Opatření společnosti COMVERGA k zabezpečení ochrany Osobních Údajů

Zpracovatel (dále „**COMVERGA**“) chrání svá aktiva a informace a rozděluje je do skupin dle jejich důvěrnosti. Toto rozdělení definuje metody vytváření, ukládání, reprodukce, předávání a skartace a všichni uživatelé jsou v těchto pravidlech proškolováni.

1. Bezpečnost informací

COMVERGA zajišťuje, že přístup k informacím pokrytým těmito opatřeními mohou mít pouze osoby, které dané informace potřebují pro výkon své práce a pro účely plnění smlouvy. Informace nebudou použity pro jiné účely než plnění smlouvy, pokud právní úprava nestanoví výslovně jinak.

COMVERGA vede řízenou dokumentaci relevantních bezpečnostních opatření týkajících se zajištění ochrany osobních údajů definovaných smlouvou s Partnerem.

2. Princip oddělení povinností

COMVERGA v rámci nastavených pravidel odděluje neslučitelné povinnosti a odpovědnosti mezi vlastními zaměstnanci, aby se snížila příležitost k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv COMVERGA.

3. Záznamová povinnost

COMVERGA pořizuje a uchovává (min. 3 měsíce) logy událostí ve vlastních systémech a aplikacích zaznamenávajících aktivity uživatelů, výjimky, selhání a další události bezpečnosti informací.

4. Technická opatření

COMVERGA má v rámci své sítě implementované firewally, antiviry a systémy pro detekci a/nebo předcházení průnikům (IDS/IDP), které jsou vždy pravidelně aktualizovány, udržovány na nejlepší možné úrovni a v souladu s oborovými best-practices. Jsou přijata opatření k identifikaci neoprávněného přístupu k Osobním údajům a/nebo Informačním Systémům i ve stádiu pokusu.

5. Instalování a provozování softwaru

COMVERGA používá pouze legální software a má nastaveny postupy pro interní schvalování používaného softwaru. COMVERGA zajišťuje včasnou instalaci oprav a bezpečnostních záplat na systémech kde jsou zpracovávány informace pokrývané dle smlouvy s Partnerem s přihlédnutím k závažnosti možné zranitelnosti – pro kritické zranitelnosti v nejbližší možné době, pro vysoce závažné do 1 měsíce, pro středně závažné do 2 měsíců, pro méně závažné do 3 měsíců.

6. Testování s reálnými daty

Testování Informačních Systémů při jejich implementaci a/nebo modifikaci nepoužívá reálná (živá) data, pokud to není nezbytné. Použití reálných (živých dat) je možné pouze v případě, že neexistuje žádná jiná smysluplná alternativa. V případě, že reálná (živá) data musí být použita, je toto použití omezeno na nezbytné minimum.

7. Používání internetu a elektronických komunikačních sítí

Internet ani žádná elektronická komunikační síť nepatří mezi bezpečná média. Osobní údaje nesmí být nikdy posílány prostřednictvím internetu a/nebo elektronické komunikační sítě bez patřičného zašifrování nebo jiných opatření, které zajistí, že informace nebudou čitelné a/nebo modifikovatelné třetí stranou.

8. Veřejná uložiště

Osobní údaje nejsou za žádných okolností ukládány na veřejná úložiště, ani v zašifrované formě.

9. Malware

Veškeré soubory stažené z internetu jsou považovány za nevěrohodné a před jejich prvním užitím je ověřeno, že neobsahují viry nebo škodlivý kód.

10. Používání e-mailu

Všechny přílohy elektronické pošty jsou kontrolovány na přítomnost škodlivých kódů. Potenciálně nebezpečné přílohy pošty jsou blokovány na serverech COMVERGA. Zaměstnanci COMVERGA především nesmí:

- užívat elektronickou poštu způsobem ohrožujícím COMVERGA a/nebo Správce,
- používat poštu ke komentářům mimo COMVERGA bez toho, aby bylo zcela jasné, že jde o osobní názory, a ne stanovisko COMVERGA a Správce.

11. Přístupová oprávnění

COMVERGA zajišťuje, že do informačních systémů a k datům COMVERGA obecně, je umožněn přístup pouze osobám, které k tomu mají příslušné oprávnění a které potřebují přístup do systémů k takovým údajům a zdrojům, které jsou nezbytné pro plnění jejich povinností („**Oprávněný uživatel**“).

- Každému Oprávněnému uživateli je vydáván osobní a jedinečný identifikátor pro tyto účely („Uživatelské ID“). Uživatelské ID je ve vybraných případech doplněno vícefaktorovou autentizací.
- COMVERGA vede aktuální seznam Oprávněných uživatelů a jsou vytvořeny identifikační a ověřovací postupy pro veškeré přístupy do informačních systémů nebo pro provádění zpracování Osobních údajů.
- Pro každého jednotlivého Oprávněného uživatele nebo pro stejnorodou skupinu Oprávněných uživatelů jsou vytvořeny autorizační profily, které jsou před započetím jakékoliv aktivity Oprávněného uživatele nakonfigurovány takovým způsobem, aby byl umožněn přístup pouze k údajům a zdrojům, jež jsou potřebné k plnění jeho povinností.
- Přístup k jakýmkoliv datům COMVERGA je Oprávněným uživatelům umožněn pouze po úspěšném ověření přístupových oprávnění.
- Přístupová oprávnění jsou oprávněni přidělovat, měnit nebo odebírat pouze prověření a pověření pracovníci COMVERGA. Schvalování přístupových práv je vícestupňové.
- Přístupy do operačních systémů a databází jsou nakonfigurovány tak, aby umožňovaly přístup pouze Oprávněných Uživatelů po autorizaci.

12. Tisk

COMVERGA má nastavena pravidla (s průběžnou kontrolou jejich plnění) týkající se listinných dokumentů, včetně pravidel odebírání výtisků z tiskáren ihned po jejich vytištění tak, aby bylo zamezeno možnému přístupu nepovolaných osob k vytištěným informacím.

Po uplynutí použitelnosti vytištěných informací je zaměstnanec povinen provést skartaci, či jinak zabezpečit zničení výtisků.

13. Papírové dokumenty

Papírové dokumenty obsahující Osobní údaje mohou být předávány pouze v uzavřeném kontejneru a/nebo dvojité obálce a předány pouze do rukou Oprávněného Uživatele.

14. Zálohování dat

Zpracovávané Osobní údaje jsou v pravidelných intervalech zálohované na zabezpečená úložiště s řízeným přístupem. Obnova dat ze záloh je pravidelně testována.

15. Report incidentů

COMVERGA má stanoveny, dokumentovány a v praxi dodržovány procesy pro řízení bezpečnostní událostí a incidentů (i ve stádiu pokusu a/nebo podezření). V případě, že by se bezpečnostní incident dotýkal Osobních údajů, bude o této skutečnosti Správce neprodleně informován.