

OBSAH

1. Úvod
2. DPO, spolupráce s dozorovým úřadem
3. Datové toky, informační aktiva, osobní údaje
4. Práva subjektů osobních údajů
5. Povinnosti při zpracování osobních údajů
6. Převzetí a předávání osobních údajů třetí straně
7. Vyřizování podnětů od subjektů osobních údajů
8. Zabezpečení osobních údajů
9. Incident, postupy
10. Kontrolní mechanismy

Přílohy

1. Definice pojmů
2. Náležitosti smlouvy o zpracování OÚ (variantně VOP)
3. Deník Podnětů
4. Hlášení incidentu

1. ÚVOD

- Aqua Angels EUROPE, s.r.o., IČ 28877128, se sídlem v Praze, Na Příkopě 17 (dále jen „Společnost“) zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C vložka 150627, emailem office@aqua-angels.com, e-shopem www.aqua-angels.cz a telefonem +420 732 138 368 tímto formuluje a vydává směrnici - POLITIKA ZPRACOVÁNÍ A OCHRANY OSOBNÍCH ÚDAJŮ (dále jen „**Politika**“ nebo „**Směrnice**“).
- Záměrem vedení Společnosti je zajistit přiměřenou ochranu informačních aktiv Společnosti a zpracovávaných osobních údajů klientů dodavatelů a zaměstnanců Společnosti (dále také jen „**Subjekty údajů**“ nebo „**Subjektů OÚ**“), v souladu se zákony a jinými právními předpisy ČR i EU.
- Tato Směrnice je závazná pro všechny zaměstnance Společnosti, obchodní manažery - OSVČ spolupracující na základě smlouvy o spolupráci (dále jen „**Obchodní manažer**“ nebo „**OM**“), i pro pracovníky pracující pro Společnost na základě jiných smluv.

1.1. LEGISLATIVA

- Tato Směrnice zajišťuje soulad zpracování osobních údajů (dále také jen „**OÚ**“), s těmito právními předpisy:
 - a) Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „**GDPR**“),
 - b) Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění (dále jen „**ZOOÚ**“),
 - c) Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod,
 - d) Zákon č. 89/2012 - Nový občanský zákoník v aktuálním znění (dále jen „**NOZ**“).

1.2. CÍLE, ZODPOVĚDNOSTI

- Cílem vedení Společnosti je vytvořit takové povědomí potřeby ochrany informačních aktiv Společnosti a ochrany osobních údajů Subjektů údajů, které se stane nedílnou součástí každodenních procesů Společnosti a celkové kultury Společnosti.
- Tato Směrnice:
 - a) stanovuje cíle a rozsah ochrany osobních údajů
 - b) popisuje a vysvětluje povinnosti při zpracování osobních údajů,
 - c) stanovuje pravidla a zásady zpracování osobních údajů.
- Základní pojmy GDPR a Směrnice jsou definovány v Příloze 1. Směrnice.

2. DPO, SPOLUPRÁCE S DOZOROVÝM ÚŘADEM

2.1. DPO

- Společnost jmenovala pověřence pro ochranu osobních údajů (Data Protection Officer), (dále jen „**Pověřenec**“ nebo „**DPO**“); dpo@aqua-angels.com.
- DPO zajišťuje provádění Politiky, a řídí v rozsahu působnosti Politiky všechny vedoucí pracovníky Společnosti.
- DPO vede záznamy o činnostech zpracování OÚ, ve kterých vede veškeré podstatné záležitosti týkající se GDPR (dále jen „**Záznamy**“), minimálně však:
 - a) jméno a kontaktní údaje správce, zástupce správce a pověřence pro ochranu osobních údajů,
 - b) popis kategorií Subjektů OÚ a kategorií zpracovávaných OÚ,
 - c) účely zpracování OÚ,
 - d) doby zpracování OÚ, případně plánované lhůty pro výmaz jednotlivých kategorií OÚ,
 - e) kategorie příjemců, kterým byly nebo budou OÚ zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
 - f) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
 - g) obecný popis HW a SW infrastruktury,
 - h) popis technických a organizačních bezpečnostních opatření,
 - i) provedené změny HW a SW infrastruktury,
 - j) provedená školení,
 - k) provedené změny šifrování,
 - l) provedené testy šifrování,
 - m) provedené audity Směrnice a dalších relevantních dokumentů Společnosti.
- DPO současně s provedením změny šifrování do SW infrastruktury uloží do uzamykatelné skříně obálku s novými hesly do příslušné SW infrastruktury.

2.2. SPOLUPRÁCE S DOZOROVÝM ÚŘADEM

- Dozorovým úřadem je Úřad na ochranu osobních údajů (dále jen „**ÚOOÚ**“).
- Společnost vede Záznamy tyto Záznamy na požádání poskytne ÚOOÚ.
- S ÚOOÚ primárně jedná DPO.

3. DATOVÉ TOKY, INFORMAČNÍ AKTIVA, OSOBNÍ ÚDAJE

3.1. DATOVÉ TOKY – OBCHODNÍ ČINNOST

- Zavedení potenciálního klienta do CRM systému Obchodním manažerem.
- Zavedení klienta do ERP systému zaměstnancem.
- Objednávka klienta – e-mail, webový formulář, telefon.
- Zpracování objednávky zaměstnanci Společnosti v ERP systému.
- Vystavení dodacího listu a faktury zaměstnanci Společnosti v ERP systému.
- Vytvoření závozní sestavy zaměstnanci Společnosti a uložení v datovém úložišti NAS.
- Závoz produktů klientům zaměstnanci Společnosti.

DATOVÉ TOKY – ZAMĚSTNANCI, OM

- Přijmutí CV přes e-mail.
- Uložení CV v PC zodpovědného pracovníka Společnosti.
- Vytvoření pracovní smlouvy (HPP, DPP, smlouvy o spolupráci s OM) zodpovědným zaměstnancem Společnosti.
- Zaslání smlouvy na zpracování mezd.
- Zasílání zpracovaných mezd na měsíční bázi zodpovědnému zaměstnanci Společnosti.

3.2. INFORMAČNÍ AKTIVA

- V rámci Společnosti je prováděna klasifikace informačních aktiv, se kterými Společnost pracuje.
- Účelem klasifikace a řízení informačních aktiv je definovat a udržovat přiměřenou ochranu informačních aktiv.

- Společnost hodnotí Informační aktiva ze dvou pohledů:
 - a) potřeba utajení a ochrany informace z důvodů obchodních - obchodní tajemství,
 - b) potřeba ochrany osobních údajů.

3.3. OSOBNÍ ÚDAJE

- Osobní údaje fyzických osob, které Společnost eviduje jsou **obecné** (jméno a příjmení), a **organizační** (adresa bydliště, adresa zaměstnání, telefonní číslo, e-mailová adresa, identifikační údaje určené státem atd.,).
- Společnost nezpracovává žádné citlivé OÚ zaměstnanců, OM, ani klientů (rasový a etnický původ, politické názory, náboženské vyznání, filozofické přesvědčení, členství v odborech, sexuální orientace, genetické a biometrické údaje, údaje o zdravotním stavu).

3.3.1. OÚ klientů

- Jméno, RČ, adresa, dodací adresa, kontaktní osoba, telefon, e-mail.
- Účel - Plnění smlouvy – OÚ klientů, kterým Společnost dodává produkty; doba zpracování maximálně 3 (tři) roky od posledního nákupu produktů či služeb Společnosti, nebo maximálně 3 (tři) roky od ukončení smlouvy.
- Účel - Splnění správních povinností – OÚ klientů při evidenci účetních dokumentů; doba zpracování maximálně 11 (jedenáct) let od posledního nákupu produktů či služeb Společnosti, nebo maximálně 11 (jedenáct) let od ukončení smlouvy.
- Evidence účelu je vedena v Záznamech a v ERP Společnosti.
- Přístup k OÚ klienta mají OM, příslušní zaměstnanci Společnosti, a zaměstnanci poskytovatele ERP systému.

3.3.2. OÚ zaměstnanců

- Jméno, RČ, věk, adresa, telefon, e-mail, bankovní účet.
- Účel - Plnění smlouvy – OÚ zaměstnanců v pracovním poměru; doba zpracování maximálně 3 (tři) roky od ukončení pracovní smlouvy.
- Účel - Splnění správních povinností – OÚ zaměstnanců (mzdové listy) při evidenci účetních dokumentů; doba zpracování maximálně 45 (čtyřicet pět) let od ukončení pracovní smlouvy.
- Evidence účelu je vedena v Záznamech.
- Uložení CV uchazečů o zaměstnání v kanceláři zodpovědného zaměstnance Společnosti; doba uložení maximálně 3 (tři) roky od přijetí CV.
- Přístup k OÚ zaměstnanců mají vedoucí zaměstnanci Společnosti, a zaměstnanci poskytovatele účetních služeb.

3.3.3. OÚ OM

- Jméno, RČ, IČ, adresa, telefon, e-mail, bankovní účet.
- Účel - Plnění smlouvy – OÚ OM, se kterými má Společnost uzavřenou smlouvu o spolupráci; doba zpracování maximálně 3 (tři) roky od ukončení smlouvy.
- Účel - Splnění správních povinností – OÚ OM jako dodavatelů při evidenci účetních dokumentů; doba zpracování maximálně 11 (jedenáct) let od ukončení smlouvy.
- Evidence účelu je vedena v Záznamech.
- Přístup k OÚ obchodního manažera mají příslušní zaměstnanci Společnosti, a zaměstnanci poskytovatele ERP.

3.4. ZÁSADY ZPRACOVÁNÍ A OCHRANY OSOBNÍCH ÚDAJŮ PŘI POSKYTOVÁNÍ SLUŽEB KLIENTŮM

- Společnost zpracovává jen ty osobní údaje, které jsou pro danou službu nutné, a po nutnou dobu.
- Společnost maže OÚ zájemců, kteří se nestali klienty, a to ihned po zjištění.
- Společnost definuje ve svých veřejných dokumentech na jak dlouhou dobu, kde a jak zpracovává osobní údaje.
- Dozví-li se Společnost o změnách OÚ, bez zbytečného odkladu je aktualizuje.
- Společnost nikdy nepoužívá osobní údaje k jinému účelu, než ke splnění dodávané služby nebo k účelu, ke kterému byl získán souhlas, případně ke splnění zákonné povinnosti.

- Společnost zajišťuje, že nikdy o klientovi nerozhoduje automat, počítačový program, ani jej žádný automat neprofiluje.
- Společnost prohlašuje, že klient může kdykoli požádat o výmaz zpracovávaných osobních údajů.
- Pokud Společnost přenáší OÚ klientů, přenáší je v šifrované podobě.
- Společnost pravidelně kontroluje zabezpečení informačního systému.
- Společnost zajišťuje pravidelné školení zaměstnanců a OM v problematice zpracování a ochrany OÚ.
- Společnost uzavírá smlouvy s OM obsahující tyto zásady zpracování a ochrany OÚ klientů Společnosti.

4. **PRÁVA SUBJEKTŮ OSOBNÍCH ÚDAJŮ**

- Společnost si je vědoma práv Subjektů OÚ.
- Fyzické osoby mají ve vztahu ke svým OÚ a ke správcům těchto osobních údajů tato práva:

Článek GDPR	Právo	Komentář
12-14	Být informován	Máte právo být informováni o tom, jaká data o Vás správce nebo zpracovatel zpracovává, za jakým účelem tak činí, jak dlouho data uchovává, zda je předává dalším subjektům nebo to má v úmyslu.
15	Na přístup	Přístup ke svým údajům, získání kopie, informace o zpracování.
16	Na opravu	Právo na opravu chybných nebo neúplných údajů.
17	Na výmaz	Pominul-li účel zpracování, odvolali jste souhlas nebo je zpracování protiprávní, můžete požadovat výmaz svých osobních údajů.
18	Na omezení zpracování	Můžete požadovat omezení zpracování vašich osobních údajů po dobu řešení námítky, o zrušení omezení musíte být informováni včetně jeho důvodu.
19	Na oznámení změn nebo výmazu či omezení zpracování	Oznámení o provedení změn Vašich osobních údajů, jejich výmazu, omezení zpracování nebo jeho ukončení, o příjemcích Vašich osobních údajů.
20	Na přenositelnost	Právo získat u některých služeb data ve strukturovaném běžném nebo standardizovaném formátu.
21	Na námitku	Při oprávněném zájmu z důvodu Vaší individuální situace nebo proti profilování nebo přímému marketingu můžete vznést námitku proti zpracování. Správce musí prokázat oprávněný důvod pro tyto činnosti.
22	Nebýt předmětem automatizovaného rozhodování včetně profilování	Právo, aby o Vás nerozhodl výhradně automat. Můžete si vyžádat rozhodnutí člověka.
77	Podat stížnost	Podat stížnost u dozorového úřadu – Úřadu pro ochranu osobních údajů. https://www.uoou.cz/
79	Na účinnou soudní ochranu	Můžete se obrátit ve sporu se správcem na soud.
80	Být zastoupen neziskovým subjektem	Můžete zplnomocnit neziskový subjekt, aby Vás zastupoval ve sporu se správcem a on je povinen s ním jednat.
82	Na náhradu újmy	Správce je povinen nahradit subjektu údajů újmu, která mu vznikla.

5. POVINNOSTI PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- Společnost si je vědoma, že ať již jako správce nebo jako zpracovatel osobních údajů, je povinna zpracovávat osobní údaje v souladu se zásadami stanovenými GDPR, kterými jsou:

Zásada	Komentář
Zákonnost Korektnost Transparentnost	Osobní údaje ve vztahu k subjektům údajů musí být zpracovávány korektně a zákonným a transparentním způsobem. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu: a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů; b) 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; c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje; d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce; f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů. Zákonnost zpracování je třeba zdokumentovat a doložit.
Účelové omezení	Osobní údaje smí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Údaje, u kterých pominul účel zpracování, jsou vymazány.
Minimalizace údajů	Rozsah zpracovávaných osobních údajů musí být přiměřený, relevantní a omezený na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány.
Přesnost a aktualizace	Osobní údaje musí být pokud možno udržovány přesné a aktuální. Nepřesné a neplatné osobní údaje mají být vymazány.
Omezení uložení	Osobní údaje smí být uloženy ve formě umožňující identifikaci subjektů údajů jen po dobu, jež je nezbytná pro účely, pro které jsou zpracovávány. Po uplynutí této doby jsou vymazány. Při zpracování výhradně pro účely statistické, archivace ve veřejném zájmu a vědeckého či historického výzkumu lze údaje uložit i po delší dobu.
Integrita a důvěrnost	Osobní údaje musí být zpracovávány způsobem, který zajistí náležitě zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.

Odpovědnost (zpracovatele)	správce	Správce/Zpracovatel musí být schopen soulad s GDPR doložit.
Informační povinnost		Správce/Zpracovatel přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 (informace o zpracování) a učinil veškerá sdělení podle článků 15 až 22 (informace na základě práv subjektu údajů) a 34 (oznámení porušení zabezpečení osobních údajů) o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

6. PŘEVZETÍ A PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ TŘETÍ STRANĚ

6.1. PŘEVZETÍ OÚ OD TŘETÍ STRANY

- Jakékoli převzetí osobních údajů od třetí strany se musí dít na základě zákonného účelu, či smlouvy.
- Společnost je povinna Subjektům OÚ jejichž osobní údaje získala od třetí strany, sdělit nejpozději při první komunikaci s nimi informaci o tom, že tyto údaje má, od koho je získala, za jakým účelem, a informovat je o rozsahu prováděného zpracování osobních údajů. Výjimkou je situace, kdy Subjekt OÚ tyto informace již prokazatelně má.

6.2. PŘEDÁVÁNÍ OÚ TŘETÍ STRANĚ

- Jakékoli předání osobních údajů třetí straně se musí dít na základě zákonného účelu nebo smlouvy.
- Subjekt OÚ, jehož osobní údaje byly předány třetí straně, musí být informován o tom, že jeho osobní údaje byly předány třetí straně, nebo že k tomu při zpracování může dojít. Subjektu OÚ musí být poskytnuta nejen identifikace takové třetí strany, ale i informace o rozsahu zpracování prováděného touto třetí stranou, a o jeho účelu.
- Při předání osobních údajů v elektronické formě mezi Společností a třetí stranou je povinností Společnosti data při přenosu zašifrovat. Tj. buď jsou přenášena šifrovaným kanálem, nebo na přenosném paměťovém zařízení v zašifrované podobě. Toto ustanovení se nevztahuje na jednotlivé osobní údaje, jejichž únik neznamena pro Subjekt OÚ zvýšené riziko např. kontaktní údaje pracovníka zaslané mailem, nebo zaslání podepsaného dokumentu.
- Při předávání rozsáhlejších seznamů nebo obsahu databází je povinností Společnosti data šifrovat vždy.
- Před poskytnutím přenosného paměťového média třetí straně musí být provedena kontrola, zda neobsahuje osobní údaje nebo jiná data, která nemají být danému subjektu poskytnuta a v souladu s předchozím odstavcem, musí být data zašifrována.

6.3. SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- Společnost provádí při realizaci svých služeb zpracování osobních údajů jako zpracovatel.
- Společnost jako zpracovatel OÚ může využít třetí stranu ke zpracování OÚ jen na základě smlouvy o zpracování osobních údajů, nebo na základě přijetí všeobecných obchodních podmínek takové třetí strany, které splňují náležitosti článku 28 odst. 3 GDPR.
- Náležitosti smlouvy o zpracování osobních údajů jsou definovány v Příloze 2. Směrnice.
- Seznam aktuálně platných Smluv o zpracování OÚ je veden u DPO.

7. VYŘIZOVÁNÍ PODNĚTŮ, ŽÁDOSTÍ A STÍŽNOSTÍ OD SUBJEKTŮ OSOBNÍCH ÚDAJŮ

- Jakoukoli žádost, stížnost nebo podnět (dále jen „Podnět“) v souvislosti se zpracováním osobních údajů od jakéhokoli subjektu, je přijímající pracovník Společnosti povinen zaevidovat v deníku Podnětů (dále jen „Deník Podnětů“), viz Příloha 3. Směrnice.

- Při převzetí Podnětu je přijímající pracovník povinen řádně ověřit totožnost předkladatele Podnětu a toto ověření zdokumentovat v Deníku Podnětů. Existuje-li pochybnost o totožnosti předkladatele Podnětu, lze jej požádat o poskytnutí dodatečných informací nezbytných k potvrzení jeho totožnosti.
- Pokud je k vyřízení daného Podnětu kompetentní pracovník, který jej přijal, zaznamená zároveň postup jeho vyřízení do Deníku Podnětů, a informuje Pověřence.
- Pokud k vyřízení daného Podnětu není pracovník, který jej přijal kompetentní, předá jej k vyřízení Pověřenci a toto zaznamená do Deníku Podnětů.
- Pokud předkladatel Podnětu podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje Společnost informace v běžně používané elektronické podobě (e-mail).
- Lhůta pro vyřízení Podnětu a informování předkladatele Podnětu je maximálně 30 (třicet) dnů. Není-li to s ohledem na složitost a počet případů možné, lze lhůtu prodloužit až o 60 (šedesát) dnů, ale předkladateli Podnětu je třeba tuto skutečnost oznámit.
- Informace je na základě předloženého Podnětu poskytována předkladateli Podnětu Společností bezplatně.
- Jedná-li se o nedůvodný, nepřiměřený (zejména opakovaný) Podnět, lze Podnětu nevyhovět nebo požadovat poplatek zohledňující náklady spojené se zpracováním Podnětu a poskytnutím informace. Nedůvodnost nebo nepřiměřenost Podnětu je třeba doložit.
- Je-li Podnětem aktualizace, výmaz nebo doplnění neúplných OÚ Subjektu OÚ, je povinen příslušný pracovník Společnosti tyto údaje aktualizovat, vymazat nebo doplnit bez zbytečného odkladu. O provedení takové změny je povinen příslušný pracovník Společnosti Subjekt OÚ informovat, a to i v případě, že jeho OÚ byly aktualizovány proto, že aktuální údaje byly získány jinak než od Subjektu OÚ. Výjimkou z informační povinnosti jsou případy, kdy se to ukáže jako nemožné, nebo to vyžaduje nepřiměřené úsilí.
- Byly-li osobní údaje, jichž se změna nebo výmaz týká, předány ke zpracování třetí straně, je povinností pracovníka, který za změnu či výmaz zodpovídá, zajistit provedení téže operace u všech třetích stran, kterým byly tyto osobní údaje předány ke zpracování, a toto zpracování trvá.
- Pokud Společnost nepřijme opatření, o které předkladatel Podnětu požádal, informuje nejpozději do 30 (třiceti) dnů předkladatele Podnětu:
 - a) o důvodech nepřijetí jeho žádosti,
 - b) o možnosti podat stížnost u dozorového orgánu a žádat soudní ochranu.

8. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

8.1. VŠEOBECNÉ ZÁSADY A OPATŘENÍ

- Společnost má zpracovanou dokumentaci:
 - a) jaké OÚ jsou zpracovávány,
 - b) kde jsou OÚ uloženy,
 - c) v jaké formě jsou OÚ uloženy,
 - d) jak dlouho jsou OÚ uloženy,
 - e) o zákonných důvodech a účelech jejich zpracování.
- Veškeré OÚ jsou po pominutí účelu jejich zpracování bezpečně vymazána, nebo jsou jejich paměťové nosiče předepsaným způsobem zničeny, případně jsou fyzické dokumenty skartovány.
- Společnost uchovává informační technologie s uloženými OÚ v uzavřených prostorech přístupných omezenému počtu pracovníků.
- Informační systém, která slouží k poskytování služeb klientům je umístěna tak, aby data zde umístěná byla chráněna a udržována ve stavu dostupnosti a integrity.
- Jsou definovány procesy správy informačního systému, zálohování a archivace dat, a procesy obnovy těchto systémů. Tyto procesy a opatření jsou pravidelně testovány.
- Pravidla pro správu přístupových práv k SW infrastruktuře jsou definována, nastavena a dokumentována.
- Jsou definována opatření pro předcházení případným útokům na informační aktiva Společnosti i opatření, která v případě útoku umožní analyzovat rozsah dat, ke kterým útočník získal přístup.

- Společnost dbá na to, aby všechna výše uvedená opatření byla řádně prováděna a dokumentace odpovídala skutečnému stavu.

8.2. FYZICKÁ BEZPEČNOST

- Datové úložiště NAS je uzamčeno v kanceláři DPO, náhradní klíč má COO.
- Provozovna je umístěna v areálu „Impera park“, který je uzavřen a hlídán.
- Do provozovny mají přístup pouze zaměstnanci Společnosti pod předávacím protokolem.
- Dokumenty obsahující OÚ jsou uzamčeny v zamykatelné skříni v kanceláři DPO, náhradní klíč má COO.

8.3. OCHRANA PROTI SW ÚTOKU ZVENČÍ

Politika správy hesel

- Hesla na SW infrastrukturu jsou vytvořena zaměstnancem zodpovědným za bezpečnost Společnosti, a poskytnuta příslušným zaměstnancům po dobu jejich potřeby příslušnou SW infrastrukturu používat.
- Po ukončení zaměstnání/spolupráce OM je přístup příslušného zaměstnance k infrastruktuře ukončen a heslo smazáno.
- Hesla jsou vytvořena dle těchto základních parametrů:
 - a) Min 6-mi místní kód obsahující číslice i písmena,
 - b) bez použití jmen a příjmení osob, jejich narození a podobných jednoduše identifikovatelných parametrů.
- Hasla jsou uložena u zodpovědného zaměstnance Společnosti v za-heslovaných souborech, ve fyzické formě, uzamčené ve zamykatelné skříni.
- Hesla jsou pravidelně měněna, a v případě útoku na SW infrastrukturu neprodleně změněna.

Zabezpečení přístupu na SW infrastrukturu

- Přístup k veškeré SW infrastruktuře je přes vlastní šifrované WIFI sítě Společnosti.
- Hesla k šifrovaným WIFI sítím je zakázáno předávat komukoliv mimo Společnost.
- V sídle Společnosti i provozovně Společnosti jsou vybudovány WIFI sítě pro návštěvy „Host“.
- Je přísně zakázán přístup na SW infrastrukturu Společnosti přes veřejné WIFI sítě.

Zabezpečení PC stanic a NTB

- Na všech PC a notebookech je spuštěna aktivní ochrana Firewall.

Zabezpečení E-mailové komunikace

- E-mailová komunikace je zabezpečena antivirovým SW Avast.
- E-mailová komunikace je zabezpečena antispamovým SW v rámci outsourcovaných služeb virtuálního serveru.

8.4. OCHRANA PROTI SW ÚTOKU ZE VNITŘÍ

Správa přístupových práv

- Přístup na SW infrastrukturu s možností změny přístupových práv má pouze zodpovědný pracovník Společnosti.
- Každý zaměstnanec s přístupem na jakoukoliv SW infrastrukturu má šifrovaný vstup do svého PC, notebooku nebo telefonu – po zapnutí, po uspání, i po naskočení spořiče obrazovky
- Každý zaměstnanec s přístupem na jakoukoliv SW infrastrukturu má šifrovaný vstup do dané SW infrastruktury.

8.5. OCHRANA PROTI ZTRÁTĚ DAT

Šifrování pevných disků

- Všechna PC a notebooky ve Společnosti používají šifrování disků.
- Je tím zamezena možnost zkopírování disků v případě SW útoku i v případě fyzické ztráty zařízení.
- Tyto šifrování disků jsou používána ve Společnosti:
 - a) BIT Locker pro systém Windows,
 - b) FileVault pro systém Apple.

Zálohování a obnova

- Datové úložiště NAS je zálohováno jedenkrát týdně; záloha je geograficky oddělená.
- PC a notebooky zaměstnanců provozu, KS a výroby neukládají žádná data a procují pouze ze SW infrastrukturou
- PC a NTB OM jsou zálohovány jedenkrát měsíčně; záloha je geograficky oddělená,
- ERP Premier je zálohován poskytovatelem denně.
- CRM Raynet je zálohován poskytovatelem denně.
- Emailová komunikace je zálohována na virtuální serveru poskytovatelem jednou za 3 (tři) týdny.

8.6. OCHRANA DAT NA MOBILNÍCH ZAŘÍZENÍCH

- Notebooky jsou chráněny šifrovaným vstupem do zařízení, šifrovaným vstupem do SW infrastruktury, a šifrováním disku.
- Telefony jsou chráněny šifrovaným vstupem do zařízení, který je vyžadován při každém obnovení činnosti, a šifrováním SIM karty.
- Na telefonech jsou nastaveny funkce pro případ ztráty či odcizení:
 - a) najdi telefon,
 - b) zablokovat,
 - c) vymaž telefon.
- Hesla SIM karet telefonu jsou uložena v uzamykatelné skříni v uzamčené kanceláři DPO.

8.7. OCHRANA DAT PŘI PŘENOSU, PŘEDÁVÁNÍ

- Předávání OÚ třetí straně je prováděno v zipovaném souboru s heslem; heslo je zasláno jiným kanálem než OÚ.
- Společnost nepředává žádné OÚ třetí straně, s výjimkou podkladů pro zpracovaných mezd.
- Za provádění tohoto opatření je zodpovědný pracovník Společnosti.

8.8. PRAVIDELNÉ TESTOVÁNÍ A VYHODNOCOVÁNÍ MÍRY ZABEZPEČENÍ

- Pro snížení možnosti výskytu incidentů Společnost využívá:
 - a) fyzické zabezpečení,
 - b) šifrování vstupu do zařízení,
 - c) šifrování disků,
 - d) antivirové zabezpečení,
 - e) antispamové zabezpečení,
 - f) šifrování přístupu na interní WIFI síť,
 - g) lokální firewaly.
- Jednou za 6 (šest) měsíců je změněno šifrování přístupu na WIFI síť Společnosti.
- Jednou za 12 (dvanáct) měsíců je změněno šifrování přístupu do interní SW infrastruktury Společnosti – NAS.
- Jednou za 12 (dvanáct) měsíců je změněno šifrování přístupu do externí SW infrastruktury Společnosti – E-mail, ERP, CRM.
- Kontrola funkčnosti šifrování všech přístupů je prováděna pravidelně jednou za 3 (tři) měsíce.
- O všech těchto změnách a kontrolách provede DPO záznam do Záznamu.

9. INCIDENT, POSTUPY

- Incident – jakákoliv situace kdy hrozí zveřejnění, ztráta, či zneužití OÚ klientů, dodavatelů a zaměstnanců.

9.1. REAKCE NA INCIDENT

- Zaměstnanci a obchodní manažeři Společnosti mají povinnost hlásit každý incident DPO na dpo@aqua-angels.com.
- Všichni zaměstnanci a OM jsou v případě incidentu povinni spolupracovat na určení rozsahu případných škod a na poskytnutí informací pro popis toho, co se stalo a pro odhad dopadu na Subjekty OÚ.
- Na základě těchto informací vyhodnotí DPO do 72 (sedmdesáti dvou) hodin od okamžiku zjištění incidentu, zda je třeba incident hlásit dozorovému úřadu a popřípadě i Subjektům OÚ. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

- Pokud ano, informuje UOOU, případně i Subjekt OÚ.
- Hlášení dozorovému úřadu není nutné, jestliže je nepravděpodobné, že by incident měl za následek riziko pro práva a svobody fyzických osob.
- DPO provede záznam o incidentu, jeho vyhodnocení a způsob řešení v deníku incidentů (dále jen „**Deník incidentů**“), viz Příloha 4 Směrnice.
- DPO rozhodne i o případných nápravných opatřeních.

10. **KONTROLNÍ MECHANISMY**

- Společnost sleduje relevantní změny legislativy.
- Při každé změně legislativy či zavedení nových technologií je provedeno přezkoumání dokumentace a procesů, které mohou být takovouto změnou dotčeny.
- Tato Směrnice podléhá revizi minimálně jedenkrát ročně a vždy, když dojde ke změně legislativy, na které je založena; za provedení revize je zodpovědný DPO.
- Všichni zaměstnanci a Obchodní manažeři Společnosti jsou pravidelně školeni a seznamováni s aktuálními povinnostmi stanovenými legislativou a interními předpisy vztahujícími se na činnosti, při nichž dochází nebo může docházet ke zpracování OÚ.