Obecné Zásady ochrany osobních údajů EU

Gruppo Bondioli & Pavesi

Obsah

1. PREMISA

Bondioli & Pavesi Group přikládá velký význam dodržování Zásad ochrany osobních údajů a s nimi spojených předpisů za účelem správného rozvoje vlastního provozu, podnikání a image na trhu. Ochrana osobních údajů, které každá společnost skupiny shromažďuje a ukládá pomocí elektronických systémů nebo klasických metod, představuje významnou a strategickou hodnotu pro skupinu a pro rozvoj podnikání.

Z tohoto pohledu představuje nařízení (EU) 2016/679 (dále také „**GDPR**“) jádro nových evropských právních předpisů o ochraně osobních údajů a představuje hlavní referenční základnu pro činnosti zahrnující osobní údaje v prostředí EU.

Z tohoto důvodu je nezbytné přijmout společné Zásady ochrany osobních údajů (dále jen „**Zásady**“) pro společnosti se sídlem v EU uvedené v bodě 3 (dále jen „**společnost**“ a souhrnně „ **EU Group** “) a upozornit všechny zaměstnance a ty, kteří pracují jménem a pro jednotlivé společnosti, na zásady a pravidla, kterými se chce EU Group řídit, aby byla zaručena jednotná a vysoká úroveň ochrany osobních informací.

S ohledem na složitost právních předpisů na jedné straně a podnikových procesů, které zahrnují osobní údaje na straně druhé, je nejprve nutné ve společnostech EU Group vytvořit strukturu řízení ochrany osobních údajů, která definuje strukturu úloh, odpovědností a úkolů souvisejících s ochranou osobních údajů

2. CÍL

Záměrem těchto Zásad je popsat:

(i). zásady a metody, které musí každá společnost dodržovat při zpracovávání osobních údajů,
(ii). organizace ochrany osobních údajů za účelem správy a řízení věci, a
(iii). přidělování úkolů a odpovědností na různých operačních úrovních.

Z tohoto důvodu musí být tyto zásady zohledněny všem osobám, které ve společnostech zpracovávají osobní údaje.

3. OBLAST PŮSOBNOSTI

Tyto Zásady je nutné dodržovat v následujících společnostech:

- všechny italské společnosti, které jsou součástí Bondioli & Pavesi Group;
- Bondioli & Pavesi GMBH;
- Bondioli & Pavesi France SA;
- Bondioli & Pavesi Iberica SA;

- Bondioli & Pavesi Sp. Zo.o.;
- OM Protivín AS.

Každá z nich musí kromě přizpůsobení se následujícím zásadám jednoznačně dodržovat GDPR a doplňkové místní předpisy o ochraně osobních údajů a ochraně osobních údajů.

4. DEFINICE

Pro účely zásad jsou v relevantním pořadí uvedeny následující definice odvozené od GDPR:

- **osobní údaj**: veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby („ **dotčený subjekt**"), identifikovatelnou osobou se rozumí fyzická osoba, kterou lze identifikovat přímo nebo nepřímo, se zvláštním odkazem na identifikátor, jako je jméno, identifikační číslo, údaje o poloze, online identifikátor nebo jeden nebo více charakteristických prvků její fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity. Dále v případě marketingových aktivit, které nejsou příjemcem požadovány (např. spontánní zasílání reklamních materiálů, přímý prodej, provádění průzkumu trhu nebo obchodní komunikace), také jakékoli informace týkající se právnické osoby - včetně organizací nebo sdružení -.
  Jedná se například o: osobní údaje, poštovní, telefonní, telematické adresy, identifikační kódy, objednávky, obrat, zjev, hlas, životopis, nákupní návyky, protokoly o přístupu k systému a obecněji vše zaznamenané na papíře nebo elektronicky, co lze případně dát do souvislosti s identifikovaným nebo identifikovatelným subjektem.

- **Zpracování:** jakákoli operace nebo soubor operací prováděných pomocí automatických procesů nebo bez nich a aplikovaných na osobní údaje nebo soubory osobních údajů, jako je shromažďování, registrace, organizace, strukturování, ukládání, přizpůsobení nebo modifikace, extrakce, konzultace, použití, komunikace přenosem, šíření nebo jakákoli jiná forma zpřístupnění, srovnání nebo propojení, omezení, vymazání nebo zničení.
  Například: správa mezd a docházky zaměstnanců, správa smluv, zasílání marketingové komunikace, profilování, video dohled atd.

- **Zvláštní kategorie osobních údajů:** osobní údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo odborové členství, jakož i genetické údaje nebo biometrické údaje určené k jednoznačné identifikaci fyzické osoby,údaje týkající se sexuálního života nebo sexuální orientace osoby. Jedná se o podsoubor osobních údajů.
  Například: Potvrzení o nemoci, členství v odborech, povolení pro odboráře, zdravotní postižení, nehody, členství v nějaké straně, zdravotní stav atd.

- **Osobní údaje. týkající se odsouzení za trestný čin a trestných činů:** (dále jen „**Údaje o trestných činech**“) osobní údaje týkající se odsouzení za trestný čin a trestných činů nebo souvisejících bezpečnostních opatření. Jedná se o podsoubor osobních údajů.

- **Správce osobních údajů**: fyzická nebo právnická osoba, orgán veřejné moci, služba nebo jiný orgán, který jednotlivě nebo společně s ostatními určuje účely a prostředky zpracování osobních údajů.
  Pokud jsou například webové stránky spravovány výhradně společností Bondioli & Pavesi S.p.A., bude za zpracování souvisejících údajů odpovídat samotná společnost jako správce.
  Správcem bude každá společnost, když si samostatně zvolí, jak provádět zpracování. Například zpracování údajů o zaměstnancích implikuje, že jednotlivé společnosti jsou správcem osobních údajů.

- **Zpracovatel osobních údajů:** fyzická nebo právnická osoba, orgán veřejné moci, služba nebo jiný orgán, který zpracovává osobní údaje jménem správce, v souladu s čl. 28 GDPR.

- **Osoba oprávněná ke zpracování osobních údajů:** (též pověřená osoba) fyzická osoba, která zpracovává osobní údaje z pověření správce nebo zpracovatele;

- **Dotčený subjekt.** Identifikovaná nebo identifikovatelná fyzická osoba, které se osobní údaje týkají. Dále, v případě marketingových aktivit, které příjemce nepožaduje (např. spontánní zasílání reklamních materiálů, přímý prodej, provádění průzkumu trhu nebo obchodní komunikace), je dotčeným subjektem také právnická osoba - včetně organizací nebo sdružení -, podle směrnice (EU) e-privacy 2002/58 o zpracování osobních údajů a ochraně soukromí a následných dodatků a změn.
  Jsou to například: zákazníci, včetně těch potenciálních, zaměstnanci, uchazeči o zaměstnání, poradci, dodavatelé, návštěvníci, uživatelé webových stránek správce atd.

5. ORGANIZAČNÍ MODEL OCHRANY OSOBNÍCH ÚDAJŮ EU GROUP

Za účelem zajištění homogenity činností v oblasti ochrany osobních údajů se EU Group se rozhodl přijmout následující organizační model:

- **Korporátní referent:** má za úkol koordinaci ochrany osobních údajů na úrovni celé EU Group a poskytovat funkční vedení všem referentům pro ochranu soukromí jmenovaným v rámci EU Group. Podrobnosti o přidělených odpovědnostech a úkolech jsou uvedeny v dokumentu [**uveďte podrobnosti]**, který je k dispozici [**uveďte podrobnosti**] a je přístupný referentům;
- **Hlavní referent**: má za úkol koordinaci ochrany osobních údajů na úrovni jednotlivé společnosti, která jej jmenovala, posuzovanou v celém rozsahu, a poskytovat funkční vedení všem případným jmenovaným referentům pro funkci uvnitř téže společnosti. Podrobnosti o přidělených odpovědnostech a úkolech jsou uvedeny v dokumentu [**uveďte podrobnosti]**, který je k dispozici [**uveďte podrobnosti**] a je přístupný referentům;

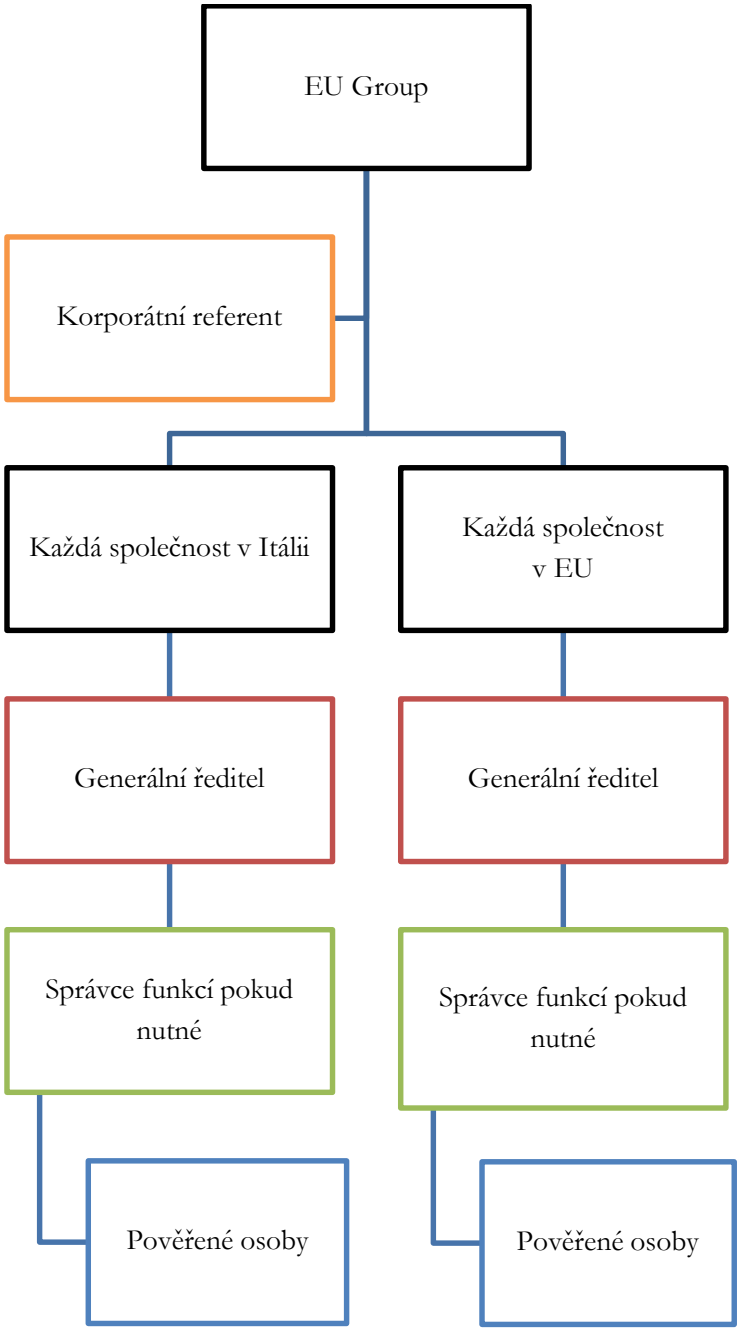
- **Referent pro funkci:** má za úkol koordinaci ochrany osobních údajů na úrovni podnikového úseku, který mu byl přidělen uvnitř společnosti, která ho jmenovala. Podrobnosti o přidělených odpovědnostech a úkolech jsou uvedeny v dokumentu [**uveďte podrobnosti]**, který je k dispozici [**uveďte podrobnosti**] a je přístupný referentům; Tento referent je jmenován, pouze pokud to hlavní referent považuje za nutné.

Aktualizovaný seznam všech jmenovaných referentů je k dispozici [**uveďte podrobnosti].**

- **Oprávněná/pověřená osoba:** je fyzická osoba, která fyzicky zpracovává osobní údaje pomocí IT nástrojů a/nebo na papíře v podnikovém úseku, k němuž je přiřazena. Každá společnost musí určit pověřenou osobu, která při plnění svých povinností zpracovává osobní údaje. Dokument jmenování pověřené osoby s definicí rozsahu povoleného zpracování, zadanými pokyny a svěřenými úkoly je k dispozici [**uveďte podrobnosti**].

6. ORGANIZAČNÍ MODEL OCHRANY OSOBNÍCH ÚDAJŮ EU

Na základě výše uvedeného je organizační schéma ochrany osobních údajů uspořádáno následovně:



7. DALŠÍ ZAPOJENÉ SUBJEKTY

Do správy osobních údajů mohou být zapojeny další subjekty, včetně:

- **Zpracovatel osobních údajů**: jak již bylo uvedeno, je to externí subjekt, který provádí zpracování osobních údajů jménem správce. Tato zpracování musí probíhat na základě písemné smlouvy, která stanoví předmět, dobu trvání zpracování, povahu a účel zpracování, druh osobních údajů, kategorie dotčených subjektů, povinnosti a práva správce. V rámci EU musí tato smlouva obsahovat také základní náležitosti předepsané čl. 28 odst.3 nařízení GDPR.

Služby, které lze obvykle přenést na externí zpracovatele, jsou například správa mezd, správa webových stránek, správa IT podpory atd.

- **DPO**: Data Protection Oficier je subjekt stanovený v čl. 37 a následujících, který musí společnost jmenovat pokaždé, když:
  - hlavní činnosti správce nebo zpracovatele osobních údajů spočívají ve zpracování, která svou povahou, rozsahem a/nebo účelem vyžadují pravidelné a systematické sledování dotčených subjektů ve velkém měřítku; nebo když,
  - hlavní činnosti správce nebo zpracovatele osobních údajů spočívají ve zpracování ve velkém měřítku speciálních kategorií osobních údajů uvedených v článku 9 GDPR nebo údajů o odsouzení za trestné činy a o trestných činech uvedených v článku 10 GDPR.

  Mezi jeho hlavní úkoly patří kontrola dodržování zásad GDPR, poskytování poradenství společnosti, sledování vykonaných operací, školení a zvyšování povědomí o daném předmětu atd.

  Pro společnosti bylo považováno za zbytečné jmenovat DPO vzhledem k typické činnosti společností, která ze své podstaty nezahrnuje rizika v oblasti ochrany osobních údajů, vzhledem k minimální činnosti zpracování osobních údajů dotčených subjektů, která se určitě neprovádí ve velkém měřítku, a vzhledem ke skutečnosti, že zpracování zvláštních kategorií údajů v rámci pracovního poměru není hlavní, ale vedlejší činností (viz WP29, Pokyny DPO, 2.1.2., s. 9), je tedy zřejmé, že neexistují podmínky k výše uvedené věci.
  Pokud místní směrnice nebo předpisy vyžadují jmenování pověřené osoby pro ochranu údajů DPO u jedné ze společností (mimo italské), je třeba o této skutečnosti předem informovat korporátního referenta.

- **Další potenciální subjekty**: místní předpisy mohou stanovit potřebu identifikovat další relevantní subjekty za účelem ochrany osobních údajů. Každá společnost má povinnost posoudit, zda existují místní právní předpisy, které ukládají podobné povinnosti.
  Například v Itálii existuje úloha správců systému, kteří jsou fyzickými osobami odpovědnými za technické řízení celého informačního systému nebo dokonce jen za jednu z jeho složek nebo za související činnosti. Tyto osoby musí obdržet zvláštní označení jako správce systému a k tomu příslušné instrukce pokyny.

8. OBECNÉ ZÁSADY

V souvislosti se zpracováním osobních údajů hodlá EU Group přijmout veškerá nejvhodnější technologická, organizační a logistická opatření k zajištění účinného dodržování záruk na ochranu osobních údajů.
Za tímto účelem musí procesy společnosti a fyzické operace zpracování osobních údajů, které jsou prováděny osobami pověřenými zpracováním, dodržovat následující zásady.

8.1. **Zákonnost, správnost a transparentnost**

Zpracování osobních údajů musí být prováděno pouze tehdy, je-li splněna jedna z podmínek vyžadovaných zákonem, která to umožňuje, a pouze pokud si je dotčený subjekt toho vědom a odpovídá to tomu, co mu je deklarováno.

8.2. **Omezení účelu**

Osobní údaje musí být zpracovávány pouze pro účely deklarované dotčenému subjektu a nesmí být neslučitelné s těmito účely.

8.3. **Minimalizace údajů**

Použití osobních údajů musí být minimalizováno, a proto, pokud lze dosáhnout účelů i bez použití osobních údajů, musí být zpracování prováděno s anonymními údaji. Anonymní údaje jsou údaje, které nelze žádným způsobem spojit s identifikovaným nebo identifikovatelným dotčeným subjektem. Osobní údaje musí být přiměřené, relevantní a omezené na to, co je nezbytné ve vztahu k účelům, pro které jsou zpracovávány.

8.4. **Přesnost**

Zpracovávané údaje musí být správné a aktuální a dotčený subjekt musí být schopen je ověřit a opravit.

8.5. **Omezení uchovávání**

Zpracovávané osobní údaje nesmí být uchovávány po neomezenou dobu. Jakmile je dosaženo účelu, musí být vymazány, a proto musí každá společnost určit dobu uchovávání, která je kompatibilní s tímto účelem a v souladu s místními předpisy.

8.6. **Integrita a důvěrnost**

Každá společnost musí zpracovávat osobní údaje tak, aby zajistila odpovídající zabezpečení a důvěrnost, a rovněž tak, aby zabránila neoprávněnému přístupu nebo použití osobních údajů a nástrojů používaných ke zpracování.

8.7. **Odpovědnost**

Každá společnost musí zaručit dodržování výše uvedených zásad a musí být schopna to prokázat.

9. OPERATIVNÍ PRAVIDLA

Při uplatňování výše popsaných zásad a dalších předpisů uvažovaných GDPR musí každá společnost fungovat v souladu s následujícími operativními pravidly.

9.1. **Registry činností zpracování.**

Každá společnost musí prostřednictvím svých referentů vést důkazy o IT a ručním zpracování prováděném vnitropodnikově různými odděleními společnosti. Každá společnost musí tuto

povinnost splnit sestavením registrů činností zpracování uvedených v čl. 30 GDPR a dodržovat pokyny poskytnuté v každé zemi místními kontrolní úřady.
Odpovědnost za zajištění toho, aby každá společnost udržovala a neustále aktualizovala registry požadované podle GDPR, nese hlavní referent, který za tímto účelem musí zavést konkrétní postup řízení, s určením odpovědností a úkolů ve společnosti a zahrnout do toho, pokud existují, referenty pro funkci.
V každém případě musí být aktualizace registrů prováděna alespoň jednou ročně.

9.2. **Informace a shromažďování osobních údajů (transparentnost a správnost).**

Obvykle jsou osobní údaje poskytovány přímo dotčeným subjektům jako součást běžných obchodních kontaktů a při výkonu provozních činností společnosti nebo prostřednictvím webových stránek, ale lze je získat také od třetích stran. Zaměstnanci, kteří shromažďují osobní údaje dotčeného subjektu, musí při příležitosti shromažďování údajů zajistit, aby dotčený subjekt byl přiměřeně informován o účelech, pro které jsou údaje shromažďovány a následně zpracovávány.
Za tímto účelem musí poskytnout příslušný „informační" dokument připravený společností.
Informaci je vždy nutné podat, i když není nutné žádat dotčený subjekt o souhlas se zpracováním jeho údajů.
Operace, pro které nebyly vydány žádné informace nebo které nejsou popsány v samotných informacích, jsou nezákonné, a proto je nelze provádět.
Informace musí být poskytnuty „jednorázově" a musí předcházet prvnímu shromažďování osobních údajů o dotčeném subjektu.
V případě změny některých prvků uvedených v dříve uvedeném informačním dokumentu musí být poskytnuty nové informace.

9.3. **Podmínky zákonnosti zpracování osobních údajů**

Pro každý účel uvedený v informacích musí být určen alespoň jeden právní základ, který činí zpracování zákonným.
Právní základy jsou ty, které jsou uvedeny v čl. 6 GDPR pro „běžné" osobní údaje, které v krátkosti spočívají v následujících alternativách:

- Souhlas
- Plnění smlouvy
- Výkon právní povinnosti
- Ochrana životně důležitých zájmů
- Úkol veřejného zájmu
- Oprávněný zájem (který nepřevažuje nad právy dotčeného subjektu)

Pokud jde o zpracování zvláštních kategorií údajů, právní základy jsou uvedeny v čl. 9 GDPR a čl. 10 pro údaje o trestných činech a jsou přísnější než pro běžné údaje.

9.4. **Souhlas dotčeného subjektu *(zákonnost*).**

Mezi právními základy zákonnosti je uveden souhlas dotčeného subjektu. Souhlas nelze shromažďovat, pokud je zpracování založeno na jedné z dalších podmínek zákonnosti (jak je uvedeno v předchozím bodě). Některé způsoby zpracování však nutně vyžadují souhlas jako podmínku zákonnosti. Operace zpracování musí být v souladu s tímto souhlasem vydaným dotčeným subjektem v reakci na informaci. Souhlas musí být svobodně udělen dotčenou stranou, může být shromážděn pouze na základě vhodných informací a musí být prokazatelný a jednoznačný.

Pokud je k provedení zpracování nezbytný souhlas, není povoleno zpracování provádět, pokud nebyl souhlas získán.

9.5. **Povolený přístup zaměstnanců k osobním údajům a činnostem.**

Přístup k osobním údajům a provádění činností zpracování je povoleno pouze těm osobám, které byly řádně oprávněny a byly jim poskytnuty náležité pokyny. Tyto osoby pověřené zpracováním osobních údajů budou mít přístup k údajům pouze na základě kritéria „need to know". Osobní údaje musí být použity pouze pro účely plnění úkolů a dalších úkolů, které jsou postupně přidělovány.

Jak již bylo uvedeno výše, je nutno zdůraznit, že:

- Operace, pro které nebyly vydány žádné informace nebo které nejsou popsány v samotných informacích, nelze provést;
- v případě potřeby není povoleno provádět zpracování, pro které nebyl získán souhlas.

9.6. **Přístup ke zvláštním kategoriím osobních údajů a údajům o trestných činech a personálu povolené činnosti.**

Tyto údaje musí být zpracovávány pouze pověřenými osobami, v rámci nezbytné nutnosti pro výkon jejich povinností a výslovně k tomu oprávněných.

Kromě výše popsaných omezení týkajících se potřeby informací a možného souhlasu, mějte na paměti, že operace zpracování těchto údajů musí také splňovat podmínky a omezení stanovené místními předpisy.

Například v Itálii jsou podmínky a omezení stanoveny v Obecných oprávněních vydaných Úřadem ochrany osobních údajů, které jsou k dispozici na webových stránkách úřadu (www.garanteprivacy.it).

Proto není povoleno provádět jiný druh zpracování, než ten, který je předepsaný místními předpisy.

9.7. **Bezpečnostní opatření.**

Všechny pověřené osoby jsou povinny přísně dodržovat bezpečnostní předpisy připravené společností. Jejich nedodržení může mít závažné právní důsledky, někdy i trestní povahy. Dodržování určitých bezpečnostních opatření závisí výlučně na jednání pověřených osob.

9.8. **Šíření osobních údajů a sdělování údajů třetím stranám.**

Osobní údaje lze povoleně šířit v rámci společností EU Group mezi pověřenými osobami, které je potřebují znát pro pracovní potřeby (*need to know*) a které v této věci obdržely instrukce. Nesmí

však být předány - ani v žádném případě zpřístupněny - třetím stranám mimo EU Group, pokud nenastane jeden z následujících případů:

- předání třetí straně je nutné pro splnění zákonné povinnosti nebo příkazu orgánu veřejné moci;
- předání třetí straně je nutné pro plnění povinností vyplývajících ze smlouvy podepsané s dotčeným subjektem, jehož se osobní údaje týkají;
- pokud byla třetí osoba jmenována zpracovatelem údajů, v souladu s čl. 28 GDPR, a údaje jsou nutné pro provedení služby zadané externě;
- osoba, jíž se týkají osobní údaje, výslovně vyjádřila souhlas s předáním příslušných údajů této třetí straně.

Jakákoli potřeba předání osobních údajů třetí straně pro jiné možné důvody, než výše uvedené, musí být založena na písemném povolení stávajícího hlavního referenta společnosti.

V žádném případě není součástí politiky EU Group, z jakéhokoli důvodu nebo k jakémukoli účelu, předávat soupisy, seznamy nebo adresy, které by mohlo být chápáno jako prodávání osobních údajů.

9.9. **Nová zpracování a zpracování s vysokým rizikem**.

Bez předchozího povolení nelze zahájit nová zpracování obnášející vysoké riziko, tak jak je definováno a upraveno v zásadách společnosti týkajících se posouzení dopadu předpokládaného zpracování na ochranu osobních údajů (posouzení dopadů nebo **DPIA**). Hlavní prvky, které je třeba posoudit a které mohou pro dotčené subjekty představovat vysoká rizika, jsou tyto:

- Hodnocení, bodování nebo profilování
- Automatizovaný rozhodovací proces, který má právní účinek nebo podobně významně ovlivňuje fyzické osoby
- Systematické monitorování
- Zpracování zvláštních kategorií údajů
- Zpracování údajů v rozsáhlém měřítku
- Vytváření shod nebo kombinací souborů údajů
- Zpracování údajů týkajících se zranitelných dotčených subjektů
- Inovativní využití nebo použití nových technologických nebo organizačních řešení
- Zpracovávání, které samo o sobě „brání dotčeným subjektům ve výkonu práva nebo využívání služby nebo smlouvy“.

Kromě těchto prvků mohou místní právní předpisy stanovit další rizikové případy nebo případy, kdy je DPIA povinné. V Itálii Úřad ochrany osobních údajů a soukromí stanovil, že DPIA je povinné v řadě případů, například během takového zpracování údajů, které není příležitostné a týká se zranitelných subjektů nebo během systematického zpracovávání biometrických údajů atd.

9.10. **Porušení osobních údajů (Data breach)**

Porušením osobních údajů e rozumí „porušení bezpečnosti, které náhodně nebo nezákonně zahrnuje zničení, ztrátu, změnu, neoprávněné vyzrazení nebo přístup k přenášeným, uloženým nebo jakkoli zpracovaným osobním údajům“ (dále jen „**Data breach**“).

V případě Data breach je povinné informovat kontrolní úřad (místní Úřad ochrany) do 72 hodin od zjištění porušení.

EU Group přijal zásady správy Data breach, která musí být známá a dostupná všem pověřeným osobám, které v případě výskytu uvedené situace musí tuto skutečnost neprodleně nahlásit svému referentovi pro funkci nebo, pokud chybí, hlavnímu referentovi, aby plně dodržena lhůta pro oznámení.

9.11. **Privacy by design a by default**

EU Group přijal zásady ochrany osobních údajů a soukromí by design a ochrany by default, které je třeba dodržovat v případě vývoje nových aplikací a nových způsobů zpracování a které musí být dány na vědomí všem pověřeným osobám zapojeným do navrhování a vývoje takových aplikací a zpracování.

9.12. **Správa práv dotčených subjektů**

GDPR uznává následující práva dotčeným subjektům:

- Právo přístupu k vlastním osobním údajům (čl. 15);
- Právo na opravu (čl. 16);
- Právo na výmaz (právo být zapomenut) (čl. 17);
- Právo na omezení zpracování (čl. 18);
- Právo na přenositelnost osobních údajů (čl. 20);
- Právo na námitku (čl. 21);
- Právo vznést námitku proti rozhodnutí založenému výhradně na automatizovaném zpracování (čl. 22);
- Právo kdykoli odvolat udělený souhlas, aniž je dotčena zákonnost zpracování založeného na souhlasu uděleném před odvoláním (čl. 7.3);

EU Group přijal zásady pro správu žádostí o výkon výše uvedených práv s doplňujícím popisem jejich obsahu. Zásady musí být známé a snadno dostupné všem pověřeným osobám zapojeným do procesu správy těchto požadavků. Vezměte prosím na vědomí, že v případně nesprávné správy žádostí v rámci zásad, má dotčený subjekt právo podat stížnost u Úřadu ochrany osobních údajů nebo se obrátit na soud za účelem ochrany svých práv.

10. ŠKOLENÍ

GDPR stanoví povinnost informovat pověřené osoby o rizicích spojených se zpracováním osobních údajů. Každá společnost proto musí zajistit, aby pověřené osoby byly informovány a bylo jim poskytnuto vhodné školení odpovídající zadaným úkolům.

Školení nemůžou být jednorázová, ale je třeba je pravidelně opakovat, zejména při změnách v předpisech nebo v případě přijetí nových interpretačních pokynů.
Pro účely školení lze dát k dispozici dokumenty a prezentace, které ilustrují hlavní aspekty legislativy, e-learningové programy, přednášky, sdělení atd.

Tato školení musí být povinně zdokumentována (v souladu se zásadou odpovědnosti). Každý zaměstnanec je povinen prohlubovat své znalosti o ochraně osobních údajů, aby mohl pracovat v plném souladu s předpisy, těmito zásadami a pokyny vydávanými ke zpracování údajů. Jakákoli další potřebná doplňující školení musí být ohlášena referentům pro funkci (nebo v případě jejich nepřítomnosti hlavnímu referentovi), aby tyto požadavky mohly být splněny.

11. PRAVIDELNÉ KONTROLY

Při plnění povinností vyplývajících z GDPR bude každá společnost muset zajistit pravidelné kontroly, a to i prostřednictvím vnitropodnikových referentů (hlavní referent a případně referenti pro funkci), dodržování ustanovení GDPR, místních předpisů a zásad EU Group a vydaných pokynů týkajících se zpracování údajů.
Kontroly musí být dokumentovatelné. Od pověřených osob se vyžaduje, aby při provádění kontrol spolupracovaly v maximální možné míře.

12. SANKCE

Částečné nebo úplné porušení ustanovení Zásad ochrany osobních údajů může mít za následek trestní, občanské a správní sankce za nezákonné zpracování nebo zpracování, které není v souladu s referenčními právními předpisy.
V nejzávažnějších případech si uvědomte, že správní peněžitá sankce podle čl. 83 odst. 5 GDPR může dosáhnout až 20 000 000 EUR, u společností až 4% z celkového ročního celosvětového obratu předchozího roku, pokud je vyšší.

Protiprávní jednání nebo nedodržování těchto zásad, zásad EU Group a vydaných pokynů týkajících se zpracování osobních údajů může vést k disciplinárním opatřením odpovídajícím závažnosti těchto skutečností.

*** *** ***