Interní směrnice o zpracování osobních údajů dle GDPR

Verze Interní směrnice: **v.1 od 8.7.2021**
Správce osobních údajů: MSM Group s r.o. IČO: 27355462 Se sídlem U Sluncové 666/12a, 186 00 Praha 8
Interní směrnice: tato Interní směrnice ve formě předpisu upravuje ochranu a zpracování osobních údajů, k provedení Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27 dubna 2016 (dále jen „Nařízení") a dalších předpisů, účinných od 25 května 2018
Schválil: Jevgenij Kolesnik, jednatel společnosti Dne: 08.07.2021
Platnost a účinnost: od 08.07.2021 na dobu neurčitou
Příloha: písemný záznam o poučení a seznámení s obsahem tohoto vnitřního předpisu

Čl. 1 Obecná ustanovení

1.1 Předmět a cíle vnitřního předpisu
Tento vnitřní předpis upravuje pravidla a postup správce při ochraně a zpracování osobních údajů fyzických osob, které správce při výkonu své pracovní činnosti zpracovává.

1.2 Působnost vnitřního předpisu
Tento vnitřní předpis je závazný pro správce jako zaměstnavatele, všechny jeho zaměstnance a osoby, které zpracovávají osobní údaje pro správce na základě smlouvy.

1.3 Aktualizace vnitřního předpisu
Obsah vnitřního předpisu je pravidelně, vždy jsou ročně, jinak kdykoliv podle potřeby, kontrolován, vyhodnocován a aktualizován pověřeným zaměstnancem správce, kterým je vedoucí společností.

1.4 Přístup k vnitřnímu předpisu
Vnitřní předpis je veřejně přístupný všem zaměstnancům správce, stejně jako fyzickým osobám, jejichž údaje správce zpracovává.

Čl. 2 Základní pojmy

Podle tohoto vnitřního předpisu a podle právních předpisů:

2.1 „**Osobními údaji**" jsou 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.

2.2 „**Subjektem údajů**" jsou fyzické osoby – zaměstnanci správce či jiné fyzické osoby („klienti správce"), jejichž osobní údaje správce při své pracovní činnosti zpracovává;

2.3 „**Zpracováním**" jsou jakékoliv operace nebo soubory operací s osobními údaji nebo se soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako jsou 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;

2.4 „**Omezením zpracování**" jsou označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

2.5 „**Evidencí**" je jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií;

2.6 „**Správcem**" jsou fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Evropské unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

Správcem podle tohoto vnitřního předpisu je společnost MSM Group s r.o.,
IČO: 27355462, se sídlem U Sluncové 666/12a, 186 00 Praha 8

2.7 „**Zpracovatelem**" jsou fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

2.8 „**Souhlasem**" subjektu údajů je jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

2.9 „**Dozorovým úřadem**" je nezávislý orgán veřejné moci zřízený členským státem podle článku 51 Nařízení;

dozorovým úřadem správce je Úřad pro ochranu osobních údajů, sídlem Pplk. Sochora 727, 170 00 Praha 7. Tentýž úřad je dozorovým úřadem v případě přeshraničního zpracování osobních údajů;

k právnímu jednání a zastupování správce při jednání s dozorovými úřady je určen jednatel společností MSM Group s.r.o.;

2.10 „**Oprávněnou osobou**" je každý zaměstnanec správce (nebo osoba, která zpracovává osobní údaje pro správce na základě smlouvy), který z důvodu výkonu svého zaměstnání pro správce přichází do styku s osobními údaji nebo je zpracovává. Oprávněné osoby musejí

být poučeny, seznámeny s obsahem tohoto vnitřního předpisu; o poučení a seznámení je sepsán písemný záznam. Oprávněné osoby je nutné opětovně poučit, pokud došlo ke změně jejich pracovního zařazení či k jiné změně mající za následek změnu či rozsah pracovních úkonů oprávněné osoby ve vztahu ke zpracování osobních údajů. Přístup k osobním údajům subjektů údajů je striktně omezen pouze na poučené oprávněné osoby;

2.11 „**Odpovědnou osobou**" je pověřený zaměstnanec správce (nebo pověřená osoba na základě smluvního vztahu), který je pověřen správcem plnit práva a povinnosti správce podle tohoto vnitřního předpisu vůči subjektům údajů a být kontaktním místem správce se subjekty údajů.

Odpovědná osoba není určena k právnímu jednání a zastupování správce s dozorovými úřady.

Čl. 3 Zásady zpracování osobních údajů

Zpracování osobních údajů správcem podle tohoto vnitřního předpisu podléhá v souladu s právními předpisy těmto zásadám:

Osobní údaje musejí 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;
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; musejí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro něž se zpracovávají, byly bezodkladně vymazány nebo opraveny;
e. uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („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").

3.2 Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit.

Čl. 4 Účely a zákonnost zpracování a kategorie osobních údajů

4.1 Účely zpracování

Účely zpracování, pro které jsou osobní údaje určeny, jsou plnění smlouvy s klienty („subjekty údajů") správce, zejména pak vytvoření databáze klientů, kontaktování klientů ohledně sjednaných služeb; a dále pak plnění zákonných povinností.

4.2 Právní základ pro zpracování

Právním základem pro zpracování osobních údajů subjektu údajů je skutečnost, že zpracování je nezbytné pro splnění právních povinností, které se podle platných právních předpisů vztahují na správce podle čl. 6 odst. 1 písm. a), b), c) a e) Nařízení.

4.3 Identifikace osobních údajů

a. klientská agenda;
b. zaměstnanci a spolupracovníci;
c. provoz společnosti správce, daně, účetnictví;
d. obchod a marketing, komunikace online;
e. ostatní.

4.4 Kategorie osobních údajů

a. klientská agenda – jméno, příjmení, datum narození, státní příslušnost telefon, email, fotografie, adresa;
b. zaměstnanci a spolupracovníci – jméno, příjmení, datum narození, adresa, telefon, email, číslo účtu;
c. provoz společnosti správce, daně, účetnictví – jméno, příjmení, datum narození, adresa, telefon, email, číslo účtu;
d. obchod a marketing, komunikace online – jméno, příjmení, email;
e. ostatní – jméno, příjmení, telefon, email.

Čl. 5 Zdroje osobních údajů

Správce získává osobní údaje od následujících subjektů údajů:

a. klienti správce;
b. zaměstnanci a spolupracovníci;
c. třetí strany (dodavatelé apod.).

Čl. 6 Předávání a zpřístupnění osobních údajů subjektu údajů třetí straně

6.1 Správce může předávat či zpřístupnit osobní údaje subjektu údajů třetí straně jen v souladu s pokyny podle tohoto vnitřního předpisu. V případě pochybností nebo otázek při předání či zpřístupnění je třeba se předem dotázat na správný postup odpovědné osoby a vyčkat jejího rozhodnutí.

6.2 Správce zpřístupňuje osobní údaje následujícím příjemcům:

a. finanční ústavy;
b. státní aj. orgány v rámci plnění zákonných povinností stanovených přísl. právními předpisy;
c. třetí strany (pojišťovny, dodavatelé apod.);

6.3 Správce je oprávněn předávat či zpřístupnit osobní údaje subjektu údajů třetí straně v rámci dodržování účelu zpracování z důvodu dodržení právních povinností správce, řídí se přitom pokyny odpovědné osoby.

6.4 Mají-li být osobní údaje subjektu údajů předány či zpřístupnit třetí straně za jiným účelem, než za kterým byly shromážděny, mohou být předány či zpřístupněny jen po předchozím písemném souhlasu odpovědné osoby.

Čl. 7 Doba uchování osobních údajů subjektu údajů

7.1 V souladu se zásadou omezení uložení podle čl. 5 odst. 1 písm. e) Nařízení lze uchovávat osobní údaje subjektu údajů pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 2 Nařízení, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením s cílem zaručit práva a svobody subjektu údajů. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, dodržovat zásadu minimalizace údajů a osobní údaje anonymizovat, jakmile je to možné.

7.2 Konkrétní doby uchování osobních údajů:

Původ osobních údajů	**Požadovaná/maximální doba uchovávání**
Ze smlouvy	10 let od konce obchodního vztahu
Z marketingových aktivit	3 roky od získání těchto osobních údajů

Není-li určeno správcem, poté právními předpisy.

Čl. 8 Zabezpečení osobních údajů

8.1 Zabezpečení zpracování

Správce provádí zabezpečení osobních údajů a zabezpečení zpracování v souladu s pokyny podle tohoto vnitřního předpisu a v souladu s pokyny odpovědné osoby. V případě pochybností nebo otázek při zabezpečení osobních údajů a zabezpečení zpracování je třeba se předem dotázat na správný postup odpovědné osoby a vyčkat jejího rozhodnutí.

8.2 S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provádí správce vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně:

a. kódování souborů obsahujících osobní údaje;
b. zavedení technických a organizačních opatření pro zajištění bezpečnosti zpracování;
c. schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
d. schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.

8.3 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.

Čl. 9 Způsob zpracování osobních údajů

9.1 Zpracování osobních údajů provádí správce. Zpracování je prováděno v sídle správce jednotlivými pověřenými zaměstnanci správce. Ke zpracování dochází prostřednictvím výpočetní techniky a dále manuálním způsobem u osobních údajů v listinné podobě, a to za dodržení bezpečnostních zásad pro správu a zpracování osobních údajů.

9.2 Za tímto účelem přijal správce následující technickoorganizační opatření k zajištění ochrany osobních údajů, zejména opatření k vyloučení možnosti neoprávněného či nahodilého přístupu k osobním údajům, jejich změně, zničení či ztrátě, jakož i k jinému zneužití osobních údajů:

a. elektronické uchování osobních údajů:
   pro uchování a přenos osobních údajů využívá společnost interní registry, vyvinuté na základě xls tabulek. Přístup k souborům s osobními údaji je zajištěn heslem. Práci s osobními údaji provádí pouze odpovědná osoba na vyhrazeném počítači s antivirovým programem. Přístup k počítači je opatřen heslem.
b. listinné uchování osobních údajů:
   v uzamčených skříních, klíče uloženy v uzamykatelné schránce

Čl. 10 Poučení a práva subjektů údajů

10.1 V souladu s čl. 12 Nařízení informuje správce na žádost subjektu údajů subjekt údajů o právu na přístup k osobním údajům a k následujícím informacím:

a. účelu zpracování;
b. kategorii dotčených osobních údajů;
c. příjemci či kategorii příjemců, kterým jsou osobní údaje zpřístupněny;
d. plánované době, po kterou budou osobní údaje uloženy;
e. veškeré dostupné informace o zdroji osobních údajů.

10.2 Každý subjekt údajů, který zjistí, nebo se domnívá, že správce provádí zpracování jeho osobních údajů, které je v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu s právními předpisy, je oprávněn:

a. požádat správce o vysvětlení;
b. požadovat, aby správce odstranil takto vzniklý stav, zejména aby zablokoval, doplnil, opravil nebo vymazal osobní údaje, event. je subjekt údajů oprávněn obrátit se na dozorový orgán, tj. na Úřad na ochranu osobních údajů;

c. v případě oprávněnosti žádosti subjektu údajů dle bodu b), je správce povinen neprodleně odstranit závadný stav;
d. neodstraní-li správce závadný stav dle bodu c), subjekt údajů má právo obrátit se na dozorový orgán, tj. na Úřad na ochranu osobních údajů.

V Praze, dne 08. 07. 2021

Příloha

k Interní směrnice o zpracování osobních údajů dle GDPR v.1 od 8.7.2021

Seznam oprávněných osob, poučených a seznámených s obsahem tohoto vnitřního předpisu:

Odpovědná osoba	Datum	Podpis
1.		
2.		

Oprávněná osoba	Datum	Podpis
1.		
2.		

Interní směrnice řešení případů porušení zabezpečení osobních údajů

Verze Interní směrnice: **v.1 od 8.7.2021**
Správce osobních údajů: MSM Group s r.o. IČO: 27355462 Se sídlem U Sluncové 666/12a, 186 00 Praha 8
Interní směrnice: tato Interní směrnice ve formě předpisu upravuje hlavní povinnosti správce osobních údajů v případě, že dojde k porušení zabezpečení osobních údajů, tak jak je definováno v článku 4 odst. 12 GDPR Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen „Nařízení").
Schválil: Jevgenij Kolesnik, jednatel společnosti Dne: 08.07.2021
Platnost a účinnost: od 08.07.2021 na dobu neurčitou
Přílohy: Příloha č. 1 Diagram znázorňující požadavky na ohlášení Porušení zabezpečení Příloha č. 2 Příklady Porušení zabezpečení a postupů Přílohač. 3 Vzor Dokumentace záznamů všech ohlášených případů Porušení zabezpečení Písemný záznam o poučení a seznámení s obsahem této interní směrnice

Čl. 1 Úvodní ustanovení

1.1 Tato Interní směrnice ve formě předpisu (dále také „Předpis") upravuje některá práva a povinnosti oprávněné osoby MSM Group s.r.o. (dále „Správce") vyplývající z pracovněprávního vztahu k Správce nebo s tímto pracovněprávním vztahem související nebo smluvního vztahu. Tento Předpis dále upravuje práva a povinnosti osoby, která má provozní odpovědnost za vyřizování případů porušení (dále také „Odpovědná osoba").

1.2 Oprávněnou osobou se pro účely tohoto Předpisu rozumějí zaměstnanci pracující pro Správce v pracovním poměru, případně i další osoby vykonávající pro Správce činnosti na základě jiných právních titulů, zejména na základě dohody o provedení práce či dohody o pracovní činnosti nebo na základě smluvního vztahu.

1.3 Předpis je pro oprávněné osoby závazný a každá oprávněná osoba je povinna jej dodržovat.

Čl. 2 Vymezení pojmů

2.1 Osobními údaji se pro účely tohoto předpisu rozumějí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále též 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.

2.2 Porušením zabezpečení osobních údajů (dála také „Porušení zabezpečení") se pro účely tohoto předpisu rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

2.3 Porušení zabezpečení je bezpečnostní incident, který má za následek, že Správce není schopen zajistit soulad se zásadami zpracování osobních údajů. Jedná se o případy:

a) porušení důvěrnosti - porušení zabezpečení osobních údajů v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.
b) porušení dostupnosti - porušení zabezpečení osobních údajů v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů. Porušením dostupnosti je vždy incident, při kterém dojde k trvalé ztrátě nebo zničení osobních údajů, a to buď smazáním náhodným nebo úmyslným, zašifrováním dat, ztrátou dešifrovacího klíče a podobně.
c) porušení integrity - porušení zabezpečení osobních údajů v případě neoprávněného nebo náhodného pozměnění osobních údajů.

2.4 Porušení zabezpečení může být zjištěno zejména:

a) přímo Odpovědnou osobou
b) na základě upozornění oprávněné osoby
c) na základě upozornění subjektů údajů
d) na základě upozornění jiných třetích stran
e) na základě jiných informací (vč. informací publikovaných v médiích).

Čl. 3 Povinnosti oprávněné osoby

3.1 Tento Předpis vymezuje povinnosti oprávněné osoby při porušení zabezpečení osobních údajů, a to dle požadavků, které na Správce klade Nařízení (EU) č. 2016/679 (GDPR).

3.2 Každá oprávněná osoba, která porušení zabezpečení způsobí nebo se o porušení zabezpečení dozví nebo má důvod se domnívat, že k porušení zabezpečení došlo, či hrozí, má povinnost toto nahlásit odpovědné osobě. Při ohlašování porušení zabezpečení se oprávněné osoby řídí čl. 5. Pokud se oprávněné osobě z jakéhokoli důvodu nepodaří kontaktovat odpovědnou osobu, je povinna nahlásit výše uvedené skutečnosti svému nadřízenému.

3.3 Každá oprávněná osoba má povinnost poskytnout Odpovědné osobě součinnost při vyšetřování Porušení zabezpečení a při odstranění jeho následků.

Čl. 4 Povinnosti Odpovědné osoby při Porušení zabezpečení

4.1 Odpovědná osoba má následující povinnosti:

a) povinnost přijímat upozornění od zaměstnanců a jiných subjektů o Porušení zabezpečení,
b) povinnost jednat na základě prvního upozornění a vyšetřit Porušení zabezpečení,
c) v případě, že jsou splněny podmínky dle čl. VII, ohlásit bezodkladné Porušení zabezpečení dozorovému úřadu - Úřadu pro ochranu osobních údajů (dále také „ÚOOÚ") a spolupracovat s ÚOOÚ úřadem při vyšetřování Porušení zabezpečení,
d) v případě, že jsou splněny podmínky dle čl. VIII, oznámit Porušení zabezpečení subjektům údajů,
e) povinnost vést záznamy a dokumentovat veškeré případy Porušení zabezpečení, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

4.2 Odpovědná osoba se při plnění povinností uvedených v odst. 1 tohoto článku řídí následujícími ustanoveními Předpisu, jakož i postupy uvedenými v příloze č. 1 a příloze č. 2.

Čl. 5 Povinnost Odpovědné osoby přijímat upozornění o Porušení zabezpečení

5.1 Odpovědná osoba má za účelem přijímání upozornění zřízený e-mail msmpraha@seznam.cz. Odpovědná osoba dále přijímá upozornění o Porušení zabezpečení na tel. +420 724 923 495.

5.2 Všichni oprávněné osoby mohou upozornit na Porušení zabezpečení na e-mail uvedený v odst. 1, tel. Odpovědné osoby a dále mohou Odpovědnou osobu kontaktovat přímo ústně nebo prostřednictvím písemného podání. Oprávněné osoby mají povinnost zvolit takový způsob upozornění Odpovědné osoby, aby se Odpovědná osoba o Porušení zabezpečení dozvěděla bezodkladně.

Čl. 6 Povinnosti Odpovědné osoby při vyšetřování Porušení zabezpečení

6.1 Odpovědná osoba má povinnost prošetřit každé upozornění obdržené dle čl. V nebo jiné obdržené upozornění o Porušení zabezpečení.

6.2 Odpovědná osoba pravidelně kontroluje, zda neobdržela ohlášení Porušení zabezpečení některým uvedeným způsobem dle čl. 5.

6.3 Odpovědná osoba může požádat při vyšetřování Porušení zabezpečení příslušný útvar Správce, který poskytne Odpovědné osobě součinnost.

6.4 Odpovědná osoba při prošetřování Porušení zabezpečení postupuje následujícím způsobem:

a) Odpovědná osoba na základě obdržených informací posoudí, zda k Porušení zabezpečení skutečně došlo;
b) Odpovědná osoba vyhodnotí, o který druh Porušení zabezpečení se jedná (viz čl. 2.3);
c) Odpovědná osoba vyhodnotí možné důsledky a rizika Porušení zabezpečení pro subjekty údajů (např. materiální, či imateriální škoda, krádež identity, podvod apod.), spolu s množstvím údajů, u nichž došlo k Porušení zabezpečení;
d) Odpovědná osoba vyhodnotí, zda je nutné Porušení zabezpečení dle čl. VII ohlásit ÚOOÚ a dle čl. VIII oznámit subjektům údajů;
e) Odpovědná osoba navrhne opatření k řešení daného Porušení zabezpečení, včetně vhodných opatření ke zmírnění možných nepříznivých dopadů (např. zprovoznění záložní kopie v případě porušení dostupnosti údajů).

Čl. 7 Povinnost ohlásit Porušení zabezpečení ÚOOÚ a spolupracovat s ním

7.1 Na základě provedeného šetření dle čl. VI Odpovědná osoba vyhodnotí, zda je Porušení zabezpečení nutno ohlásit ÚOOÚ.

7.2 Porušení zabezpečení Odpovědná osoba ohlásí ÚOOÚ v každém případě, pokud k Porušení zabezpečení skutečně došlo, mimo případy kdy:
a) došlo k Porušení zabezpečení, které nemá a nemůže mít žádný vliv na subjekty údajů,
b) došlo ke ztrátě zařízení, které je však bezpečně zašifrované a není zde možnost, že by mohlo být zneužito třetí osobou,
c) došlo k Porušení zabezpečení, ale osoba, která osobní údaje obdržela, je důvěryhodná, data zaslala zpět, či je bezpečně zničila.

Při posuzování nutnosti ohlásit Porušení zabezpečení ÚOOÚ se Odpovědná osoba přiměřeně řídí příklady uvedenými v příloze č. 2.

7.3 Odpovědná osoba má povinnost ohlásit Porušení zabezpečení ÚOOÚ bez zbytečného odkladu po tom, co je potvrzeno, že k Porušení zabezpečení došlo a bylo zjištěno, že toto porušení vyžaduje ohlášení ÚOOÚ. Odpovědná osoba Porušení zabezpečení ohlásí ÚOOÚ nejpozději do 72 hodin od okamžiku jeho zjištění.

7.4 V případě, že Odpovědná osoba neohlásí Porušení zabezpečení ve stanovené lhůtě, bude ÚOOÚ informovat bezodkladně a kromě informací uvedených v následujícím odstavci uvede Odpovědná osoba v ohlášení také důvody zpoždění při ohlášení a tyto důvody doplní dokumentací prokazující důvody zpoždění.

7.5 Při ohlašování Porušení zabezpečení ÚOOÚ Odpovědná osoba uvede:
a) popis povahy daného případu Porušení zabezpečení včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
b) své jméno a kontaktní údaje;
c) popis pravděpodobných důsledků Porušení zabezpečení;
d) popis opatření, která Správce přijal nebo navrhl s cílem vyřešit dané Porušení zabezpečení, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

7.6 Nemůže-li Odpovědná osoba poskytnout všechny údaje uvedené v odst. V tohoto článku současně, poskytne je ÚOOÚ následně bez dalšího zbytečného odkladu.

Čl. 8 Povinnost oznámit Porušení zabezpečení subjektům údajů

8.1 Pokud je pravděpodobné, že určitý případ Porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Odpovědná osoba toto Porušení zabezpečení bez zbytečného odkladu subjektu údajů.

8.2 V oznámení subjektu údajů podle odstavce 1 tohoto článku použije Odpovědná osoba jasných a jednoduchých jazykových prostředků, popíše povahu Porušení zabezpečení a uvede v něm přinejmenším informace a opatření uvedená v čl. VII odst. 5 písm. b), c) a d) a je-li to možné, také kroky, které mohou subjekty údajů učinit pro vlastní ochranu.

8.3 Oznámení subjektu údajů uvedené v odstavci 1 se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených Porušením zabezpečení. Jde zejména o taková opatření, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (např. šifrování);
b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 tohoto článku se již pravděpodobně neprojeví;
c) oznámení by vyžadovalo nepřiměřené úsilí, v takovém případě Odpovědná osoba zajistí, že subjekty údajů budou informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Čl. 9 Povinnost vést záznamy a dokumentovat případy Porušení zabezpečení

9.1 Odpovědná osoba dokumentuje všechny případy Porušení zabezpečení, které byly ohlášeny.

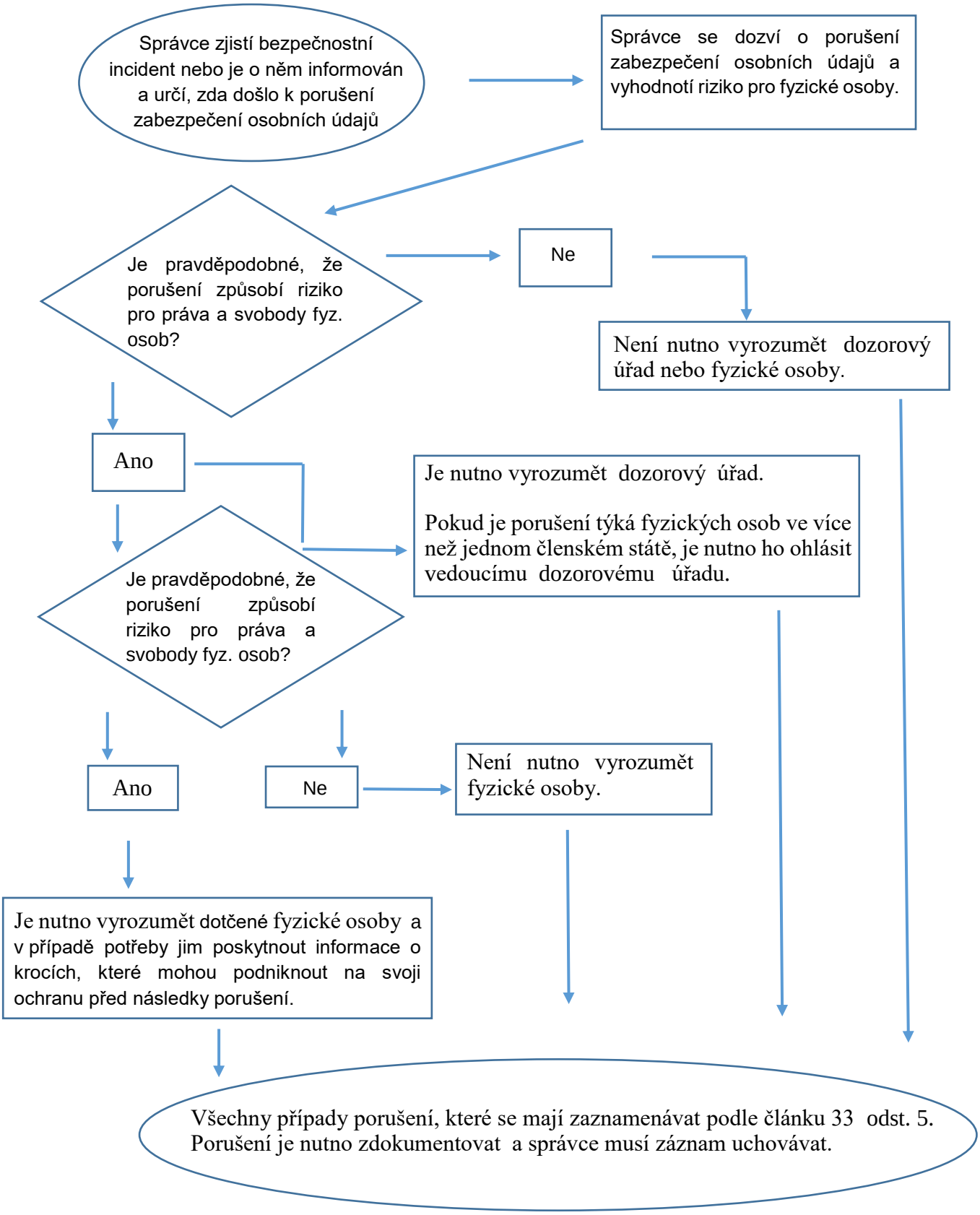
9.2 Odpovědná osoba dokumentaci vede v takové podobě, aby z ní byl zřejmý přinejmenším:

a) popis Porušení zabezpečení (popis toho, co se stalo),
b) datum, kdy bylo Porušení zabezpečení zjištěno,
c) zdroj zjištění Porušení zabezpečení,
d) osobní údaje dotčené Porušením zabezpečení,
e) zjištěné příčiny Porušení zabezpečení,
f) důsledky Porušení zabezpečení,
g) nápravná opatření přijatá Správce,
h) pokud bylo Porušení zabezpečení ohlášeno ÚOOÚ, či oznámeno subjektům údajů, také informace o tomto ohlášení a oznámení.

9.3 Pro vedení dokumentace Odpovědná osoba využívá přílohy č. 3.

V Praze, dne 08. 07. 2021

Diagram znázorňující požadavky na ohlášení Porušení zabezpečení



Zdroj: Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679 vytvořené Pracovní skupinou pro ochranu údajů zřízenou podle článku 29, přijaté dne 3. října 2017, revidované a přijaté dne 6. února 2018.

Příklady Porušení zabezpečení a postupů

Odpovědná osoba se při ohlašování Porušení zabezpečení přiměřeně řídí postupy uvedenými v této příloze.

Příklad	Je nutno vyrozumět	Je nutno vyrozumět subjekt	Poznámky a doporučení
i. Správce uložil zálohu archivu osobních údajů zašifrovaných na USB úložišti. Během vloupání dojde k odcizení úložiště.	Ne.	Ne	Pokud jsou údaje zašifrovány pomocí nejmodernějšího algoritmu, existují jejich zálohy, nebylo narušeno zabezpečení jedinečného klíče a údaje lze dostatečně rychle obnovit, nemusí se jednat o porušení, které je nutno ohlásit. Pokud však později dojde k narušení jejich zabezpečení, je nutno incident ohlásit.
ii. Správce provozuje online službu. V důsledku kybernetického útoku na tuto službu dojde k úniku osobních údajů fyzických osob. Správce má své zákazníky v jednom členském státě.	Ano, vyrozumějte dozorový úřad, pokud existuje pravděpodobnost důsledků pro fyzické osoby.	Ano, oznamte porušení fyzickým osobám v závislosti na povaze dotčených osobních údajů, a tehdy, pokud je závažnost pravděpodobných důsledků pro fyzické osoby vysoká.	
iii. V call centru správce dojde ke krátkému výpadku dodávky elektrického proudu, který trvá několik minut, takže zákazníci nemohou volat správce a mít přístup ke svým záznamům.	Ne.	Ne	Nejde o porušení, které se musí ohlásit, ale stále je to incident, který je nutno podle čl. 33 odst. 5 zaznamenat. Správce by měl uchovávat příslušné záznamy.
iv. Správce utrpí útok ransomwarem, který má za následek zašifrování všech údajů. Nejsou k dispozici žádné zálohy	Ano, vyrozumějte dozorový úřad, pokud existuje pravděpodobnost důsledků pro fyzické osoby, jelikož se jedná	Ano, vyrozumějte fyzické osoby v závislosti na povaze dotčených osobních údajů a možném dopadu nedostupnosti	Pokud by byla k dispozici záloha a údaje by bylo možno dostatečně rychle obnovit, není nutno tento incident ohlašovat dozorovému úřadu ani

a údaje nelze obnovit. Vyšetřování ukáže, že jedinou funkcí ransomwaru bylo zašifrování údajů a že v systému neexistuje žádný jiný škodlivý software.	o ztrátu dostupnosti.	údajů, jakož i na dalších pravděpodobných důsledcích.	oznamovat fyzickým osobám, protože by nedošlo k trvalé ztrátě dostupnosti nebo důvěrnosti. Pokud by se však dozorový úřad dozvěděl o incidentu jinými prostředky, může zvážit možnost provést šetření, aby posoudil soulad se širšími bezpečnostními požadavky článku 32.
v. Fyzická osoba zavolá do call centra banky, aby ohlásila porušení zabezpečení údajů. Osoba obdržela měsíční výpis z účtu někoho jiného. Správce provede krátké prošetření (tzn. takové, které dokončí během 24 hodin) a s přiměřenou mírou jistoty zjistí, zda skutečně došlo k porušení zabezpečení osobních údajů a zda se jedná o systémový nedostatek, který může znamenat, že jsou nebo mohou být dotčeny další osoby.	Ano.	Pokud existuje vysoké riziko a je zřejmé, že jiné osoby nebyly incidentem dotčeny, porušení se oznamuje pouze dotčeným fyzickým osobám.	Pokud se po dalším vyšetřování zjistí, že je dotčeno více fyzických osob, je nutno to ohlásit dozorovému úřadu a kromě toho správce oznámí porušení ostatním osobám, jestliže jim hrozí vysoké riziko.
vi. Správce provozuje internetové tržiště a má zákazníky ve více členských státech. Tržiště utrpí kybernetický útok a útočník zveřejní na internetu uživatelská jména, hesla a historii nákupů.	Ano, informujte vedoucí dozorový úřad, pokud se incident týká přeshraničního zpracování.	Ano, protože incident by mohl mít za následek vysoké riziko.	Správce by měl přijmout vhodná opatření, např. nucené přenastavení hesel dotčených účtů, jakož i další kroky ke zmírnění rizika. Správce by měl vzít v úvahu také případné další oznamovací povinnosti, např. podle směrnice o bezpečnosti sítí a informací jakožto poskytovatel digitálních služeb.

vii. Webhostingová firma působící jako zpracovatel údajů zjistí chybu v kódu, který řídí autorizaci uživatelů. V důsledku této chyby může každý uživatel přistupovat k podrobnostem účtu kteréhokoli jiného uživatele.	Jakožto zpracovatel musí webhostingová firma bez zbytečného odkladu vyrozumět své dotčené klienty (správce). Za předpokladu, že tato webhostingová firma provedla vlastní vyšetřování, měli by mít dotčení správci dostatečnou míru jistoty, zda každý z nich utrpěl porušení zabezpečení, a proto se bude pravděpodobně mít za to, že jakmile byli webhostingovou firmou (zpracovatelem) vyrozuměni, ví o dotyčném incidentu. Správce pak musí vyrozumět dozorový úřad.	Pokud fyzickým osobám pravděpodobně nehrozí vysoké riziko, není nutno jim incident oznamovat.	Webhostingová firma (zpracovatel) musí vzít v úvahu případné další oznamovací povinnosti (např. podle směrnice o bezpečnosti sítí a informací jakožto poskytovatel digitálních služeb). Pokud neexistují důkazy o tom, že by toto slabé místo bylo u některého z jejích správců zneužito, může to znamenat, že se nejedná o porušení, které je nutno ohlásit, avšak je pravděpodobné, že jde o incident, který se má zaznamenat, nebo který představuje nedodržení článku 32.
viii. V důsledku kybernetického útoku nej sou v nemocnici po dobu 30 hodin k dispozici zdravotní záznamy.	Ano, nemocnice je povinna incident ohlásit, jelikož může představovat vysoké riziko pro zdraví a soukromí pacienta.	Ano, incident je nutno oznámit dotčeným fyzickým osobám.	
ix. Osobní údaje velkého počtu studentů jsou nedopatřením odeslány do nesprávného seznamu zasílacích adres s více než 1000 příjemců.	Ano, incident je nutno ohlásit dozorovému úřadu.	Ano, vyrozumějte fyzické osoby v závislosti na rozsahu a typu osobních údajů a závažnosti možných důsledků.	
x. E-mailová zpráva pro účely přímého marketingu je zaslána příjemcům, kteří jsou všichni uvedeni v kolonce adresátů nebo příjemců kopie zprávy, takže každý příjemce vidí e-mailovou adresu ostatních příjemců.	Ano, ohlášení incidentu dozorovému úřadu může být povinné, pokud se týká velkého množství fyzických osob, pokud došlo k prozrazení citlivých údajů (např. seznam adres pacientů psychoterapeuta) nebo pokud jiné faktory představují vysoké riziko (např. pokud zpráva obsahuje původní hesla).	Ano, vyrozumějte fyzické osoby v závislosti na rozsahu a typu osobních údajů a závažnosti možných důsledků.	Ohlášení nemusí být nutné, pokud nejsou prozrazeny žádné citlivé údaje a pokud je prozrazen jen malý počet e-mailových adres.

Příloha č. 3

Vzor Dokumentace záznamů všech ohlášených případů Porušení zabezpečení

a) Popis Porušení zabezpečení:

……

b) Datum zjištění Porušení zabezpečení:

……

c) Zdroj zjištění Porušení zabezpečení:

……

d) Zjištění Odpovědné osoby.
Bylo zjištěno, že k Porušení zabezpečení skutečně došlo?

Ano □ Ne □

e) Osobní údaje dotčené Porušením zabezpečení:

……..

f) Zjištěné příčiny Porušení zabezpečení:

……

g) Důsledky Porušení zabezpečení:

……

h) Přijatá nápravná opatření:

……

i) Ohlášení Porušení zabezpečení ÚOOÚ (datum a obsah)

……

j) Oznámení Porušení zabezpečení subjektům údajů (datum a obsah)

…….

Příloha

k Interní směrnice řešení případů porušení zabezpečení

osobních údajů v.1 od 8.7.2021

Seznam zaměstnanců Společností, poučených a seznámených s obsahem této interní směrnice:

Odpovědná osoba	Datum	Podpis
1.		
2.		

Oprávněná osoba	Datum	Podpis
1.		
2.		
3.		
4.		

Внутренний регламент обработки персональных данных в соответствии с GDPR

Версия внутреннего регламента: **v.1 от 8.7.2021**
Контролер персональных данных: MSM Group s r. o. IČO: 27355462 Юридический адрес: U Sluncové 666/12a, 186 00 Прага 8
Внутренний регламент: этот внутренний регламент регулирует защиту и обработку персональных данных во исполнение постановления (ЕС) № 2016/679 Европейского парламента и Совета Европы от 27 апреля 2016 года (далее именуемый "регламент") и другие нормативные акты, вступившие в силу 25 мая 2016 года.
Утвердил: Евгений Колесник, директор компании Дата: 08.07.2021
Срок и начало действия: с 08.07.2021 на неограниченный срок
Приложение: ведомость инструктажа и ознакомления с содержанием настоящего внутреннего регламента

Ст. 1 Общие положения

1.1 Предмет и цели внутреннего регламента

Настоящий внутренний регламент (далее «регламент») регулирует правила и порядок действий контроллера по защите и обработке персональных данных физических лиц, которые контроллер обрабатывает в ходе своей профессиональной деятельности.

1.2 Сфера применения внутреннего регламента

Настоящий регламент является обязательным для контроллера, всех его сотрудников и лиц, которые обрабатывают персональные данные для контроллера на основании договора.

1.3 Актуализация внутреннего регламента

Содержание внутреннего регламента систематически, всегда ежегодно, либо по мере необходимости, проверяется, оценивается и обновляется уполномоченным сотрудником контроллера, являющимся руководителем компании.

1.4 Доступ к внутреннему регламенту

Внутренний регламент находится в открытом доступе для всех сотрудников контроллера, а так же для физических лиц, данные которых обрабатывает контроллер.

Ст. 2 Основные определения

В соответствии с регламентом и в соответствии с законодательством:

2.1 "Персональные данные" - любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько характерных для указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности;

2.2 "**Субъект данных**" - физическое лицо - сотрудники контроллера или другие физические лица ("клиенты контроллера"), чьи персональные данные обрабатываются контроллером в ходе его профессиональной деятельности;

2.3 "Обработка" означает любую операцию или набор операций, которые выполняются над персональными данными или над наборами персональных данных, автоматическими или не автоматическими средствами. Такие как сбор, запись, организация, структурирование, хранение, адаптация или изменение, просмотр, использование, раскрытие (путем передачи, распространения или иначе, делая их доступными), выравнивание или комбинирование, ограничение, удаление или уничтожение;

2.4 "Ограничение обработки" маркировка сохраненных персональных данных в целях ограничения их обработки в будущем;

2.5 "Картотека" означает любой структурированный набор персональных данных, которые доступны по определенным критериям.

2.6 "Контроллер" физическое или юридическое лицо, публичное учреждение, агентство или иная структура, которая самостоятельно или совместно с другими определяет цели и способы обработки персональных данных; если цели и способы такой обработки определены правовыми актами Европейского союза или государства-члена ЕС, то контроллер или частные критерии для его назначения могут быть предусмотрены этими правовыми актами;

контроллером в соответствии с этим регламентом является MSM Group s. r. o., IČO: 27355462, юр. адрес: U Sluncové 666/12a, 186 00 Прага 8

2.7 "Процессор" это физическое или юридическое лицо, государственный орган, агентство или другой орган, который обрабатывает личные данные от имени контроллера;

2.8 "Согласием" субъекта данных является любое свободное, конкретное, сознательное и однозначное указание на пожелания субъекта, которыми

субъект путем уведомления или чёткого подтверждающего действия даёт согласие на обработку своих персональных данных;

2.9 "Надзорное учреждение" – это независимое публичное учреждение, созданное Государством-членом ЕС с учётом Статьи 51;

надзорным учреждением контроллера является управление по защите персональных данных, которое находится по адресу Pplk. Sochora 727, 170 00 Praha 7. Это же управление является надзорным учреждением в случае трансграничной обработки персональный данных;

управляющий директор MSM Group s r. o. является лицом, уполномоченным представлять интересы контроллера в коммуникации с надзорными органами;

2.10 "Уполномоченное лицо" - любой сотрудник контроллера (или лицо, которое обрабатывает персональные данные для контроллера на основании договора), который в ходе своей работы для контроллера ознакомляется с персональными данными или обрабатывает их. Уполномоченные лица должны быть проинструктированы, ознакомлены с содержанием регламента; о чём составляется письменный протокол инструктажа и ознакомления. Уполномоченные лица должны быть повторно проинструктированы, если произошло изменение в классификации их должностей или любое другое изменение, повлекшее за собой изменение или объем работы уполномоченного лица в связи с обработкой персональных данных. Доступ к персональным данным субъектов данных строго ограничен и предназначен только проинструктированным уполномоченным лицам;

2.11 "Ответственное лицо" это сотрудник контроллера (либо уполномоченное лицо на), который уполномочен исполнять права и обязанности контроллера в соответствии с регламентом в отношении субъектов данных и быть контактным лицом контроллера с субъектами данных.

Ответственное лицо не уполномочено для ведения юридических переговоров и представления контроллера в надзорных органах.

Ст. 3 Принципы обработки персональных данных

Обработка персональных данных осуществляется контроллером в рамках регламента в соответствии со следующими принципами и правовыми нормами:

3.1 Персональные данные:

a. обрабатываются законно, честно, в предусмотренной для субъекта данных форме («законность, конкретность и прозрачность»);

b. собираются для конкретных, ясных и законных целей, и их дальнейшая обработка не осуществляется несовместимым с этими целями способом;
c. являются адекватными, актуальными и ограниченные в той мере, в какой это необходимо для целей обработки («минимизация данных»);
d. являются точными и, при необходимости, обновляются; необходимо принимать все разумные меры для того, чтобы обеспечить немедленное удаление или исправление неточных данных, с учётом целей, для которых они обрабатываются («точность»).
e. хранятся в форме, допускающей идентификацию субъектов данных, не дольше, чем это необходимо в целях, для которых обрабатываются персональные данные («ограничение по хранению»);
f. обрабатываются таким способом, чтобы была обеспечена безопасность персональных данных, в том числе защита от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения («целостность и конфиденциальность»).

3.2 Контроллер несёт ответственность за соответствие пункту 1 и обязан при необходимости это доказать.

Ст. 4 Цели, легитимность обработки и категории персональных данных

4.1 Цели обработки

Целями обработки, для которой используются персональные данные, являются выполнение контракта с клиентами ("субъектами данных") контроллера, в частности создание базы данных клиентов с целью установление контактов с клиентами по поводу договоренных услуг; а также исполнение обязательств в соответствии с действующим законодательством.

4.2. Правовая основа для обработки

Правовым основанием для обработки персональных данных субъекта данных является тот факт, что обработка необходима для выполнения юридических обязательств, которые возникают у контролера в соответствии с параграфом 6 статьей 1 пункт a), b), c) и e) Регламента.

4.3 Классификация персональных данных

a. клиентская база;
b. сотрудники и партнеры;
c. текущая деятельность компании, налогообложение, бухгалтерский учет;
d. бизнес, маркетинг, online коммуникация;
e. прочее.

4.4 Категории персональных данных

a. клиентская база - имя, фамилия, дата рождения, гражданство, телефон, электронная почта, фотография, адрес;
b. сотрудники и партнеры - имя, фамилия, дата рождения, адрес, телефон, электронная почта, номер счета;
c. текущая деятельность компании, налогообложение, бухгалтерский учет – имя, фамилия, дата рождения, адрес, телефон, электронная почта, номер счета;
d. бизнес, маркетинг, online коммуникация - имя, фамилия, адрес электронной почты;
e. прочее - имя, фамилия, телефон, электронная почта

Ст. 5 Источники персональных данных

Контролер получает персональные данные от следующих субъектов данных:

a. клиенты контроллера;
b. сотрудники и партнеры;
c. третьи стороны (поставщики и т.д.).

Ст. 6 Передача и раскрытие персональных данных субъекта данных третьей стороне

6.1 Контроллер может передавать или раскрывать персональные данные субъекта данных третьей стороне только в соответствии с инструкциями, предусмотренными регламентом. В случае сомнений или вопросов по поводу передачи или раскрытия информации следует заранее запросить ответственное лицо о правильной процедуре и дождаться его решения.

6.2 Контроллер предоставляет персональные данные следующим получателям:

a. финансовые органы;
b. государственные и другие органы в рамках выполнения законодательных норм;
c. третьи стороны (страховые компании, поставщики и т.д.);

6.3 Контроллер имеет право передавать или раскрывать персональные данные субъекта данных третьей стороне в рамках исполнения целей обработки в соответствии с юридическими обязательствами контролера, следуя инструкциям ответственного лица.

6.4 Если персональные данные субъекта данных должны быть переданы или предоставлены третьей стороне для целей, отличных от тех, для которых они были собраны, они могут быть переданы или предоставлены только с предварительного письменного согласия ответственного лица.

Ст. 7 Срок хранения персональных данных

7.1. В соответствии с принципом ограничения, упомянутым в статье 5, пункт 1 e) Регламента ЕС, можно сохранять персональные данные субъекта данных только в течение периода, необходимого для целей их обработки. По истечении этого периода персональные данные могут храниться исключительно в целях архивирования в общественных интересах, в целях научных или исторических исследований или в статистических целях, как указано в статье 89 (2), с условием, что права и свободы субъекта данных гарантируются при условии реализации соответствующих технических и организационных мер, предусмотренных Регламентом. При использовании в этих целях следует соблюдать право на защиту от несанкционированного вмешательства в частную и личную жизнь субъекта данных, соблюдать принцип минимизации данных и как можно скорее обезличивать персональные данные.

7.2 Конкретные сроки хранения личных данных:

Источник персональных данных	**Требуемый / максимальный срок хранения**
С момента заключения контракта	10 лет с момента окончания деловых отношений
От маркетинговой деятельности	3 года с момента получения этих персональных данных

Если не определено контроллером – то согласно действующему законодательству

Ст. 8 Защита персональных данных

8.1 Безопасность обработки

Контроллер обеспечивает безопасность персональных данных и безопасность обработки в соответствии с инструкциями и в соответствии с регламентом. В случае возникновения сомнений или вопросов относительно безопасности обработки персональных данных необходимо заранее узнать о правильной процедуре у ответственного лица и дождаться его решения.

8.2. Принимая во внимание состояние техники, стоимость выполнения, характер, объем, контекст и цели обработки, а также риски для прав и свобод физических лиц, контроллер должен принять соответствующие

технические и организационные меры для обеспечения уровня безопасности, соответствующего риску, в том числе, при необходимости:

a. кодировать файлы, содержащие персональные данные;
b. внедрять технические и организационные меры по обеспечению безопасности переработки;
c. обеспечивать постоянную конфиденциальность, целостность, доступность и стабильность обработки;
d. обеспечивать возможность своевременного восстановления доступности и доступа к персональным данным в случае физических или технических инцидентов.

8.3 При оценке надлежащего уровня безопасности следует учитывать, в частности, риски, связанные с обработкой, в частности случайное или незаконное уничтожение, потеря, изменение, несанкционированное раскрытие или несанкционированный доступ к персональным данным, передаваемым, хранящимся или иным образом обрабатываемым.

Ст. 9 Способ обработки персональных данных

9.1 Обработка персональных данных осуществляется контроллером по месту нахождения контроллера отдельными уполномоченными сотрудниками. Обработка персональных данных осуществляется с помощью компьютера, а также вручную в бумажной форме с соблюдением принципов безопасности обработки персональных данных.

9.2 С этой целью контроллер принял следующие технические и организационные меры для обеспечения защиты персональных данных, в частности меры по исключению возможности несанкционированного или случайного доступа к персональным данным, их изменению, уничтожению или потери, а также другого неправомерного использования персональных данных:

a. электронное хранение персональных данных:
   для хранения и передачи персональных данных компания использует внутренние реестры, разработанные на основе таблиц в формате xls. Доступ к файлам с персональными данными обеспечивается паролем. Работа с персональными данными осуществляется только ответственным лицом на выделенном компьютере с антивирусной программой. Доступ к компьютеру обеспечивается паролем.
b. документальное хранение персональных данных:
   в запертых шкафах, ключи хранятся в запирающемся ящике.

Ст. 10 Разъяснение и права субъектов данных

10.1 В соответствии со статьей 12 Регламента ЕС контроллер должен информировать субъекта данных по запросу субъекта данных о праве доступа к персональным данным и к следующей информации:

a. цель обработки;
b. категория затрагиваемых персональных данных;
c. получатели или категории получателей, которым раскрываются персональные данные;
d. планируемый период, в течение которого будут храниться персональные данные;
e. вся доступная информация об источнике персональных данных.

10.2 Субъект данных, который обнаружит или подозревает нарушение правовых норм касательно персональных данных, имеет право:

a. обратиться за разъяснениями к контроллеру;
b. потребовать от контроллера исправить возникшую ситуацию, в частности заблокировать, дополнить, скорректировать или удалить персональные данные. Так же субъект данных имеет право обратиться в надзорный орган, т.е. в управление по защите персональных данных;
c. в случае обоснованности запроса субъекта данных в соответствии с пунктом b), контроллер обязан незамедлительно устранить нарушение;
d. если контроллер не исправит спорную ситуацию в соответствии с пунктом c), субъект данных имеет право обратиться в надзорный орган, т.е. в управление по защите персональных данных.

Прага 08.07.2021

Приложение
к внутреннему регламенту обработки персональных данных в соответствии с GDPR v.1 от 8.7.2021

Список уполномоченных лиц, проинструктированных и ознакомленных с содержанием настоящего внутреннего регламента:

Ответственное лицо	**Дата**	**Подпись**

Уполномоченное лицо	**Дата**	**Подпись**
1.		
2.		
3.		