, údaje o zápisu do registrů (např. obchodní, živnostenský), identifikační údaje odpovědných osob,*
- b) *další údaje, pokud jejich zpracovávání je nezbytné pro účely plnění dalších povinností firmy (např. údaje nezbytné pro realizaci zakázky),*
- c) *údaje dotýkající se platební morálky, a to zejména za účelem řádného vedení účetnictví, sledování insolvenčních a jiných obdobných rejstříků.*

Zpracování osobních údajů obchodních partnerů je nezbytné pro plnění povinností vyplývajících z dotčených právních předpisů, případně plnění smluvních závazků firmy. V případě nesdělení daných údajů nebude moci firma plnit předmětné povinnosti.

Obchodní partner je povinen sdělovat firmě změny svých údajů, a to za účelem zajištění správnosti, úplnosti a autenticity údajů zpracovávaných firmou. Zároveň má obchodní partner právo požadovat opravu jednotlivých evidovaných údajů. Za účelem ověření správnosti a autenticity údajů je firma povinna vyhovět žádosti obchodního partnera o sdělení údajů, které o něm jsou zpracovávány, a to ve formě potvrzení o tom, jaké osobní údaje jsou o něm zpracovávány v jakém rozsahu, za jakým účelem, apod.

V případě, že firma zřídí pověřence pro ochranu osobních údajů, pak je povinna obchodnímu partnerovi tuto skutečnost sdělit, a to včetně náležité identifikace tohoto pověřence.

Firma zpracovává účetní agendu.

Každý ze subjektů, o němž firma zpracovává osobní údaje, je oprávněn se obrátit na dozorový orgán.

Jakmile odpadne důvod pro zpracování osobních údajů, kdy obchodní partner naposledy realizoval obchodní spolupráci s firmou, je firma povinna vymazat osobní údaje obchodního partnera.

Firma je povinna informovat obchodního partnera o jakémkoliv ohrožení jeho osobních údajů. Firma případy porušení ochrany osobních údajů ve smyslu čl. 33 GDPR ohlásí Úřadu pro ochranu osobních údajů do 72 hodin. Tuto povinnost firma nebude mít v případě, že je velmi nepravděpodobný vliv na riziko úniku osobních údajů.

Firma bude zpracovávat osobní údaje obchodních partnerů pouze pro účely zákonné, archivační, daňové a účetní.

Žádosti obchodních partnerů ohledně uplatnění práva na:

- a) *přenositelnost,*
- b) *omezení zpracování (žádost o dočasný přesun do jiného systému nebo zneprístupnění),*
- c) *opravu, vydání potvrzení o zpracovávání údajů o něm,*
- d) *vymazání,*
- e) *informace o přijatých opatřeních,*

vyřídí bez zbytečného odkladu, nejpozději však do 30 dnů pověřený pracovník, který předem písemně informuje svého nadřízeného a po odsouhlasení nadřízeným zašle obchodnímu partnerovi zprávu o způsobu a termínu vyřešení jeho žádosti.

Nabídka produktů:

Podle § 7 ZSIS, stejně jako dle čl. 13 e-Privacy, je možné šířit obchodní sdělení pouze se souhlasem příjemce. Výjimkou je zaslání nabídek obdobných produktů a služeb elektronickou poštou na kontakty, které správce získal v souvislosti s prodejem svého zboží a služeb. V takovém případě je možné zaslání nabídek bez souhlasu, tedy za podmínky, že správce při získání kontaktu a při každém dalším obchodním sdělení umožní adresátovi jednoduchým způsobem zdarma zaslání nabídek odmítnout.[10] Tato výjimka pokrývá obchodní sdělení zasláná formou e-mailu či textové zprávy,[11] nevztahuje se však na telefonní marketing, který podléhá souhlasu vždy.

ČLÁNEK 5 – NĚKTERÁ TECHNICKÁ OPATŘENÍ

1. Firma je povinna realizovat veškerá nezbytná technická opatření k zajištění náležité ochrany osobních údajů, a to jak svých pracovníků, tak obchodních partnerů.
2. Pracovníci firmy jsou povinni navrhopvat svým jednotlivým vedoucím pracovníkům přijetí nezbytných opatření k zajištění náležité ochrany osobních údajů subjektu údajů.
3. Pracovníci jsou povinni zejména zajistit, aby jakékoliv osobní údaje obchodních partnerů popřípadě pracovníků firmy i dalších osob nebyly uloženy na pracovních stolech, popřípadě v jiných prostorách, kde by měly bez dalšího přístup jiné osoby, než konkrétní pověřeni pracovníci.
4. V případě, že není s osobními údaji pracovníků nebo obchodních partnerů pracováno, tyto musí být (ve své fyzické podobě) uloženy v neprůhledných složkách a musí být uloženy v uzamykatelných, resp. uzamknutých prostorách, skříních, ke kterým budou mít zajištěn přístup pouze oprávněné osoby.
5. V případě, že není s osobními údaji pracovníků nebo obchodních partnerů pracováno, tyto musí být (v elektronické podobě) uloženy pouze v PC nebo v noteboocích či na datových nosičích (včetně zálohových médií), které jsou dostatečně zahaslovány. Tato opatření platí také pro osobní údaje uložené ve všech ostatních elektronických zařízeních.
6. Údaje o subjektech údajů budou likvidovány po uplynutí příslušných zákonných archivačních, účetních, popřípadě daňových lhůt. O tomto předem pracovník provádějící likvidaci informuje svého nadřízeného.
7. Likvidace listinných dokumentů musí být prováděna tak, aby po provedené likvidaci nebyly čitelné ani jakkoliv jinak zjistitelné údaje o subjektech údajů.
8. Likvidace elektronických údajů musí být prováděna tak, aby byly likvidace (vymazání, fyzická likvidace média, apod.) provedeny úplně, tedy tak, aby je nebylo možno dohledat.
9. Pracovníci firmy nejsou oprávněni užívat vedením firmy či alespoň nadřízeným pracovníkem neschválený software, www aplikace či platformy.
10. Při zaslání jakýchkoliv osobních údajů elektronickou cestou, je příslušný odesílající pracovník povinen si nejprve ověřit soulad příslušné osoby adresáta a cílové elektronické adresy či úložiště dané osoby.
11. V případě, že by ve firmě byly shromažďovány biometrické údaje (např. otisky prstů v docházkových systémech), tak je příslušný pracovník, který za zavedení odpovídá, povinen o zavedení písemně informovat vedení společnosti (nejlépe přímo statutární orgán) a informovat o splnění povinností ve smyslu plnění předpisů na ochranu osobních údajů. Firma případy porušení ochrany osobních údajů ve smyslu čl. 33 GDPR ohlásí Úřadu pro ochranu osobních údajů do 72 hodin. Tuto povinnost firma nebude mít v případě, že je velmi nepravděpodobný vliv na riziko úniku osobních údajů.

ČLÁNEK 6 – ZÁVĚREČNÁ USTANOVENÍ

1. Vedoucí pracovníci jsou povinni zajistit seznámení všech pracovníků firmy s touto směrnici, jakožto i její důsledné naplňování.