| | |
|---|---|
| **Název:** | **NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI (GDPR) – VE SPOLEČNOSTI SNP INVEST, INVESTIČNÍ FOND, A.S.**<br>*V souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů* |
| **Číslo vnitřního předpisu:** | **13** |
| **Přílohy:** | Příloha č.1 – Obecné zásady IT bezpečnosti<br>Příloha č.2 - Formulář pro hlášení porušení zabezpečení osobních údajů |
| **Určena:** | Všem pracovníkům Fondu |
| **Pracovník / útvar odpovědný za vytvoření a aktualizaci:** | Pracovník compliance |
| **Pracovník / útvar odpovědný za schválení** | Představenstvo |
| **Účinnost od:** | 21.12.2023 |

# OBSAH

## 1. ÚČEL DOKUMENTU

Tato směrnice upravuje zpracování osobních údajů ve společnosti SNP INVEST, investiční fond, a.s., IČ: 21049939, se sídlem Praha 1, Václavské náměstí 772/2, PSČ 110 00, (dále jen "**Společnost**") v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**" nebo „**Nařízení**").

Účelem této směrnice je zajistit dodržování povinností vyplývajících z Nařízení ve Společnosti a umožnit subjektům údajů výkon jejich práv.

## 2. POUŽITÉ POJMY

Pojmy použité v této směrnici mají následující význam:

- „**osobní údaj**" veškeré informace o identifikované nebo identifikovatelné fyzické osobě, tj. osobě, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. 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);
- „**zvláštní kategorie osobních údajů**" osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;
- „**zpracování**" jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
- „**omezení zpracování**" označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
- „**správce**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
- „**zpracovatel**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;
- „**příjemce**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují;
- „**třetí strana**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;
- „**souhlas**" subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

- „**porušení zabezpečení osobních údajů**“ jakékoliv porušení důvěrnosti, dostupnosti či integrity osobních údajů, tedy porušení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
- „**dozorový úřad**“ Úřad pro ochranu osobních údajů České republiky;
- „**likvidace**“ osobních údajů znamená fyzické zničení jejich nosiče nebo jejich vymazání.

## 3. ROLE A ODPOVĚDNOSTI

### 3.1. Pracovníci

Každý pracovník Společnosti odpovídá za to, že zpracování osobních údajů provádí v souladu s právními předpisy a tímto interním předpisem a dalšími předpisy a dokumenty Společnosti.

## 4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

### 4.1. Obecné zásady zpracování osobních údajů

Při zpracování osobních údajů ve Společnosti je nezbytné dodržovat následující zásady:

- **zákonnost, korektnost a transparentnost**
  - ve vztahu k subjektu údajů musí být osobní údaje zpracovávány korektně, zákonným a transparentním způsobem;
- **účelové omezení**
  - osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
- **minimalizace údajů**
  - zpracování musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou osobní údaje zpracovávány;
- **přesnost**
  - osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;
- **omezení uložení**
  - osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány;
- **integrita a důvěrnost**
  - osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením;

## 5. OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Systém ochrany osobních údajů je tvořen komplexem organizačních a technických opatření, která jsou ve Společnosti realizována za účelem zabezpečení ochrany a bezpečnosti osobních údajů.

### 5.1. Fyzická bezpečnost

#### *5.1.1. Pracovníci*

Každý pracovník je povinen zajistit ochranu pracovní stanice tak, aby nemohlo dojít k jejímu zneužití jiným pracovníkem, případně cizí neoprávněnou osobou.

Tato povinnost zahrnuje:

- Zamknutí/zakódování dveří kdykoli při odchodu z kanceláře (pokud je v kanceláři sám nebo pokud odchází jako poslední)
- Neponechávat klíče v zámku kanceláře
- Dodržování pravidla čistého stolu, tzn. neponechávat v době své nepřítomnosti na pracovním stole volně položené dokumenty klasifikované jako neveřejné a aktivování funkce uzamknout stanici (WINDOWS + L), při odchodu z místnosti
- Odpovědnost za návštěvu po dobu jejího pobytu, návštěva nesmí zůstat bez dozoru
- V případě, že pracovník opouští pracovní místo a v místnosti se nenacházejí žádné další osoby, je povinen zkontrolovat uzavření oken a uzamknout místnost
- Všechny dokumenty obsahující osobní údaje musejí být při opuštění pracoviště v uzamčených skříních.

#### *5.1.2. Sídlo Společnosti*

Budova, v níž se nacházejí kanceláře Společnosti je vybavena recepcí a ostrahou, která je přítomna 24/7. Přístup k výtahům je možný na kartu, následně je pro vstup do prostor Společnosti (do části sdílené s dalším nájemníkem) pouze pomocí karty.

Přímo od kanceláří Společnosti má každý z pracovníků vlastní klíč, který je vydáván na základě předávacího protokolu. Na jednotlivých odděleních jsou uzamykatelné skříně, v nichž jsou uloženy dokumenty citlivé a obsahující osobní údaje.

Technická místnost, v níž jsou umístěné aktivní prvky informačních technologií je uzamykatelná s omezeným přístupem pro předem definovaný seznam osob. Jednotlivé vstupy do technické místnosti jsou zaznamenány v dokumentu s názvem „Protokol o přístupu do serverovny“.

### 5.2. IT bezpečnost

- Viz. příloha č.1 této směrnice – Obecné zásady IT bezpečnosti

### 5.3. Postup při vzniku incidentu

Každý pracovník Společnosti je povinen hlásit veškerá porušení zabezpečení osobních údajů nebo potenciální porušení, a to neprodleně poté, co se o něm dozví. Ohlášení se provede prostřednictvím vyplnění formuláře, který je přílohou této směrnice jako její příloha č. 2. Vyplněný formulář je nutné zaslat na email: pavel.makovec@snpinvest.cz.

GDPR požaduje, aby bylo porušení zabezpečení osobních údajů, je-li to možné, nahlášeno dozorovému úřadu do 72 hodin od okamžiku, kdy se správce údajů o porušení zabezpečení dozvěděl. Okamžik, kdy se správce o porušení zabezpečení dozvěděl dozorový úřad posuzuje objektivně, tj. jako okamžik, kdy se nejdříve dozvědět měl a mohl.

Uvedené ohlášení není nutné činit pouze v případě, že je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Jedná se obecně o situace, kdy je nepravděpodobné, že porušení zabezpečení osobních údajů bude mít pro subjekty údajů za následek fyzickou, hmotnou či nehmotnou újmu.

Oznámení dozorovému úřadu musí obsahovat alespoň:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů (DPO), je-li ustanoven;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Bezprostředně po interním zjištění či nahlášení možného porušení zabezpečení osobních údajů, je nutné provést kroky k:

- identifikaci možného porušení zabezpečení osobních údajů a vyhodnocení, zda se skutečně jedná o porušení zabezpečení osobních údajů;
- posouzení rizika a vyhodnocení, zda není riziko natolik nízké, že nevznikne povinnost událost ohlašovat jako porušení zabezpečení osobních údajů;
- získání všech nezbytných údajů pro řádné hlášení dozorovému úřadu, a
- zvládnutí případu porušení a odstranění jeho následků.

Jakmile dojde k provedení shora uvedených kroků a posouzení, že událost je nutno hlásit dozorovému úřadu, je statutární orgán povinen podat řádné hlášení dozorovému úřadu se všemi předepsanými náležitostmi a připojit své kontaktní údaje.

Společnost následně provede šetření bezpečnostního incidentu s tím, že vedení Společnosti zajistí, že jsou pro šetření k dispozici adekvátní zdroje (zejména příslušní odborní pracovníci, např. z IT, bezpečnosti) a určí, co je možné udělat k nápravě ztrát a omezení škod, které může únik způsobit.

Shora uvedené povinnosti oznámit případ porušení zabezpečení osobních údajů dozorovému úřadu se vztahují na Společnost, pokud je v pozici správce osobních údajů. Vystupuje-li Společnost jako zpracovatel, má toliko povinnost bezodkladně informovat správce o případu možného porušení zabezpečení osobních údajů.

GDPR stanoví, že pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, správci údajů musí toto porušení bez zbytečného odkladu ohlásit subjektům údajů. Určujícím hlediskem pro stanovení stupně rizikovosti je míra pravděpodobnosti a závažnosti takového rizika pro práva

a svobody subjektu údajů. Pravděpodobnost a závažnost rizika by se měly určovat na základě povahy, rozsahu, kontextu a účelům zpracování (např. odcizení klientské databáze v nezašifrované podobě, obsahující identifikační údaje, rodné číslo, číslo účtu, přístupové údaje, uživatelské jméno, zákaznické číslo, zdravotní stav, přičemž cílem zcizení databáze bylo zneužití osobních údajů, je nutné považovat za vysoce rizikové).

Za předpokladu, že dojde k naplnění povinnosti informovat subjekty údajů, jak je shora popsáno, zajistí vedení Společnosti, aby byly subjekty údajů dotčené porušením zabezpečení osobních údajů bezodkladně informovány, a to v rozsahu vyžadovaném GDPR.

Po jakémkoli porušení zabezpečení osobních údajů následuje důkladné vyhodnocení incidentu. Účelem je vyhodnotit, zda kroky učiněné během incidentu byly správné, a určit oblasti, které je možné zlepšit.

### 5.4. Kontrolní činnost

Pravidelně, minimálně 1x ročně, nebo v případě výskytu závažného incidentu je prováděn interní audit se zaměřením na dodržování pravidel stanovených touto směrnicí. Audit provádí statutární orgán Společnosti nebo jím určená osoba a je o něm pořizována písemná zpráva zachycující výsledky auditu.

### 5.5. Školení zaměstnanců

Pravidelně, minimálně 1x ročně, nebo v případě výskytu závažného incidentu je prováděno školení všech pracovníků Společnosti se zaměřením na dodržování pravidel stanovených touto směrnicí. Školení je realizováno elektronickou formou nebo osobně. O školení jsou vedeny záznamy.

### 5.6. Pravidelná revize a aktualizace interních předpisů

Tento interní předpis je revidován pravidelně 1x krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve Společnosti s možným dopadem na ochranu osobních údajů nebo v případě narušení zabezpečení ochrany osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá statutární orgán.

### 5.7. Vedení a aktualizace záznamů o činnostech zpracování

Záznamy o činnostech zpracování jsou součástí pravidelné revize a aktualizace interních předpisů. Revize kompletnosti a přesnosti katalogu zpracování je prováděna pravidelně 1x krát ročně. Ad hoc revize je prováděna zejména v případě výraznějších změn ve Společnosti s možným dopadem na ochranu osobních údajů. O provedení revize a aktualizace je vedena evidence. Za revizi a aktualizaci odpovídá statutární orgán.

### 5.8. Zpracovatelské vztahy

Ve všech případech, kdy Společnost využívá zpracovatele a stejně tak v případech, kdy je Společnost v pozici zpracovatele je uzavřena písemná smlouva o zpracování osobních údajů v souladu s čl. 28 Nařízení.

### 5.9. Předávání osobních údajů do třetích zemí

Při předávání osobních údajů do třetích zemí postupuje Společnost v souladu s kapitolou V. GDPR.

## 6. VÝKON PRÁV SUBJEKTŮ ÚDAJŮ

Všechny požadavky subjektů údajů musí být vyřízeny bez zbytečného odkladu, nikdy ne později než do 1 měsíce ode dne jejich obdržení.

Pokud není možné dodržet lhůtu, vedení Společnosti pak stanoví, jak postupovat dále.

Všichni pracovníci Společnosti jsou povinni poskytnout součinnost při vyřizování žádostí subjektů údajů.

Všechny systémy Společnosti jsou nastaveny tak, aby bylo možné vyhovět žádostem subjektů údajů.

### 6.1. Poskytování informací

Společnost poskytuje subjektům údajů informace v souladu s článkem 13 a 14 GDPR, a to v požadovaném rozsahu, čímž zajišťuje transparentnost zpracování.

### 6.2. Právo subjektů údajů na přístup k osobním údajům

V případě, že o to subjekt údajů požádá, společnost poskytne subjektu údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, umožní subjektům údajů získat přístup k těmto osobním údajům a k informacím způsobem a v rozsahu dle článku 15 GDPR.

### 6.3. Právo na opravu

V případě, že o to subjekt údajů požádá, případně se o nepřesných osobních údajích dozví Společnost jinak, opraví bez zbytečného odkladu nepřesné osobní údaje. V případě, kdy si to účel zpracování vyžaduje, zajistí Společnost doplnění neúplných osobních údajů dle článku 16 GDPR.

### 6.4. Právo na výmaz

V případě, že je dán jeden z následujících důvodů, zajistí Společnost na základě uplatnění práva subjektem údajů bez zbytečného odkladu výmaz osobních údajů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
b) subjekt údajů odvolá souhlas, na jehož základě byly osobních údaje zpracovávány, a neexistuje žádný další právní důvod pro zpracování;
c) subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být vymazány ke splnění právní povinnosti, která se na Společnost vztahuje;
f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační Společnosti podle čl. 8 odst. 1 GDPR.

### 6.5. Právo na omezení zpracování

V případě, že je dán jeden z následujících důvodů, zajistí Společnost omezení zpracování osobních údajů:

a) subjekt údajů popírá přesnost osobních údajů;
b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
c) Společnost již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
d) subjekt údajů vznesl námitku proti zpracování.

### 6.6. Právo na přenositelnost údajů

V případě, že o to subjekt údajů požádá a zároveň je zpracování založeno na souhlasu nebo smlouvě, a zároveň se zpracování provádí automatizovaně, umožní Společnost subjektu údajů výkon práva na přenositelnost. Osobní údaje, které subjekt údajů Společnosti poskytl a které se ho týkají, poskytne společnost ve strukturovaném, běžně používaném a strojově čitelném formátu. Součástí tohoto práva je zajištění možnosti přenesení předmětných osobních údajů k jinému správci dle požadavku subjektu údajů.

## 7. ARCHIVACE A LIKVIDACE OSOBNÍCH ÚDAJŮ

Společnost provádí likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovávány, případně na základě žádosti subjektu.

Konkrétní lhůty pro likvidaci osobních údajů jsou stanoveny v jednotlivých záznamech o činnostech zpracování.

Při likvidaci jsou dodržovány zákonné výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

Veškeré listinné dokumenty likvidovány výhradně skartací a to svépomocí, nebo využitím externí společnosti. Data uchovávána v elektronické podobě jsou likvidována tak, aby nebylo možné jejich obnovení. V případě konce životnost jednotlivých elektronických zařízení jsou tato mechanicky likvidována tak, aby nebylo možné data obnovit.

Společnost využívá archiv, která je umístěn v prostoru kanceláře Společnosti. Přístup do prostor je zajištěn zámkem. Přístup do prostor spisovny mají pouze oprávnění pracovníci Společnosti.

## 8. ZÁVĚREČNÁ USTANOVENÍ

Za dodržování pravidel stanovených touto směrnicí odpovídají všichni pracovníci Společnosti.

**PŘÍLOHA Č.1**

**OBECNÉ ZÁSADY IT BEZPEČNOSTI**

## 1. ÚVOD

a) Správu informačních technologií vykonává společnost Necrosoft s.r.o., (dále jen „Necrosoft“) se sídlem Praha 3 – Žižkov, Roháčova 188/37, PSČ: 130 00, vedená u Městského soudu v Praze, oddíl C, vložka 92560, IČ: 26770539. Necrosoft poskytuje služby v oblasti správy elektronické pošty a správy a údržby serverů a webhostingu (zejména aktualizace, úpravy a opravy). Jako cloudové úložiště využívá služeb datového centra DC Tower Českých radiokomunikací a.s., se sídlem Praha 6 – Břevnov, Skokanská 2117/1, PSČ: 169 00, vedená u Městského soudu v Praze, oddíl B, vložka 16505, IČ: 24738875.

b) Procesu definování a autorizace uživatelů se vždy účastní nadřízený, který písemně definuje práva k síťovým složkám a přístupová práva. Toto nastavení pak zašle e-mailem Necrosoftu, která provede vlastní nastavení uživatele.

c) Všichni zaměstnanci odpovídají za IT zařízení, jsou povinni chránit majetek Společnosti, včetně informací. Není povoleno přemisťovat jakékoli zařízení z jeho původního místa bez písemného souhlasu nadřízeného.

d) Veškeré IT zařízení musí být používáno pouze k účelům souvisejícím s předmětem činnosti společnosti.

e) Zaměstnanci musí používat síť Společnosti a její data v souladu s obecně respektovanými zásadami etiky a morálky.

f) Zaměstnanci nesmí poskytovat data třetím osobám nebo rodinným příslušníkům.

g) Před odchodem z pracoviště musí každý zaměstnanec zkontrolovat, zda jsou všechna IT zařízení vypnuta a není umožněn neautorizovaný přístup.

h) Přístup k datům mají pouze zaměstnanci, kteří s těmito údaji pracují. Tato data jsou uložena na síťových discích, ke kterým mají přístup pouze oprávnění zaměstnanci.

i) Přístup ke sdíleným složkám je revidován a aktualizován každých šest měsíců.

## 2. ZÁSADY POUŽÍVÁNÍ FIREMNÍ ELEKTRONICKÉ POŠTY

a) Firemní elektronická pošta (dále také jako „e-mail“) Společnosti je přidělena každému zaměstnanci a je používána v souladu s pracovní náplní.

b) **Nevhodné používání firemní elektronické pošty**

- přihlašování se na nelegální, nespolehlivé, pochybné nebo podezřelé webové stránky a služby;
- posílání nevhodného obsahu nebo nevhodných reklamních e-mailů;
- posílání urážlivých nebo diskriminačních zpráv a obsahu;
- záměrné rozesílání nevyžádané pošty jiným osobám, včetně svých spolupracovníků;
- používání e-mailu pro soukromé účely.

c) **Vhodné používání firemní elektronické pošty**
Zaměstnanci mohou používat firemní e-mail pro pracovní účely bez omezení, avšak vždy v souladu s jejich pracovním zařazením a pracovní náplní.

d) **Zabezpečení firemní elektronické pošty**
E-mail je často prostředkem hackerských útoků, narušení důvěrnosti, virů a dalšího škodlivého softwaru. Tyto problémy mohou ohrozit naši pověst, legalitu a bezpečnost našeho zařízení.

**Zaměstnanci musí:**

- volit silná hesla s nejméně osmi znaky (velká a malá písmena, symboly a číslice) bez použití osobních údajů (např. data narození) – Nastaveno pomoci GPO politiky v Active Directory;
- hesla si pamatovat, nezapisovat a držet v tajnosti;
- každých 90 dní měnit své e-mailové heslo – Nastaveno pomoci GPO politiky v Active Directory;
- při používání e-mailu být vždy ostražití, aby zachytili e-maily, které obsahují malware nebo pokusy o phishing; Emailový server využívá svůj vlastní firewall i anti pishing, malware server, který eliminuje tyto útoky.
- vyvarovat se otevírání příloh a klikání na odkazy, pokud není obsah dostatečně vysvětlen (např. "Podívejte se na toto video, je úžasné.");
- být obezřetní vůči clickbaitovým titulkům;
- kontrolovat e-maily a jména neznámých odesílatelů, aby se ujistili, že jsou legitimní;
- hledat nesrovnalosti v obsahu (např. gramatické chyby, velká písmena, nadměrný počet vykřičníků);
- počítače v lokální síti jsou udržovány vlastním WSUS serverem, který pomocí GPO politiky udržuje PC aktualizované;
- v případě podezření na ohrožení bezpečnosti neprodleně kontaktovat Necrosoft a svého nadřízeného.

e) **Podpis firemní elektronické pošty**
Zaměstnanci mohou využívat jednotný e-mailový podpis, který definuje Společnost a je přidělen při zřízení emailové adresy.

## 3. SOCIÁLNÍ SÍTĚ

Zaměstnanci mohou používat sociální sítě pouze v případě, že je to nezbytné pro výkon jejich práce a se schválením přímého nadřízeného.

Je přísně zakázáno používat jakoukoli sociální síť k jakémukoli jinému účelu a za jakýchkoli jiných okolností, než je uvedeno výše.

## 4. ZASÍLÁNÍ OKAMŽITÝCH ZPRÁV

Zaměstnanci mohou používat pouze dvě následující služby pro zasílání okamžitých zpráv:

- Skype
- WhatsApp

## 5. FYZICKÝ PŘÍSTUP

a) Přístup do sídla Společnosti je možný pouze prostřednictvím bezpečnostních čipů.
b) Tento čip je osobní a nesmí být zapůjčen jiné osobě.
c) Pokud dojde k ukončení pracovního poměru zaměstnance, musí být čip vrácen neprodleně v poslední den jeho působení v zaměstnání.
d) Návštěvníci nesmí bez povolení vstupovat do prostor Společnosti. Návštěva může vstoupit do nejbližší zasedací místnosti pod dohledem zaměstnance.

## 6. POUŽÍVÁNÍ SYSTÉMU

a) Informační systém, podnikové sítě a terminály jsou majetkem společnosti.
b) Každý zaměstnanec musí být proškolen v používání informačního systému.
c) V rámci zabezpečení a údržby sítě mají pověření zaměstnanci právo kontrolovat zařízení, systémy, pracovní stanice a notebooky v reálném čase.
d) Zaměstnanec není povoleno měnit nastavení FW nebo nastavení PC. Vše je hlídáno pomocí GPO politiky AD a přístupových práv.
e) Zaměstnanci jsou povinni používat výhradně software schválený Společností. Pokud je vyžadován speciální software, žadatel si jej musí vyžádat u přímého nadřízeného, který kontaktuje Necrosoft a ten, posléze nainstaluje daný software do PC uživatele.
f) Zaměstnanci jsou povinni na konci každého pracovního dne vypnout pracovní stanici.
g) Zaměstnanci nesmí ničit části počítače, lepit nálepky na monitory ani jinak poškozovat zařízení.
h) Zaměstnanci nesmí používat ani instalovat modemy, externí hardware, PDA, chytré telefony, jednotky USB atd. pokud jim to nepovolí jejich nadřízený.
i) Zaměstnanci nesmí svévolně instalovat programy, viry, makra, applety, ovládací prvky ActiveX nebo jiný software/zařízení.

## 7. ZABEZPEČENÍ DAT

a) Zabezpečení dat zajišťuje Necrosoft.
b) Zdrojová data jsou uložena na souborovém serveru, všechna ostatní data jsou uložena na SQL serveru.

## 8. HESLA

a) **Tvorba hesel**
Každý zaměstnanec musí používat silná hesla s minimálním standardem:
- Jedinečnost: je striktně zakázáno sdílet hesla nebo pověření.
- Délka: Minimálně osm znaků.
- Heslo nesmí obsahovat jméno zaměstnance účtu nebo část jména zaměstnance sestávající se z více než dvou po sobě jdoucích znaků.
- Musí obsahovat alespoň jeden (1) znak ze tří následujících kategorií:

- Velká písmena anglické abecedy (A až Z), malá písmena anglické abecedy (a až z),
- 10 základních číslic (0 až 9),
- ostatní nealfanumerické znaky (např. !, $, #, %).

b) **Ochrana hesel**
Následující pokyny musí být vždy dodržovány:

- Hesla nesmí být nikomu prozrazena.
- Hesla se nesmí zobrazovat na obrazovce ve formě čitelného textu.
- V žádném případě se nesmí používat funkce "zapamatovat si heslo".
- Hesla se nesmí zapisovat ani ukládat na místech, kde by mohla být odcizena.
- Hesla nesmí být uložena v počítačovém systému bez šifrování.
- V hesle nesmí být použita žádná část uživatelského jména.
- Stejné heslo nesmí být použito pro přístup do různých systémů Společnosti.
- Stejné heslo se nesmí používat pro systémy v rámci práce i mimo ni.

V případě tří po sobě jdoucích neúspěšných pokusů o připojení k systému bude ID zaměstnance a související heslo zablokováno.

c) **Změna hesel**
Všechna hesla na uživatelské úrovni je třeba měnit minimálně jednou za 90 dní nebo kdykoli systém vyzve k jejich změně. Výchozí hesla musí být změněna okamžitě. Pokud zaměstnanec zjistí nebo má podezření na prozrazení hesla, musí jej neprodleně změnit a tuto skutečnost nahlásit nadřízenému a Necrosoftu. Zaměstnanci nesmí v rámci 5 změn hesla použít stejné heslo opakovaně.

## 9. DŮVĚRNOST INFORMACÍ

a) Soubory obsahující data nesmí být nikdy uloženy na lokálním disku počítače, ale na síťovém disku. Data na lokálních discích nejsou zálohována.
b) E-mailová korespondence se automaticky ukládá na e-mailový server, aby se předešlo riziku ztráty dat v důsledku poškození, krádeže nebo zničení počítače.
c) Porty USB jsou standardně blokovány pro všechny zaměstnance. Necrosoft povolí USB porty pouze těm zaměstnancům, kteří je potřebují ke své práci, a to s předchozím souhlasem jejich nadřízeného.

d) Pracovní stanice a notebooky zaměstnanců neobsahují hardware pro zápis na disky CD, DVD, Blu-Ray, pokud k tomu konkrétní zaměstnanec nemá písemné povolení nadřízeného.
e) Software je aktualizován automaticky a zaměstnanci nemají právo tyto aktualizace měnit nebo deaktivovat (zabezpečení Windows atd.).
f) Všichni zaměstnanci musí být velmi obezřetní při přijímání příloh z neznámých zdrojů. Zaměstnanci jsou povinni upozornit IT podporu na jakýkoli podezřelý obsah.
g) Pokud je e-mailem zasílán soubor chráněný heslem, nesmí být heslo v e-mailu obsaženo.

h) Zaměstnanci se nesmí pokoušet číst, mazat nebo jakkoli upravovat e-maily svých kolegů, nadřízených nebo podřízených bez jejich souhlasu.
i) Zaměstnanci nesmí zasílat pyramidové nebo řetězové zprávy.
j) Zaměstnanci odpovídají za škody způsobené nebezpečnými přílohami otevřenými z e-mailů, zejména za poškození firemního hardwaru a softwaru.

## 10. PŘÍSTUP K INTERNETU

Přístup na internet je možný prostřednictvím serveru WebProxy, který jasně definuje, kteří zaměstnanci a v jakém čase mají oprávnění k přístupu na internet. O nastavení pro konkrétní zaměstnance rozhoduje nadřízený.

## 11. TECHNICKÉ PROBLÉMY

Všichni zaměstnanci jsou povinni ohlásit jakékoliv technické problémy neprodleně Necrosoftu a svému přímému nadřízenému.

**PŘÍLOHA Č.2**

**Formulář pro hlášení porušení zabezpečení osobních údajů**

| **Identifikace ohlašovatele** | |
|---|---|
| **Jméno a příjmení** | |
| **Emailová adresa** | |
| **Telefonní číslo** | |
| **Poznámka**<br>*V případě, že máte o incidentu připravené elektronické zápisy, přílohy či další soubory, zde prosím uveďte jejich počet, název a krátký popis. Soubory nepřikládejte, budou vyžádány zvlášť.* | |
| **Hlášení - povinné informace** | |
| **Popis situace**<br>*Uveďte, co zapříčinilo bezpečnostní incident* | |
| **Stav řešení incidentu** *(vyberte možnost ze seznamu)* | □ K porušení zabezpečení již nedochází. Incident byl kompletně vyřešen.<br>□ K porušení zabezpečení již nedochází. Incident nebyl ještě kompletně vyřešen.<br>□ Bezpečnostní incident stále probíhá.<br>□ Nedovedu rozhodnout. |

| | |
|---|---|
| **Počet zasažených subjektů údajů** | |
| **Kategorie subjektů údajů zasažených bezpečnostním incidentem** | □ zaměstnanci SNP INVEST, investiční fond, a.s.<br>□ klienti SNP INVEST, investiční fond, a.s.<br>□ jiné subjekty údajů, specifikujte<br>…… |
| **Popis pravděpodobných důsledků bezpečnostního incidentu**<br><br>*Popište, jaké důsledky by bezpečnostní incident mohl mít na zasažené subjekty údajů, zejména z hlediska způsobení fyzické, hmotné či nehmotné újmy.* | |
| **Nápravná opatření**<br><br>*Uveďte, jaké kroky jste podnikli, aby se situace již nikdy neopakovala. Stav řešení incidentu je pouze indikací současného stavu incidentu.* | |