Směrnice JRD GROUP

009. Zpracování a ochrana osobních údajů

(Verze č. 1)

Působnost směrnice

Název společnosti
JRD Group a.s. IČO:26778092, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 26960, se sídlem Korunní 810/104, Vinohrady, 101 00 Praha 10
JRD Services s.r.o. IČO: 02811022, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 224078, se sídlem Korunní 810/104, Vinohrady, 101 00 Praha 10
JRD Invest s.r.o. IČO: 02882892, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 224074, se sídlem Korunní 810/104, Vinohrady, 101 00 Praha 10
Millenium Technologies a.s. IČO: 61325732, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 15863, se sídlem Národní 39/364, 110 00 Praha 1

Autor	Jméno a příjmení	Datum
Compliance specialista	Ing. Kateřina Spěváková	15.8.2025

Datum účinnosti: 1.9.2025

Obsah

1. PREAMBULE 4
2. Základní zásady Zpracování osobních údajů 4
3. Povinnosti nadřízených pracovníků 5
4. Organizační a technická opatření 5
   4.1. Proces určení účelu zpracování 5
   4.2. Proces určení rozsahu zpracovávaných Osobních údajů 6
   4.3. Proces určení právního základu zpracování 7
   4.4. Určení doby uchovávání Osobních údajů a výmaz údajů 8
   4.5. Proces určení procesních prostředků zpracování 9
   4.6. Proces určení technického zabezpečení zpracování 9
5. Vytváření audiovizuálních záznamů a jejich sdílení 10
6. Řízení bezpečnosti a bezpečnostních incidentů 11
   6.1. Hlášení bezpečnostních incidentů 11
7. Oznámení Subjektům údajů 12
8. Předávání osobních údajů 13
9. Určení postavení JRD a dalších stran 14
   9.1. Vztah správce x zpracovatel 14
   9.2. Vztah společných správců 14
   9.3. Vztah správce x správce 14
10. Předávání Osobních údajů do třetích zemí mimo Evropskou unii 14
11. Informování subjektů údajů 15
12. Školení 16
13. Pověřenec pro ochranu osobních údajů 16

Použité pojmy a zkratky

AML … oblast boje proti praní špinavých peněz podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů;

Anonymizace ... proces změnění nebo získání údajů tak, že buď v původním tvaru nebo po úpravě nelze údaje vztáhnout ke konkrétnímu subjektu údajů – nejedná se tedy o osobní údaj (např. statistická data);

Biometrické údaje ... osobní údaje vyplývající z fyzických či fyziologických znaků nebo znaků chování fyzické osoby jako např. zobrazení obličeje, údaje o otiscích prstů apod.;

Evidence ... jakýkoliv soubor Osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

JRD … znamená společnosti uvedené na první straně této Směrnice a veškeré aktuální společnosti – SPV, jejichž mateřskou společností je jedna z takto uvedených společností, jakož i makléři/ obchodníci aktuálně spolupracující s kteroukoli z takto uvedených společností.

Nařízení GDPR ... nařízení 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;

Osobní údaje...veškeré informace o Subjektu údajů. Za osobní údaje se považují i informace, které se samy o sobě netýkají fyzické osoby, ale ve spojení s jinými informacemi by již bylo možné tato data vztáhnout (i jen potenciálně) ke konkrétní fyzické osobě, např. VIN číslo auta, zůstatek na účtu atd.;

Pověřený člen správní rady... člen správní rady JRD Group a.s. Ing. Jan Sadil

Pověřený Pracovník Compliance … pracovník na pozici Compliance specialista Ing. Kateřina Spěváková

Pracovník ... všichni zaměstnanci JRD, všichni členové orgánů JRD, osoby spolupracující s JRD jako osoby samostatně výdělečné činné a osoby, jež podléhají interním předpisům JRD;

Projekt … nemovitostní projekty prováděné JRD;

Pseudonymizace ... proces změnění Osobních údajů tak, že již údaj nemůže být přiřazen konkrétnímu Subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny Subjektu údajů;

Směrnice ... tato směrnice o zpracování Osobních údajů;

Subjekt údajů ... Identifikovaná nebo identifikovatelná fyzická osoba (tj. nikoliv osoba právnická – společnost nebo organizace). 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;

Pracovník IT ... pracovník zodpovědný za správu sítě a webu;

Odpovědný Pracovník týmu ... pracovník zodpovědný za proces či projekt zpracování Osobních údajů v rámci JRD, zejm. vedoucí jednotlivých oddělení, či vedoucí jednotlivých projektů;

Zvláštní kategorie osobních údajů ... Osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, 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; zvláštní ochrany požívají údaje týkající se odsouzení za trestné činy.

1. PREAMBULE

Účelem Směrnice je stanovení závazných pravidel pro nakládání s Osobními údaji a s dokumenty obsahujícími tyto Osobní údaje při zpracování Osobních údajů v JRD. Směrnice je jedním z organizačních opatření ochrany Osobních údajů ve smyslu článku 32 Nařízení GDPR.

Tento vnitřní předpis zejména obsahuje:

- postupy a způsoby zpracování Osobních údajů JRD;
- práva a povinnosti Pracovníků, kteří Osobní údaje zpracovávají;

Směrnice je interním závazným předpisem, který zavazuje všechny Pracovníky.

V rámci JRD je za zajištění dodržování této Směrnice při činnosti JRD odpovědný Pověřený člen správní rady.

2. ZÁKLADNÍ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Všichni Pracovníci jsou povinni:

- zpracovávat Osobní údaje v souladu s podmínkami stanovenými příslušným Odpovědným Pracovníkem týmu a v souladu se všemi kapitolami této Směrnice, zejména s použitím stanovených prostředků a stanoveným způsobem zpracování, a to v souladu s účelem, za nímž byly Osobní údaje shromážděny, pouze v rozsahu potřebném pro dosažení stanoveného účelu;
- zpracovávat pouze Osobní údaje nezbytné pro plnění svých pracovních úkolů. Odpovědný Pracovník týmu za tímto účelem zřizuje Pracovníkům přístup pouze k nezbytně nutným Evidencím;
- zajistit ochranu a bezpečnost jimi zpracovávaných Osobních údajů v písemné, anebo elektronické podobě před neoprávněným či náhodným přístupem neoprávněných osob, neoprávněným přenosem, neoprávněným zpracováním, změnami, zničením či ztrátou nebo jiným zneužitím.
- zachovávat mlčenlivost o Osobních údajích a o bezpečnostních opatřeních přijatých podle této Směrnice či jiných vnitřních dokumentů JRD. Povinnost mlčenlivosti trvá i po skončení zaměstnání či spolupráce s JRD.

Osobní údaje jsou zpracovávány po dobu určenou právními předpisy nebo po dobu naplnění účelu ke zpracovávání, kterou určuje odpovědný Pracovník týmu spolu s pověřeným Pracovníkem Compliance. Účel, doba uchování a další informace týkající se procesu zpracování Osobních údajů jsou evidovány v záznamech o činnostech zpracování.

Má-li Pracovník podezření nebo dozví-li se, že jsou Osobní údaje jakéhokoliv Subjektu údajů nepřesné, neúplné či zastaralé, ohlásí to pověřenému Pracovníkovi Compliance.

Má-li Pracovník podezření nebo dozví-li se, že jsou Osobní údaje zpracovávány déle, než je nezbytné pro účely, pro které jsou zpracovávány, ohlásí to pověřenému Pracovníkovi Compliance.

3. POVINNOSTI NADŘÍZENÝCH PRACOVNÍKŮ

Odpovědnost za navrhování opatření v oblasti ochrany Osobních údajů a každodenní vymáhání této ochrany nesou odpovědní Pracovníci týmů, kteří jsou:

- zodpovědní za zpracovávání Osobních údajů v rámci příslušných procesů či projektů, tj. zejména za stanovení účelu, rozsahu, právního základu, a pro každý účel zpracování procesní a technické prostředky, dobu zpracování a okruh příjemců za účelem zajištění odpovídající úrovně zabezpečení Osobních údajů, viz kapitola 4 této Směrnice;
- zodpovědní za splnění podmínek při pořizování audiovizuálních záznamů, viz kapitola 5 této Směrnice;
- zodpovědní za každodenní řízení bezpečnosti v souvislosti s ochranou Osobních údajů v rámci příslušných oddělení a Evidencí viz kapitola 6 této Směrnice;
- povinni zajistit aktualizaci informací v záznamech o činnostech zpracování;
- zodpovědní za výběr zpracovatelů Osobních údajů, či rozhodnutí o předání Osobních údajů třetím osobám, viz kapitola 8 této Směrnice;
- povinni zajistit, aby byl Subjekt údajů informován o všech skutečnostech vyžadovaných příslušnými právními předpisy, zejména čl. 13 a 14 Nařízení GDPR, viz kapitola 11 této Směrnice;

Pověřený Pracovník Compliance je:

- zodpovědný za řízení bezpečnostních incidentů při zpracovávání Osobních údajů;
- povinen zajistit školení Pracovníků;
- zajištění komunikace s Úřadem pro ochranu osobních údajů či jinými orgány veřejné správy ve věci ochrany Osobních údajů;
- odpovědný za zajištění souladu této Směrnice s aktuální legislativou, rozhodovací praxí Úřad pro ochranu osobních údajů a soudů.

4. ORGANIZAČNÍ A TECHNICKÁ OPATŘENÍ

4.1. Proces určení účelu zpracování

Účel zpracování Osobních údajů je cíl, kterého má být zpracování Osobních údajů dosaženo. Jednat se může např. o následující účely:

- vedení mzdové evidence za účelem výplaty mezd zaměstnancům;
- pořízení skupinových fotografií z teambuildingu pořádaného JRD za účelem jejich zveřejnění;
- nabízení Projektů potenciálním zájemcům;
- rozesílání newsletterů;
- sjednávání a uzavření smluvní dokumentace (rezervační smlouva, smlouva o úschově, kupní smlouva)

- plnění povinností v rámci AML;
- řešení reklamací;
- pořádání akcí JRD – např. Mikulášská atd.;

Nemá-li zpracování určitého Osobního údaje žádný účel, jde o protiprávní zpracování.

V případě, že byly Osobní údaje shromážděny pro jeden účel, je možné je využít pro jiný účel za dodržení pravidel dle následujících ustanovení. Pokud JRD Osobní údaje shromáždilo na základě:

- oprávněného zájmu,
- smlouvy; nebo
- ochrany životně důležitých zájmů,

mohou být použity k jinému účelu, ale až po kontrole toho, zda je nový účel slučitelný s původním účelem.

Pokud JRD Osobní údaje shromažďuje na základě:

- souhlasu;
- nebo na základě zákonného požadavku,

není možné žádné další zpracovávání kromě toho, co je pokryto původním souhlasem nebo zákonnými ustanoveními. Další zpracovávání by vyžadovalo získání nového souhlasu nebo nového právního základu (což může být i např. oprávněný zájem JRD v případě vedení sporu).

Pokud JRD chce Osobní údaje využít ke statistice nebo vědeckému výzkumu, není třeba provádět test slučitelnosti účelů, tj. posouzení, zda je další zpracování osobních údajů pro nový účel slučitelné s původním účelem, pro který byly tyto údaje shromážděny.

Při posuzování slučitelnosti účelů Pracovník zváží:

- spojení mezi původním účelem a novým/nadcházejícím účelem;
- kontext, v němž byly Osobní údaje shromážděny (zejm. vztah mezi JRD a Subjektem údajů;
- typ a povahu Osobních údajů (zda se např. jedná o Zvláštní kategorii osobních údajů);
- možné důsledky zamýšleného dalšího zpracovávání (jaký dopad to bude mít na Subjekt údajů);
- existenci vhodných záruk (například šifrování nebo pseudonymizace).

4.2. Proces určení rozsahu zpracovávaných Osobních údajů

JRD smí pro stanovený účel zpracovávat Osobní údaje vždy pouze v potřebném rozsahu, tj. např. pro uzavření kupní smlouvy s klientem není třeba vyžadovat informace o jeho vzdělání, či počtu dětí, pro sjednání pracovní smlouvy není třeba vyžadovat informace o finanční situaci zaměstnance. V rámci stanového účelu tedy JRD vždy zváží, zda je požadovaný Osobní údaj nutný pro dosažení daného účelu zpracování.

4.3. Proces určení právního základu zpracování

Právní základ pro zpracování může být pouze jeden z následujících:

a) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je Subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto Subjektu údajů (např. sjednání smluvní dokumentace, sjednání pracovní smlouvy);

b) zpracování je nezbytné pro splnění právní povinnosti, která se na JRD vztahuje (například povinnosti JRD evidovat zaměstnance a spravovat jejich mzdové údaje, povinnosti týkající se AML);

c) zpracování je nezbytné pro ochranu životně důležitých zájmů Subjektu údajů nebo jiné fyzické osob (např. v případě řešení život ohrožujících situací ohledně Pracovníků – požár atd.);

d) Subjekt údajů udělil souhlas pro jeden či více konkrétních účelů (např. při pořizování nebo sdílení fotografiích jedinců, udělování souhlasu se zasíláním newsletterů);

e) zpracování je nezbytné pro účely oprávněných zájmů JRD, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody Subjektu údajů vyžadující ochranu Osobních údajů (např. v případě vymáhání nároků JRD před soudy, či ochrana proti takovým nárokům, skupinové fotografie z akcí pro jejích následné zveřejnění v rámci zpravodajské licence, oslovování stávajících klientů s nabídkou služeb JRD);

Každý účel zpracování může mít pouze jeden právní základ zpracování. Existuje-li více právních základů v rámci jednoho účelu, je nutné je rozdělit na samostatné účely (např. při sjednávání a plnění kupní smlouvy jsou zpracovávány údaje jak na základě právního titulu plnění smlouvy, tak pro na základě plnění právní povinnosti (podávání daňových přiznání), bude se tedy jednat o dva samostatné účely zpracování.

Odpovědní Pracovníci týmů jsou povinni před zahájením nového účelu zpracování důkladně analyzovat a určit, který právní základ je pro zpracování vhodný, a tuto skutečnost zdokumentovat. Při posuzování nejvhodnějšího právního základu musí vzít odpovědní Pracovníci týmů ve spolupráci s pověřeným Pracovníkem Compliance v úvahu řadu faktorů, a to zejména:

- účel, jehož se JRD snaží zpracováním dosáhnout;
- zda lze zamýšleného účelu dosáhnout méně do soukromí zasahujícím způsobem;
- zda je zpracování dobrovolné či povinné.

Právní základ souhlas subjektů údajů a oprávněný zájem je nutné používat pouze výjimečně, kdy nelze použít jiný právní základ. Odpovědní Pracovníci týmů zajistí upřednostnění právní základů jiných, než je souhlas a oprávněný zájem, tj. upřednostní právní základy dle bodu a) – c) (viz výše), před právními základy dle bodu d) – e) (viz výše). Zejména v pracovněprávních vztazích je nutné souhlas jako právní titul zpracování používat velmi výjimečně (např. zveřejnění fotek jednotlivců z teambuildingu).

V případě, že má JRD zájem o zpracovávání Osobních údajů z titulu svých oprávněných zájmů, musí odpovědní Pracovníci týmů provést posouzení existence oprávněného zájmu JRD, přičemž musí vzít v úvahu celé okolnosti zpracování, zejména:

- otázku, kdo bude mít ze zpracování prospěch;
- předvídatelnost zpracování ze strany Subjektů údajů;

- vztah JRD se Subjekty údajů;
- otázku, zda je JRD v nadřízeném/nadřazeném postavení vůči Subjektům údajů;
- dopad zpracování na Subjekty údajů;
- otázku, zda lze některé Subjekty údajů považovat za zranitelné;
- míru pravděpodobnosti, že Subjekty údajů proti zpracování vznesou námitku;
- schopnost JRD zpracování Osobních údajů na žádost Subjektu údajů kdykoli ukončit.

Je-li existence oprávněného zájmu osvědčena, odpovědní Pracovníci musí na základě výše uvedených informací rovněž provést tzv. balanční test a zvážit, zda oprávněné zájmy JRD převažují nad zájmy nebo základními právy a svobodami Subjektu údajů. Pro obdobné účely postačuje vypracování jednoho balančního testu. Vypracované balanční testy archivuje pověřený Pracovník Compliance.

V rámci balančního testu odpovědný Pracovník:

- posoudí důležitost oprávněného zájmu JRD, tj. jaký má zájem pro JRD význam;
- zváží důsledky zpracování Osobních údajů pro Subjekt údajů, a to zejména zájmy Subjektů údajů a důsledky pro jejich základní práva (možnou diskriminaci, narušení soukromí apod.). JRD rovněž musí posoudit, zda Subjekt údajů může takové zpracování důvodně očekávat.
- zváží důležitosti oprávněného zájmu JRD a důsledků pro Subjekty údajů, tj. zda nad zájmem JRD nepřevažují zájmy Subjektů údajů a rizika, které pro ně zpracování Osobních údajů má.

Pokud Pracovník dospěje k závěru, že Osobní údaje lze na základě oprávněného zájmu JRD zpracovávat, ale přesto existují rizika pro zpracování Osobní údaje, Pracovník přijme dodatečné záruky pro ochranu Subjektů údajů proti rizikům zpracování (např. povinná pseudonymizace, zvýšené zabezpečení atd.)

4.4. Určení doby uchovávání Osobních údajů a výmaz údajů

Doba uchování závisí na účelu, resp. právním základu zpracování, tj:

- je-li zpracování založeno na povinnosti stanovené právním předpisem, bude se zpravidla vycházet z povinností stanovených daným předpisem, plus doby, po kterou může být splnění dané povinnosti kontrolováno (např. povinnosti vyplývající ze sociálního zabezpečení, kdy právní předpis přímo stanoví dobu, po kterou musí být údaje uloženy, lhůta pro stanovení daně, lhůta pro uchování dokumentů dle AML atd.);
- je-li zpracování založeno na povinnosti stanovené smlouvou, bude se zpravidla vycházet z doby trvání smlouvy plus doby, po kterou jde ze smlouvy vymáhat práva a povinnosti, s tím, že jsou-li některé údaje potřebné pouze po kratší dobu, je nutné stanovit pro ně kratší dobu zpracování (např. v případě registrace na team building budou veškeré potřebné údaje uchovávány do doby konání akce, následně je nutné uchovat pouze údaje nutné pro jiný účel, tj. pro případné spory, tj. například velikost mikiny je nutné smazat, nejsou-li potřeba k jiným účelům).

JRD bude uchovávat Osobní údaje pouze po dobu nezbytně nutnou pro daný účel, pro který se Osobní údaje zpracovávají. Osobní údaje musí být bez zbytečného odkladu vymazány, pokud neexistují žádné další účely pro zpracování těchto Osobních údajů.

Výmazem Osobních údajů obsažených v tištěných dokumentech se rozumí fyzické zničení nosiče těchto Osobních údajů. Výmazem Osobních údajů v elektronické podobě se rozumí jejich odstranění, Anonymizace nebo jejich trvalé a nevratné vyloučení ze zpracování.

4.5. Proces určení procesních prostředků zpracování

Odpovědní Pracovníci týmů zajistí, že proces zpracování proběhne dle následujících pravidel:

- zpracování Osobních údajů probíhá pouze za stanoveným účelem, tj. údaje získané pro jeden účel (např. údaje o zaměstnancích pro účely sjednání a výkonu pracovního poměru), nevyužijí jinak (např. oslovení těchto zaměstnanců s nabídkou Projektů bez souhlasu s marketingovou komunikací), aniž by pro takové využití existoval účel a právní zaklad, a tyto účely byly slučitelné;
- ke zpracovávaným Osobním údajům mají přístup pouze osoby, které se přímo podílí na zpracování (tj. např. nevyvěsíme na nástěnku seznam osob).

4.6. Proces určení technického zabezpečení zpracování

Odpovědní Pracovníci týmů zajistí, že technické zabezpečení zpracování proběhne dle následujících pravidel:

Osobní údaje obsažené v elektronické formě na datovém nosiči informací musí být uloženy buď na samostatných datových nosičích umístěných v uzamykatelných skříních, a/nebo místnostech přístupných pouze Pracovníkům s patřičným pověřením anebo na serveru, k němuž mají fyzický přístup pouze tito Pracovníci. Tento server musí být umístěn v uzamykatelné skříni a zamykatelné místnosti;

- přístup k Osobním údajům je udělený pouze vybraným Pracovníkům, kteří se na zpracování podílejí. Přístupová oprávnění k příslušným databázím a systémům jsou pravidelně, alespoň jednou ročně, přezkoumávána tak, aby účty Pracovníků byly včas přidány, upraveny a smazány, aby se snížilo riziko neoprávněného a nevhodného přístupu k Osobním údajům;
- v případě ukončení pracovního poměru či spolupráce s Pracovníkem je jeho nadřízený Pracovník povinen bez zbytečného odkladu informovat oddělení HR, které prostřednictvím informačního systému zadá požadavek na odstranění přístupů a následně Pracovník IT, zruší přístupy Pracovníka do jednotlivých systémů;

Datové soubory musí být šifrovány zejména v následujících případech:

- při zpracování Osobních údajů na přenosných zařízeních – notebook, mobil, tablet;
- v souvislosti s posíláním Osobních údajů přes internet a zejména ve veřejné Wi-Fi síti;

uchování dat na serveru.

Pracovníci jsou zejména povinni:

- nezanechávat svá zařízení obsahující Osobní údaje, bez dozoru, pokud nejsou zabezpečeny v uzamčené místnosti (tj. při odchodu z místnosti Pracovník uzamkne své zařízení);

- používat příslušná bezpečná hesla pro přihlášení do systémů nebo databází obsahujících Osobní údaje, zajistit, aby tato hesla zůstala důvěrná a tato hesla průběžně měnit, tj. nesdělovat hesla a vstupní údaje jiným osobám nebo poskytnout přístup prostřednictvím svých přihlašovacích oprávnění do systému;
- dodržovat vždy standardní postupy pro odhlášení ze systémů. Nesprávným odhlášením může vzniknout příležitost ke zneužití pod identitou Pracovníka;
- nepoužívat sdílené účty.

Odpovědní Pracovníci týmů zajistí zadání informací o nově zaváděném nebo upravovaném procesu zpracování Osobních údajů do Záznamů o činnostech zpracování, a to minimálně pět dní před zahájením nového či změněného procesu zpracování Osobních údajů.

Pověřený Pracovník zajistí vedení a aktualizace vzorových dokumentů (např. posouzení oprávněného zájmu v rámci tzv. balančního testu, posouzení vlivu na ochranu osobních údajů, vzorové souhlasy). Vzorové dokumenty budou vždy uloženy na intranetu.

5. VYTVÁŘENÍ AUDIOVIZUÁLNÍCH ZÁZNAMŮ A JEJICH SDÍLENÍ

Při vytváření audiovizuálních záznamů a jejich šíření, platí, kromě standardních pravidel kapitoly 4, následující pravidla:

a) skupinové audiovizuální záznamy mohou být zpravidla pořizovány bez získání souhlasu Subjektů údajů, na základě oprávněného zájmu JRD a na základě takového oprávněného zájmu a zpravodajské licence šířeny, za splnění následujících podmínek:
   - audiovizuální záznamy jsou pořízeny očekávatelným způsobem v očekávatelném místě a době (tj. např. během koncertu na akci pořádané JRD, nikoliv v šatnách před akcí, prostřednictvím nočního vidění atd.);
   - audiovizuální záznamy nezachycují jedince jakýmkoliv urážlivým či dehonestujícím způsobem;
   - k audiovizuálním záznamům nejsou přiřazené další identifikující informace, např. není pod jejich zobrazením uvedeno jméno osob na fotografiích;
   - v případě žádosti o výmaz provede JRD posouzení trvání oprávněného zájmu a v případě vyhodnocení, že konkrétní zájem dané osoby převyšuje zájem JRD, resp. přesahuje zpravodajskou licenci JRD, audiovizuální záznam odstraní ze zveřejněné zprávy;
   - audiovizuální záznamy nejsou používány čistě k propagačním/reklamním účelům JRD.

b) Veškeré audiovizuální záznamy, které nesplňují podmínky podle písm. a) výše, tj. zejména audiovizuální záznamy jednotlivců, audiovizuální záznamy doprovozené osobními údaji daných osob (např. jméno a příjmení), příp. audiovizuální záznamy určené pro marketingové/reklamní účely JRD musí být pořízeny/sdíleny pouze na základě souhlasu se zpracováním osobních údajů, který může být nicméně poskytnut i po pořízení daného záznamu (např. před použitím takového záznamu v rámci marketingu JRD).

6. ŘÍZENÍ BEZPEČNOSTI A BEZPEČNOSTNÍCH INCIDENTŮ

Za zajištění technické bezpečnosti Osobních údajů odpovídá Pracovník IT, který zajistí, že systémy pro zpracování Osobních údajů JRD splňují následující požadavky:

- zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenává se zejména použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, vytváření nebo rušení objektu informačního systému nebo činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému;
- možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého Pracovníka, bezpečnostního správce nebo správce informačního systému;
- ochranu důvěrnosti dat během přenosu mezi zdrojem a cílem a jejich integritu;
- možnost šifrování Osobních údajů;
- schopnost obnovit dostupnost Osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- možnost pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
- bezpečnost a funkcionalita všech systémů musí být průběžně testovány a vyhodnocovány.
- server, na kterém jsou Osobní údaje uloženy, musí být chráněn proti útoku z internetu firewallem a antivirovým systémem či obdobnými zabezpečovacími prostředky;
- do příslušných Evidencí, včetně fyzických verzí, mají přístup jen ti Pracovníci, kteří je při výkonu své práce potřebují, přičemž přístupová oprávnění jsou definována dle funkcí. Každý Pracovník může do systémů přistupovat pouze pod svým unikátním ID a přístupové údaje nesmí sdílet s dalšími osobami. O udělení přístupu jakýchkoli třetích osob do systémů JRD rozhoduje příslušný odpovědný Pracovník týmu po konzultaci s Pracovníkem IT;
- systém musí pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly Osobní údaje zaznamenány nebo jinak zpracovány/pozměněny;
- datové soubory uložené u JRD jsou pravidelně, alespoň jednou za dva týdny, zálohovány, resp. zálohy se v pravidelných, maximálně dvoutýdenních, intervalech přepisují. JRD může stanovit častější frekvenci zálohování v případech, kdy by ztráta nebo změna Osobních údajů znamenala zvýšené riziko. Zálohy jsou šifrovány. Za zálohování údajů v aplikacích a systémech provozovaných třetími stranami odpovídají tyto třetí strany na základě smluvních povinností jimi převzatými dle smluvního ujednání s JRD.

6.1. Hlášení bezpečnostních incidentů

Jakýkoliv případ porušení zabezpečení Osobních údajů, zejména ztrátu, odcizení, poškození či zničení Osobních údajů (bez ohledu na riziko zásahu do práv Subjektů údajů související s konkrétním případem porušení zabezpečení Osobních údajů) je každý Pracovník, který se o takové skutečnosti dozví, povinen neprodleně oznámit Pověřenému Pracovníkovi Compliance.

V rámci tohoto hlášení uvede Pracovník, který se se dozví o případu porušení zabezpečení Osobních údajů nebo pouhé hrozbě, především:

- co nejúplnější a nejpřesnější popis povahy daného případu porušení zabezpečení Osobních údajů nebo hrozby, včetně, pokud je to možné, kategorií a přibližného počtu dotčených Subjektů údajů a kategorií a přibližného množství dotčených záznamů Osobních údajů;
- popis pravděpodobných důsledků porušení zabezpečení Osobních údajů;
- návrh možných opatření s cílem vyřešit dané porušení zabezpečení Osobních údajů, příp. předejít dané hrozbě, včetně případných opatření ke zmírnění možných nepříznivých dopadů, který bude konzultován či připraven ve spoluprací s pověřeným Pracovníkem Compliance.

Pověřený Pracovník Compliance zhodnotí, zda se může jednat o porušení zabezpečení Osobních údajů, při kterém dochází k rizikům ohledně práv a svobod Subjektů údajů. Porušením zabezpečení Osobních údajů, při kterém dochází k rizikům ohledně práva svobod Subjektů údajů se rozumí např. únik Osobních údajů, jejich pozměnění nebo jiné zneužití, které může vést k poškození práv a svobody Subjektů údajů, např. ztrátu listinných dokumentů obsahujících Osobní údaje, které byly součástí manuálně vedené Evidence nebo byly vytištěny z počítače, ve kterém je taková Evidence vedena, odeslání Osobních údajů neoprávněnému adresátovi.

Porušením zabezpečení Osobních údajů nejsou situace, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby (např. momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené Evidence (kartotéky) fyzických osob nebo byl vytištěn z počítače, ve kterém je taková Evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení, odeslání Osobních údajů na neexistující e-mail).

Jakékoliv porušení zabezpečení Osobních údajů s potenciálním rizikem pro Subjekty údajů je JRD povinen bez zbytečného odkladu nahlásit ÚOOÚ, pokud možno do 72 hodin od okamžiku, kdy se JRD o tomto porušení dozvěděl. Pokud tuto skutečnost ÚOOÚ neoznámí do 72 hodin, uvede JRD současně s oznámením důvody tohoto zpoždění.

Oznámení ÚOOÚ lze učinit výhradně podle rozhodnutí pověřeného Pracovníka Compliance, který o odeslání oznámení informuje Pověřeného člena správní rady.

K Oznámení JRD připojí oznámení případu porušení zabezpečení dotčeným Subjektům dle následujícího článku.

7. OZNÁMENÍ SUBJEKTŮM ÚDAJŮ

Subjektům údajům dotčeným porušením zabezpečení jejich Osobních údajů je nutné ohlásit, pokud je pravděpodobné, že případ bude mít za následek vysoké riziko pro práva a svobody dotčených osob, (tj. například unikly, nebo byly zneužity mzdové informace zaměstnanců JRD, informace o kupní smlouvě / způsobu financování koupě Projektu klientů JRD, zdravotní či jiné údaje kohokoliv atd.). Oznámení dotčeným Subjektům údajů musí obsahovat popis povahy porušení zabezpečení, a přinejmenším tyto informace:

- jméno a kontaktní osoby, která může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení Osobních údajů (zejména ve vztahu vůči dotčeným Subjektům údajů);

- popis opatření, která JRD přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení Osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

8. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

Při každé spolupráci s třetí stranou, při které dochází k jakémukoli předání Osobních údajů (tj. sdílení, export, náhled atd.), je nutné určit, v jakém postavení se bude tato třetí strana – příjemce nacházet.

Třetí strana může být v postavení zpracovatele, v postavení společných správců spolu s JRD, nebo v postavení samostatného správce, v případě že jsou takové třetí straně Osobní údaje pouze předány a ta následně rozhoduje o zpracování Osobních údajů jako samostatný správce (např. přepravní společnosti, společnosti zajišťující ubytování v případě teambuildingu atd.)

9. URČENÍ POSTAVENÍ JRD A DALŠÍCH STRAN

a) Správcem je při zpracování osobních údajů vždy ta strana, která rozhoduje:

- o samotném shromáždění a zpracování Osobních údajů;
- o určení účelu zpracování Osobních údajů;
- o dalších podmínkách a prostředcích zpracování, zejména:
- jaké kategorie Osobních údajů budou zpracovávány;
- Osobní údaje, kterých Subjektů údajů budou zpracovávány;
- obecné prostředky zpracování Osobních údajů;
- dobu uchování Osobních údajů
- zda údaje předat, a pokud ano, komu; a
- jak reagovat na žádosti Subjektů údajů.

b) Zpracovatel může na základě dohody s JRD rozhodnout, jak provádět určité činnosti v rámci zpracování, aniž by se sám stal správcem, např. určit:

- jaké IT systémy použít ke zpracování osobních údajů;
- jak uchovávat osobní údaje;
- podrobnosti o bezpečnostních opatřeních k ochraně osobních údajů;
- jak bude získávat osobní údaje, je-li jejich získáním pověřen;
- jak zajistí dodržení doby uchování a jakým způsobem data vymaže nebo zlikviduje.

Společné správcovství vzniká pouze pokud JRD spolu s jiným subjektem spoluurčují účel a prostředky zpracování osobních údajů (bod a) viz výše). Role lze rozdělit, že obě strany se

dohodnou na všech podmínkách zpracování, ale i tak, že jeden ze společných správců bude určovat účel a druhý prostředky zpracování. Jedná se zejména o vztahy v rámci skupiny JRD.

9.1. Vztah správce x zpracovatel

JRD může udělit jinému subjektu oprávnění zpracovatele ke zpracování Osobních údajů pouze na základě písemné smlouvy o zpracování Osobních údajů, pokud takové oprávnění nevyplývá z příslušných právních předpisů.

Odpovědný Pracovník týmu rozhodne o využití pouze těch zpracovatelů, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky platných právních předpisů a aby byla zajištěna ochrana práv Subjektů údajů.

9.2. Vztah společných správců

JRD může spolupracovat s jiným subjektem, u kterého vznikne společné správcovství, pouze na základě písemného vymezení podílů na odpovědnosti za plnění povinností dle Nařízení GDPR.

9.3. Vztah správce x správce

Pokud JRD Osobní údaje pouze předává je nutné mít k takovému předání správný právní základ předání (např. plnění smlouvy o organizace akce při předání přepravní společnosti, plnění právní povinnosti správce v rámci daňového řízení aj.). V rámci předávání nemusí JRD uzavírat žádnou smlouvu o ochraně Osobních údajů.

10. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ MIMO EVROPSKOU UNII

K předání Osobních údajů mimo Evropskou unii, resp. mimo Evropský hospodářský prostor (a to v jakékoliv verzi rozdělení odpovědnosti, tj. správce x zpracovatel, společní správci či správce x správce) může dojít pouze po konzultaci s pověřeným Pracovníkem Compliance a zástupcem oddělení Legal, a pouze tehdy, pokud je v dotyčné třetí zemi zajištěna odpovídající úroveň ochrany dle čl. 10.1. anebo jsou zavedena opatření dle čl. 10.2.

10.1.Odpovídající úroveň ochrany Osobních údajů ve třetí zemi jako celku nebo v určitém sektoru třetí země může být konstatována výlučně prostřednictvím rozhodnutí Evropské komise (aktuální seznam zde).

10.2. Pokud neexistuje rozhodnutí Evropské komise o odpovídající ochraně Osobních údajů v dané zemi, mohou být Osobní údaje do třetí země předány, pouze:

- na základě tzv. závazných podnikových pravidel;
- na základě smluvních ujednání s příjemcem Osobních údajů např. za použití standardních smluvních ustanovení schválených Evropskou komisí;

- dodržování kodexu chování nebo mechanismu pro vydávání osvědčení společně se získáním závazných a vymahatelných závazků od příjemce pro uplatnění vhodných záruk na ochranu předaných Osobních údajů (aktuálně není subjekty využíváno).

11. INFORMOVÁNÍ SUBJEKTŮ ÚDAJŮ

a) V případě, kdy JRD získalo Osobní údaje přímo od Subjektu údajů, je povinno jej poučit ve smyslu čl. 13 GDPR Za tím účelem zajistí, aby se Subjekt údajů řádně seznámil s obsahem poučení a aby Subjekt údajů tuto skutečnost stvrdil svým podpisem či jiným prokazatelným projevem vůle.

b) V případě, že Osobní údaje nebyly získány od Subjektu údajů, je JRD povinno jej poučit ve smyslu čl. 14 GDPR. Za tímto účelem zajistí, aby se Subjekt údajů řádně seznámil s obsahem poučení a aby Subjekt údajů tuto skutečnost stvrdil svým podpisem či jiným prokazatelným projevem vůle.

Informace uvedené v bodu a) (viz výše) poskytne JRD Subjektu údajů nejpozději v okamžiku získání Osobních údajů a informace uvedené v bodu b) (viz výše) poskytne JRD Subjektu údajů v přiměřené lhůtě po získání Osobních údajů, ale nejpozději do 30 dnů. V případech, kdy mají být Osobní údaje použity pro účely komunikace, poskytne tyto informace v okamžiku, kdy poprvé dojde k této komunikaci, anebo pokud mají být Osobní údaje zpřístupněny jinému příjemci, poskytne JRD informace při prvním zpřístupnění Osobních údajů.

11.1. Uplatní-li Subjekt údajů právo na přístup ke svým Osobním údajům dle čl. 15 GDPR, je mu JRD povinen tuto informaci předat bez zbytečného odkladu, ale nejpozději do 30 dnů ode dne doručení žádosti. Informace jsou poskytnuty zásadně ve formě, ve které Subjekt údajů uplatňuje své právo (tj. elektronická žádost – elektronická odpověď atd.)

JRD je povinno před sdělením informací o zpracování v rámci uplatněného práva na přístup ze strany Subjektu údajů ověřit identitu dotazujícího se Subjektu údajů. K ověření identity Subjektu údajů, který žádá o přístup k Osobním údajům, využije JRD všech vhodných opatření (např. v případě klienta JRD – informace o kupní smlouvě, v případě zaměstnance – informace o pracovním poměru, obecně vyžádání např. potvrzení rodného čísla atd.) Není-li JRD schopno dostatečně identifikovat Subjekt údajů, informuje ho o této skutečnosti, pokud je to možné. Ověřování identity není zneužíváno k získávání dalších údajů a k jejich uchování za jinými účely, než je reakce na konkrétní žádost Subjektu údajů.

Obsahem informace uvedené v čl. 11.1. je sdělení o:

- účelu zpracování Osobních údajů,
- Osobních údajích, případně kategoriích Osobních údajů, které jsou předmětem zpracování,
- příjemci, případně kategoriích příjemců,
- době, po kterou budou Osobní údaje uloženy,
- existenci práva požadovat od JRD opravu nebo výmaz Osobních údajů týkajících se Subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování,
- právu podat stížnost u Úřadu pro ochranu osobních údajů,
- veškerých dostupných informacích o zdroji Osobních údajů, pokud nejsou získány od Subjektu údajů, a

- skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování a v těchto případech smysluplné informace týkající se použitého postupu, jakož i sdělení o významu a předpokládaných důsledcích takového zpracování pro Subjekt údajů.

12. ŠKOLENÍ

Všem Pracovníkům je nutné poskytnout pokyny ohledně dodržování ochrany Osobních údajů adekvátní k práci, kterou vykonávají. Pověřený Pracovník Compliance zajistí zavedení školicího programu o ochraně Osobních údajů.

Za účelem posílení ochrany Osobních údajů zajistí Pověřený Pracovník Compliance zejména pravidelná školení a osvětové programy v oblasti ochrany Osobních údajů, kterých se zúčastní všichni Pracovníci., není-li rozhodnuto jinak. V rámci poskytovaného školení je třeba zajistit, aby všechny školené osoby byly seznámeny s touto Směrnicí.

13. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

JRD nejmenoval pověřence pro ochranu Osobních údajů, neboť neprovádí zpracování, jehož hlavní činnost spočívá v operacích, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé, pravidelné a systematické monitorování Subjektů údajů anebo v operacích spočívajících v rozsáhlém zpracování zvláštních kategorií Osobních údajů a Osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.