KASPEN/JUNGvMATT

SMĚRNICE

SPOLEČNOST:	**Kaspen s.r.o.**
NÁZEV DOKUMENTU:	**Ochrana osobních údajů ve společnosti**
GARANT DOKUMENTU:	**Tomáš Kopečný**
ZPRACOVATEL:	**Marcela Tylšová**
PLATNOST OD:	**01.05.2018**
ÚČINNOST OD:	**25.05.2018**
SCHVÁLIL:	**Tomáš Kopečný - jednatel**
PODPIS:	

OBSAH:

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

1 ÚVODNÍ USTANOVENÍ

1.1 Účel

Účelem tohoto dokumentu je stanovit všeobecně platnou metodiku pro nakládání a zpracování osobních údajů (dále jen OÚ) ve společnosti tak, aby byly zajištěny podmínky ochrany stanovené NAŘÍZENÍM EVROPSKÉHO PARLAMENTU A RADY (EU) 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 (obecné nařízení o ochraně osobních údajů, dále jen Nařízení) zákonem č. 101/2000 Sb., o ochraně osobních údajů, zákonem č. 127/2005Sb., o elektronických komunikacích a směrnicí, zákona č. 181/2014 Sb., o kybernetické bezpečnosti a podmínky, za kterých se OÚ zpracovávají ve společnosti, a to za účelem zajištění jejich řádné ochrany a zabránění jejich úniku, vyzrazení, zneužití, zničení a zamezení jejich ztrát.

Cílem je stanovit hlavní a jednoznačné zásady odpovědnosti, povinnosti a pravomoci při zpracování a zabezpečování ochrany OÚ ve společnosti. Tato směrnice stanovuje, povinnost, aby společnosti zpracovávající OÚ zpracovávaly pouze údaje, které potřebují k výkonu svých činností a zároveň jsou oprávněni tyto OÚ zpracovávat, aby vynaložily veškerou péči na eliminaci rizik spojených se zneužitím, nesprávným nakládáním, nesprávným stanovením účelu zpracování nebo neoprávněným shromažďováním a zpracováním OÚ.

1.2 Rozsah závaznosti

Dokument je závazný pro všechny subjekty ve společnosti – vedení společnosti, zaměstnance a externí spolupracovníky.

2 ODPOVĚDNOSTI, POVINNOSTI A PRAVOMOCI

2.1 **Garant** (Jednatel / Managing Director)

Odpovídá za:

- vytvoření, udržování a řízení systému ochrany OÚ a ve společnosti, v souladu s Nařízením a ZOOÚ,
- výkon činností osob oprávněných zajišťovat ochranu osobních údajů
- řešení a vyšetřování bezpečnostních incidentů vzniklých v souvislosti s ochranou OÚ, analýzu jejich příčin a zajišťování nápravných opatření,
- obsahovou náplň vzdělávání a výchovy v oblasti ochrany OÚ (ve spolupráci s útvarem personalistika),
- plnění povinností společnosti vůči ÚOOÚ jménem společnosti,

Má pravomoc:

- provádět kontrolu dodržování Nařízení a ZOOÚ dokumentů systémů řízení a další dokumentace
- vyžadovat pomoc a stanoviska osob oprávněných zajišťovat ochranu osobních údajů při řešení situací souvisejících s ochranou OÚ a zákonností jejich shromažďování.

2.2 Určená osoba

Odpovídá za:

- rozpracování, udržování a řízení ochrany OÚ v souladu s touto směrnicí v rozsahu své působnosti,

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

- řešení a vyšetřování bezpečnostních incidentů, analýzu jejich příčin a vyžadování nápravných opatření v rámci své působnosti
- provádění kontroly dodržování Nařízení a ZOOÚ,
- včasné informování Garanta o porušení Nařízení nebo ZOOÚ a o následných nápravných opatřeních.

Má pravomoc:
- vyžadovat součinnost a stanoviska všech osob ve společnosti při řešení situací souvisejících s ochranou OÚ a zákonností jejich shromažďování,
- být kontaktní osobou při komunikaci mezi Správcem a Garantem,
- řídit zajištění ochrany a bezpečnosti OÚ ve společnosti, pro kterou byl jmenován.

Pokud ve společnosti není „Určená osoba“, vykonává jeho činnost „Garant“ či jím dočasně pověřená osoba.

2.3 Oprávněné osoby

Jsou povinny zejména:
- zajistit přiměřenou úroveň ochrany OÚ, k jejichž zpracování jsou oprávněni, zejména používáním šifrové ochrany proti ztrátě a zneužití
  - dat předávaných elektronickou poštou nebo přenášených nechráněnými telekomunikačními sítěmi, např. uzamčením připojených příloh obsahující OÚ, heslo odeslat samostatným komunikačním kanálem (SMS),
  - dat v souborech a sdílených datových úložištích,
  - dat v pevných a přenosných počítačích, tabletech, mobilních telefonech a externích paměťových médiích.
- zpracovávat OÚ pouze v souladu s účelem, ke kterému byly shromážděny a v rozsahu nezbytném pro naplnění stanoveného účelu a nesdružovat OÚ, které byly získány k rozdílným účelům.

2.4 Všichni zaměstnanci a osoby přicházející do styku s osobními údaji

Jsou povinni zejména:
- zachovávat mlčenlivost o OÚ a o bezpečnostních opatřeních k jejich ochraně; povinnost mlčenlivosti trvá i po skončení pracovního poměru, práce konané mimo pracovní poměr nebo příslušných prací,
- v případě zjištění neoprávněného nakládání s OÚ - případů porušení zabezpečení OÚ - informovat přímého nadřízeného či Garanta.
- poskytnout Určenému útvaru/Určené osobě potřebnou součinnost.

3 POJMY A ZKRATKY

3.1 Pojmy

Bezpečnostní událost – možné porušení bezpečnostní politiky, nebo na selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá. Může být příčinou nebo mít vliv na vznik bezpečnostního incidentu.

Bezpečnostní incident – jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností společnosti a ohrožení bezpečnosti informací; událost, při které došlo nebo mohlo dojít ke ztrátě, bez ohledu na závažnost.

Blokování osobních údajů – operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování OÚ, s výjimkou nezbytných zásahů.

Dozorový úřad – v ČR Úřad na ochranu osobních údajů.

Důvěrnost – vlastnost vyjadřující omezení v oprávnění autorizované entity k přístupu a sdílení informačních aktiv a ochranu osobních a proprietárních dat.

Integrita – vlastnost zajištění informačního aktiva proti neoprávněné modifikaci nebo zničení, včetně zajištění autenticity a neodmítnutelnosti (s aktivem nemůže nakládat nikdo bez oprávněného přístupu).

Koordinátor IDP – osoba odpovědná za řízení realizační fáze Řízených změn v oblasti IT (zejména se jedná o provozní korekce).

Neoprávněné nakládání s osobními údaji – jejich únik, vyzrazení, zneužití, poškození, znehodnocení, neoprávněný přístup a likvidace, porušení jejich ochrany nebo ztráta.

Nosič osobního údaje – prostředek, jehož prostřednictvím jsou OÚ udržovány v podobě, která umožňuje je dále zpracovávat. Může mít listinnou podobu nebo jinou hmotnou podobu nebo to může být elektronické médium, které je pevnou nebo oddělitelnou, přenosnou nebo nepřenosnou součástí počítačového systému.

Nositel rodného čísla – fyzická osoba, které bylo rodné číslo přiděleno.

Ochrana osobních údajů – soubor opatření v oblasti personální, administrativní, fyzické ochrany a informační bezpečnosti potřebných pro zajištění ochrany OÚ (v souladu s požadavkem na zvýšenou úroveň ochrany informací)

Omezení zpracování – označení uložených OÚ za účelem omezení jejich zpracování v budoucnu.

Oprávněná osoba – zaměstnanec (nebo jiná fyzická osoba konající práce pro společnost v jiném než pracovněprávním vztahu), který byl Garantem určen a do jehož pracovní náplně je zařazeno zpracovávání nebo uchovávání OÚ pro vymezenou oblast.

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.

Pověřenec ochrany OÚ – osoba jmenovaná společností jako pověřenec pro ochranu OÚ podle článku 37 Nařízení.

Pověřený zaměstnanec (původce/vlastníka) – zaměstnanec původcem/vlastníkem určený k úkonům ve spisové službě, zejména k ukládání a skartaci dokumentů.

Příjemci – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.

Rodné číslo – identifikátor fyzické osoby, přidělovaný v souladu se zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech.

Řízená změna – změna prováděná v rámci procesu uplatňování změn v dané společnosti.

Shromažďování osobních údajů – systematický postup nebo soubor postupů, jehož cílem je získání OÚ za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

Souhlas subjektu údajů – jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých OÚ.

Správce OÚ – právnická osoba (společnost), která prostřednictvím svých oprávněných osob určuje účel a prostředky zpracování OÚ, provádí zpracování a odpovídá za něj. Správce může zmocnit nebo pověřit zpracováním OÚ Zpracovatele.

Subjekt údajů (subjekt osobních údajů) – fyzická osoba, k níž se OÚ vztahují. Subjekt údajů se považuje za identifikovaný, nebo identifikovatelný, jestliže lze na základě jednoho či více OÚ přímo či nepřímo zjistit jeho identitu.

Třetí strana – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů

Uchovávání osobních údajů – udržování údajů v takové podobě, která je umožňuje dále zpracovávat.

Určená osoba – osoba, který odpovídá za realizaci systému ochrany OÚ.

Úřad pro ochranu osobních údajů – zřízen zákonem o ochraně osobních údajů a o změně některých zákonů. Jsou mu svěřeny kompetence ústředního správního úřadu pro oblast ochrany OÚ v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem.

Vedoucí oprávněného útvaru – zaměstnanec zastávající místo ředitele nebo vedoucího organizačního útvaru, který zpracovává OÚ nebo v zastoupení Správce určuje účel a prostředky zpracování.

Vlastník změny – zaměstnanec nebo jiná fyzická osoba konající pro Správce práce v jiném než pracovněprávním vztahu, uplatňující Řízenou změnu.

Zachování mlčenlivosti – povinnost nesdělovat OÚ a informace o opatřeních k jejich zabezpečení osobě, která není oprávněna se s OÚ seznamovat.

Změna – zavedení nových nebo změna již zavedených činností, procesů, postupů apod., prováděných v rámci výkonu pracovních činností Zaměstnance, která má nebo může mít dopad či vliv na ochranu a zpracování OÚ. Změnou se dále rozumí uzavření nové smlouvy Správcem, na základě které bude či může dojít ke zpracování OÚ nebo jejíž plnění má nebo může mít dopad či vliv na ochranu a zpracování OÚ.

Zaměstnanec – fyzická osoba, která vykonává práci ve společnosti v pracovním poměru na základě uzavřené pracovní smlouvy nebo koná práce na základě dohod o pracích konaných mimo pracovní poměr.

Zničení (likvidace) osobních údajů – fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.

Zpracování osobních údajů – jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ, 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.

Zpracovatel OÚ – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává OÚ pro správce.

Zveřejněný osobní údaj – údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

Zvláštní kategorie údajů (citlivé údaje) – OÚ, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech,

a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Poznámky:

Zvláštní kategorie OÚ (citlivé OÚ) se v rámci společnosti vyskytují při zpracování záznamů z kamerových systémů, při používání některých biometrických identifikačních zařízení, nebo i při zaznamenávání telefonního hovoru.

Za OÚ, které přímo identifikují subjekt údajů, je považován například soubor obsahující jméno, příjmení, adresu bydliště a datum narození. Za OÚ, který nepřímo umožňuje identifikovat subjekt údajů, je považován například i záznam GPS ze služebního vozidla nebo IP adresa.

3.2 Zkratky

ČR	Česká republika
EKV – ACS	Technické prostředky řízení vstupů – elektronická kontrola vstupů
PZTS	Poplachové zabezpečovací a tísňové systémy
EU	Evropská Unie
GPS	Global positon system
ICT	Hardware a software - prostředky informačních technologií – Information and Communication Technologies
NDA	Non-disclosure agreement - Dohoda o mlčenlivosti
OÚ	Osobní údaje
PD	Pracovní dny
PIA	Privacy Impact Assessments – dopadová analýza - posouzení vlivu zamýšlených operací zpracování na ochranu OÚ
SLA	Service Legal Agreement – Smlouva o poskytování služeb
SoZOÚ	Smlouva o zpracování osobních údajů
ÚOOÚ	Úřad pro ochranu osobních údajů
ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

4 OCHRANA OSOBNÍCH ÚDAJŮ

4.1 Subjekty údajů

Typickými subjekty údajů v podmínkách společnosti jsou:

- fyzické osoby v zaměstnaneckém nebo obdobném vztahu ke Správci,
- zaměstnanci jiných zaměstnavatelů, kteří pracují na zařízeních Správce, resp. vstupují do objektu Správce,
- bývalí zaměstnanci – důchodci,
- rodinní příslušníci zaměstnanců,
- uchazeči o zaměstnání,
- obchodní partneři – fyzické osoby nebo zástupci právnických osob,
- další osoby I (zákazníci, uživatelé informačních systémů Správce apod.),

- další osoby II (účastníci marketingových akcí apod.).

V souvislosti s identifikací subjektu údajů je třeba posoudit, jaký je účel zpracovávání a zda je ke zpracovávání nutný souhlas subjektu údajů nebo zda je zpracování OÚ možné na základě jiného právního titulu.

Dále je nutné stanovit způsob získávání OÚ od subjektů, zejména s ohledem na to, aby nedocházelo k využívání údajů získaných k jinému účelu, případně ke slučování údajů získaných k jiným účelům, a způsob plnění informační povinnosti Správce vůči subjektu údajů.

4.2 Systém opatření k ochraně osobních údajů

Opatření k ochraně OÚ zahrnují organizační, personální, administrativní, ICT opatření a opatření fyzické ochrany realizovaná na straně Správce nebo Zpracovatele OÚ v souladu se standardy informační a kybernetické bezpečnosti, fyzické bezpečnosti a požadavky na ochranu OÚ.

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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.

4.2.1 Personální opatření

Zaměstnanci nebo smluvnímu partnerovi společnosti (právnická nebo fyzická osoba s oprávněním) je umožněn přístup k OÚ při správě nebo zpracování na základě splnění všech následujících podmínek:

- oprávněného požadavku (požadavek pracovního místa na přístup k OÚ, plnění smlouvy),
- prokazatelného seznámení se způsobem, jakým mohou fyzické osoby s oprávněním s OÚ nakládat (školení ochrany OÚ),
- prokazatelného souhlasu se závazkem mlčenlivosti,
- schválení přístupu odpovědným zaměstnancem ze společnosti,
- smluvnímu partnerovi společnosti (právnická nebo fyzická osoba s oprávněním) na základě uzavřené Smlouvy o zpracování osobních údajů, viz. - Návrh smlouvy o zpracování osobních údajů.

4.2.2 Administrativní opatření

Administrativní ochrana OÚ zahrnuje zejména:

- vedení Záznamů o činnostech zpracování,
- vedení katalogů účelů a právních titulů zpracování,
- označování a evidenci nosičů, v souladu se spisovým a skartačním řádem,
- vedení záznamů o předávání a příjmu nosičů,
- ukládání, archivaci a skartaci nosičů,
- řízenou likvidaci nosičů informací (listinných, elektronických). Pro řízenou likvidaci musí být použito příslušné skartovací zařízení, nebo uzamčené sběrné kontejnery, jejichž obsah je bezpečně likvidován za přítomnosti pověřené osoby, neaktuální dokumenty musí být zničeny tak, aby byla vyloučena možnost zpětné rekonstrukce informací, existuje záznam o zničení všech verzí,
- oprávnění k manipulaci s OÚ v rámci správy nebo zpracování je možné pouze na základě souhlasu příslušného správce nebo zpracovatele (vlastníka) informace,

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

- přeprava je zajišťována důvěryhodným kurýrem.

4.2.3 Fyzická ochrana osobních údajů

Fyzická ochrana OÚ zahrnuje v souladu se standardy fyzické ochrany společnosti zejména:

- příslušná režimová opatření: informace musí být udržovány v zabezpečených monitorovaných prostorech s pravidelnou kontrolou přístupu,
- mechanické zábranné prostředky,
- poplachové zabezpečovací a tísňové systémy (PZTS).

4.2.4 Ochrana osobních údajů v systémech a prostředcích ICT

Systémy a prostředky ICT určené pro správu a zpracování OÚ jsou klasifikovány z hlediska důvěrnosti stupněm „A“. Požadavky na opatření nad rámec základních požadavků jsou zejména:

- šifrování u notebooků, přenositelných paměťových médií a při přenosu v nechráněných telekomunikačních sítích,
- řízení přístupů k OÚ striktně dle schválených autorizačních konceptů,
- auditování autorizovaných i neautorizovaných přístupů,
- zajištění retence 3 měsíců auditních záznamů,
- napojení a vyhodnocování bezpečnostních událostí v bezpečnostním dohledu,
- zpracování a pravidelné ověřování plánů pro případ mimořádných situací, operativní postupy pro zajištění bezpečné činnosti systémů a prostředků ICT,
- zajištění logování, zálohování a obnovy dat,
- řízení verzí, archivace a skartace.

Přenos a ukládání OÚ je zakázán na paměťových nosičích, které nejsou v majetku společnosti.

4.2.5 Ohlašování případů porušení zabezpečení osobních údajů

Jakékoli porušení zabezpečení OÚ, včetně informace o provedených nápravných opatřeních, ohlásí Správce (Určená osoba) dozorovému úřadu bez zbytečného odkladu, nejpozději však do 72 hodin od okamžiku, kdy se o něm dozvěděl, 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.

4.2.5.1 Ohlašovací povinnost

Každý zaměstnanec či spolupracující osoba, je v případě zjištění neoprávněného nakládání s OÚ - případů porušení zabezpečení OÚ povinen neprodleně informovat:

- přímého nadřízeného
- nebo Určenou osobu společnosti

Zpracování osobních údajů, které není v souladu s Nařízením a ZOOÚ se ve společnosti zakazuje.

4.2.6 Podmínky zpracovávání osobních údajů

Garant odpovídá za oznámení záměru zpracovávat OÚ Určené osobě.

Oznámení o záměru zpracovávat OÚ obsahuje:

- Zákonné zdůvodnění zpracování OÚ, účel, rozsah, místo, prostředky a zdroje zpracovávání OÚ.

- Seznam všech zpracovatelů, příjemců OÚ a platných Smluv o zpracování OÚ.
- Pokud Oprávněný útvar hodlá použít zpracovávané OÚ k jinému než původně stanovenému účelu, rozšířit zpracování za již stanoveným účelem o další údaje nebo je zpřístupnit jinému útvaru nebo využít ke zpracovávání nové zpracovatele, je povinen tuto skutečnost neprodleně oznámit Určené osobě a předložit veškeré výše jmenované informace a dokumenty.
- Bez posouzení záměru zpracovávat OÚ Určenou osobou je zakázáno zahájit zpracování OÚ, nebo jeho změnu.

4.2.6.1 Účel zpracování

Stanovený účel zpracovávání musí být pravdivý a jednoznačný.

OÚ lze zpracovávat pouze s ohledem na platné právní předpisy ČR a Nařízení v souladu s účelem, k němuž byly shromážděny. Zpracovávat je k jinému účelu je možné jen tehdy, pokud o této změně zpracování byl subjekt údajů informován, a nelze-li takové zpracování provádět na základě právního titulu nevyžadujícího předchozí souhlas, pokud k tomu dal subjekt údajů souhlas.

4.2.6.2 Rozsah zpracovávaných údajů

Rozsah zpracovávaných údajů musí být stanoven tak, aby splnil stanovený účel, a přitom nebyly shromažďovány a zpracovávány nadbytečné OÚ.

4.2.6.3 Zdroje osobních údajů

Zdrojem pro zpracovávání osobních údajů jsou primárně údaje poskytnuté subjektem údajů (a ověřené zaměstnancem z oprávněného útvaru).

Jiné zdroje OÚ lze využít pouze výjimečně a při splnění všech povinností stanovených ZOOÚ a Nařízením.

4.2.6.4 Místo a způsob zpracování, opatření k ochraně osobních údajů

Garant či Určená osoba společnosti stanoví místa, na kterých jsou OÚ zpracovávány, prostředky a způsob (technologie), který je ke zpracovávání využíván.

Dále stanoví personální, administrativní a režimová opatření sloužící k zajištění ochrany OÚ, které zpracovává.

Určená osoba může zahájit zpracování OÚ jen za předpokladu, že jsou splněny veškeré podmínky stanovené Nařízením a ZOOÚ, tj. je zejména splněna zákonnost zpracování, získán souhlas subjektů údajů a jejich informování.

4.2.7 Posouzení vlivu na ochranu osobních údajů

Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, provede Správce v součinnosti s Určenou osobou před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu OÚ (PIA), a to v souladu s článkem 35 Nařízení.

Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

4.2.7.1 Předchozí konzultace

Pokud z PIA vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by Správce nepřijal opatření ke zmírnění tohoto rizika, konzultuje Správce prostřednictvím Pověřence toto zpracování před jeho započetím s dozorovým úřadem.

Při konzultaci Správce postupuje v souladu s článkem 36 Nařízení.

4.2.8 Posuzování změn ve společnosti z pohledu Nařízení a ZOOÚ

4.2.8.1 Posuzování Řízených změn

V rámci platného procesu uplatňování změn je zakomponováno posouzení dopadů Nařízení a ZOOÚ Určeným útvarem/Určenou osobou.

Za zajištění vyjádření v rámci procesu odpovídá Garant cestou Oprávněné osoby. Určená osoba má na posouzení dopadů lhůtu 5 PD. Oprávněný útvar je povinen poskytnout Určené osobě pro zpracování posouzení dopadů potřebnou součinnost. Lhůta 5 PD může být Určenou osobou přiměřeně prodloužena v závislosti na rozsahu a složitosti Řízené změny.

V případě, že Určená osoba identifikuje výše uvedený dopad, podílí se metodicky na tvorbě definice Řízené změny tak, aby byl zajištěn soulad s Nařízením a ZOOÚ.

4.2.8.2 Posuzování Změn

Garant je povinnen zajistit posouzení Změny Určenou osobou z pohledu dopadů Nařízení a ZOOÚ.

Určená osoba má na posouzení dopadů lhůtu 5 PD. Všichni zaměstnanci jsou povinni poskytnout pro zpracování posouzení dopadů potřebnou součinnost. Lhůta 5 PD může být přiměřeně prodloužena v závislosti na rozsahu a složitosti Změny.
V případě, že Určená osoba identifikuje výše uvedený dopad, podílí se metodicky na tvorbě definice Změny tak, aby byl zajištěn soulad s Nařízením a ZOOÚ.

4.2.9 Vedení záznamů zpracování

Správce vede v souladu s čl. 30 Nařízení záznamy o činnostech zpracování, za něž zodpovídá, tyto záznamy obsahují všechny tyto informace:

- jméno a kontaktní údaje Správce
- účely zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie Příjemců, kterým byly nebo budou OÚ zpřístupněny, včetně Příjemců ve třetích zemích nebo mezinárodních organizacích;
- informace o případném předání OÚ do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce Nařízení, doložení vhodných záruk;
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 Nařízení.

Záznamy se vyhotovují písemně, v to počítaje i elektronickou formu.

Záznamy zpracování je Správce povinen udržovat v aktuálním stavu a zajistit jejich aktuálnost.

4.2.10 Zpřístupnění údajů, zpracování prostřednictvím Zpracovatele

Ke zpracovávání OÚ je možno využít externí dodavatele – Zpracovatele. **Podmínkou je uzavření Smlouvy o zpracovávání osobních údajů mezi Správcem a Zpracovatelem.**

4.2.10.1 Uzavření smlouvy o zpracování osobních údajů

Za uzavření Smlouvy o zpracování osobních údajů (dále SoZOÚ) odpovídá Oprávněná osoba, která uzavírá smluvní vztah (v souladu s podpisovým řádem dané společnosti), součástí jehož plnění je i zpracovávání OÚ (smlouvu o dodávce zboží nebo poskytnutí služeb apod.). SoZOÚ nelze uzavřít bez vyjádření Určené osoby, jako garanta oblasti ochrany OÚ.

SoZOÚ se zpravidla uzavírá jako samostatný dokument, pouze ve výjimečných případech je ujednání o zpracování OÚ součástí jiného, zpravidla obchodního, smluvního vztahu.

Zpracováním OÚ prostřednictvím Zpracovatele není dotčeno právo Správce stanovit oprávnění přístupu k OÚ jak pro své zaměstnance, tak pro třetí strany.

Zpracovatel není oprávněn zpracovávat OÚ k jinému účelu a jiným způsobem než smluvně dohodnutým. Stejně tak není oprávněn předávat nebo zpřístupňovat zpracovávané OÚ jiným osobám než určeným Správcem v souladu s čl. 28, odst. 3 nařízení.

4.2.11 Souhlas se zpracováváním, informace o zpracovávání, ochrana a výkon práv subjektu údajů

4.2.11.1 Souhlas subjektu údajů

Pokud Společnost zpracovává OÚ na základě článku 6, odst. 1, písm. b), c), d), e), f) Nařízení, není nutný souhlas subjektu údajů, ale Společnost zajistí informační povinnost vůči Subjektu údajů.

V ostatních případech může Správce zpracovávat OÚ pouze s předchozím souhlasem Subjektu údajů. Tento souhlas je nutný i v případě, že Společnost zpracovává OÚ k jinému účelu, než k jakému byly shromážděny.

Oprávněný útvar musí být schopen udělení souhlasu prokázat, a to po celou dobu zpracování OÚ, k jejichž zpracování byl dán souhlas. Součástí získání souhlasu je i informování Subjektu údajů o účelu zpracovávání.

4.2.11.2 Informování Subjektu údajů

Společnost je povinna včas a řádně v souladu s článkem 13 a 14 Nařízení ve stanoveném rozsahu informovat Subjekt údajů o tom, že Správce zpracovává jeho OÚ.

Kromě výše uvedených informací uvedených poskytne Správce Subjektu údajů další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k Subjektu údajů v rozsahu stanoveném Nařízením.

Společnost musí Subjekt údajů informovat o jeho právech vyplývajících z Nařízení.

4.2.11.3 Právo na přístup k informacím

Správce je povinen, na základě žádosti Subjektu údajů, bezplatně jej informovat o tom, jaké údaje o něm zpracovává. Náležitosti sdělení jsou uvedeny v Nařízení.

Veškeré záznamy o poskytnutí informací se vedou v písemné formě (v to počítaje i elektronickou formu).

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

4.2.11.4 Právo na opravu

Oprávněný útvar bez zbytečného odkladu opraví či doplní nepřesné, resp. neúplné OÚ, které se týkají Subjektu údajů, a to na základě žádosti Subjektu údajů.

4.2.11.5 Omezení zpracování

Správce omezí zpracování pokud:

- Subjekt údajů popírá přesnost OÚ, a to na dobu potřebnou k tomu, aby Správce mohl přesnost OÚ ověřit;
- zpracování je protiprávní a Subjekt údajů odmítá výmaz OÚ a žádá místo toho o omezení jejich použití;
- Správce již OÚ nepotřebuje pro účely zpracování, ale Subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- Subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 Nařízení, dokud nebude ověřeno, zda oprávněné důvody Správce převažují nad oprávněnými důvody Subjektu údajů.

4.2.11.6 Likvidace osobních údajů, právo na výmaz (právo být zapomenut)

Společnost nebo na základě jejího pokynu Zpracovatel, je povinen provést likvidaci OÚ, jakmile pomine účel, pro který byly OÚ zpracovány,

Oprávněný útvar bez zbytečného odkladu vymaže OÚ, které se týkají Subjektu, který uplatnil právo na výmaz OÚ, nebo který využil práva být zapomenut, a to za předpokladu, že je dán jeden z těchto důvodů:

- OÚ již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- Subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) Nařízení zpracovány, a neexistuje žádný další právní důvod pro zpracování;
- Subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 Nařízení a neexistují žádné převažující oprávněné důvody pro zpracování nebo Subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2 Nařízení;
- OÚ byly zpracovány protiprávně;
- OÚ musí být vymazány ke splnění zákonné povinnosti;
- OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1. Nařízení.

Jestliže Správce OÚ zveřejnil a je povinen je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval Správce, kteří tyto OÚ zpracovávají, že je Subjekt údajů žádá, aby vymazali veškeré odkazy na tyto OÚ, jejich kopie či replikace.

Výše uvedené právo Subjektu údajů se neuplatní, pokud je zpracování nezbytné:

- pro výkon práva na svobodu projevu a informace;
- pro splnění zákonné povinnosti, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce pověřen;
- z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení;
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1 Nařízení, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;
- pro určení, výkon nebo obhajobu právních nároků.

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM

4.2.11.7 Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Správce oznamuje jednotlivým Příjemcům, jimž byly OÚ zpřístupněny, veškeré opravy nebo výmazy OÚ nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18 Nařízení, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje Subjekt údajů o těchto Příjemcích, pokud to Subjekt údajů požaduje.

4.2.11.8 Právo na přenositelnost údajů

Společnost umožní Subjektu údajů získat OÚ, které se ho týkají a které poskytl Správci, ve strukturovaném, běžně používaném a strojově čitelném formátu a umožní Subjektu údajů předání těchto údajů jinému Správci, a to na základě žádosti Subjektu údajů a v případě, že

- zpracování je založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1 písm. b); Nařízení,
- zpracování se provádí automatizovaně.

Při výkonu práva na přenositelnost údajů má Subjekt údajů právo na to, aby OÚ byly předány přímo jedním Správcem Správci druhému, je-li to technicky proveditelné.

Právem na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob.

4.2.12 Zpracování zvláštních kategorií údajů

Zpracovávání zvláštních kategorií (citlivých) údajů je možné jen při splnění všech podmínek stanovených Nařízením a pouze v následujících případech:

- subjekt údajů udělil výslovný souhlas se zpracováním těchto OÚ pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo EU nebo členského státu stanoví, že zákaz nemůže být subjektem údajů zrušen;
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem EU nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto OÚ nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
- zpracování se týká OÚ zjevně zveřejněných subjektem údajů;
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí;
- zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v Nařízení;

- zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 Nařízení na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

4.2.13 Využívání rodného čísla

Rodným číslem se rozumí i jakákoliv kombinace čísel vyjadřující den, měsíc, rok narození a třímístnou nebo čtyřmístnou koncovku rodného čísla, z níž je možné dovodit identifikaci fyzické osoby.

Rodná čísla lze v evidencích, databázích a jiných zpracováních v rámci Společnosti využívat pouze:
- při zpracovávání OÚ dle zvláštního právního předpisu nebo
- s písemným souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

4.2.14 Kontrolní činnost

4.2.14.1 Vnější kontrola

Vnější kontrolu dodržování Nařízení a ZOOÚ je oprávněn provádět výhradně příslušný Dozorový úřad.

Podmínky pro činnost inspektora dozorového úřadu a jeho spolupracovníků zajišťuje Určená osoba.

4.2.14.2 Interní kontrola

Kontrolu dodržování vnitřních předpisů a opatření ochrany OÚ v rámci Společnosti provádí Garant či Určená osoba.

4.2.14.3 Externí kontrola

Správce má právo kontrolovat dodržování sjednaných podmínek ochrany OÚ u smluvních partnerů Společnosti. Ve smlouvě (SoZOÚ) musí být uložena smluvnímu partnerovi povinnost umožnit za účelem kontroly zaměstnancům Správce:
- přístup k systémům a prostředkům ICT určených pro nakládání s OÚ, včetně prostředků fyzické ochrany údajů v systémech a prostředcích ICT,
- přístup k prostředkům fyzické ochrany OÚ,
- přístup ke všem administrativním/technickým opatřením týkajících se nakládání s OÚ.
- z kontrol jsou vyloučeny komunikační systémy, které zajišťují funkčnost technických a programových prostředků kritické informační infrastruktury

5 VAZBY MEZI DOKUMENTY

5.1 Vazby na vnější dokumenty a vnitřní dokumenty neevidované v ECM ŘD

V kapitole jsou uvedeny dokumenty v platném znění k datu nabytí platnosti dokumentu.

nařízení EU 2016/679	o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
zákon č. 101/2000 Sb.	o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
zákon č. 133/2000 Sb.	o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů
zákon č. 40/2009 Sb.	Trestní zákoník
zákon č. 418/2011 Sb	o trestní odpovědnosti právnických osob
zákon č. 480/2004 Sb	o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
zákon č. 89/2012	Občanský zákoník
zákon č. 127/2005	o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
zákon č. 181/2014Sb.	o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
Vyhláška č. 316/2014 Sb.	o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Pozn. Aktuální konsolidované znění vnějších předpisů Sbírky zákonů ČR je například k dispozici zde.

6 ZÁVĚREČNÁ A PŘECHODNÁ USTANOVENÍ

Implementace dokumentu do systému řízení dotčených právních subjektů musí být realizována nejpozději do 3 měsíců od schválení dokumentu.

Seznam formulářů:

Návrh smlouvy o zpracování osobních údajů

IČ: 25798502
DIČ: CZ25798502

Zlatnická 1582/10
110 00 Praha 1

Zapsaná v Obchodním rejstříku
vedeném Městským soudem
v Praze, oddíl C, vložka 71245

INFO@KASPENJVM.COM
KASPENJVM.COM