PIRÁTSKÁ STRANA

Smlouva o zachování důvěrnosti informací (NDA)

Česká pirátská strana, se sídlem: Na Moráni 360/3, 128 00 Praha 2, e-mail: info@pirati.cz
zastoupena Radkem Holomčíkem (dále též jen **„Poskytovatel"**)

a

Jméno osoby: **Matěj Kubíček**, datum narození: , bydliště:

(dále též jen **„Příjemce"**)

(Poskytovatel a Příjemce jsou dále uvedeni společně také jako **„Smluvní strany"**.)

1. Úvodní ustanovení

1.1. Příjemce vykonává pro Poskytovatele činnost, při které je potřebné nakládat s Důvěrnými informacemi – je členem či spolupracovníkem týmu SF. Cílem této smlouvy je naplnit zájem Poskytovatele na zajištění vysokého standardu ochrany soukromých dat a dalších Důvěrných informací.

1.2. Pro účely Smlouvy budou **„Důvěrné informace"** znamenat (není-li v článku 2.2 níže uvedeno jinak) neveřejné údaje sdělené na jednání týmu, např. informace o soukromí osob pracujících pro Poskytovatele, telefonní čísla a jiné chráněné osobní údaje, identifikace whistleblowerů, přístupové údaje, hesla a jiné informace používané ke správě zařízení, záznamy, zápisy a jiné informace z uzavřených jednání, tajné úkoly, strategie, e-maily, cizí soukromé zprávy a jiné osobní informace ostatních uživatelů uložené na spravovaném zařízení a jiné informace, které jsou jako důvěrné Poskytovatelem označeny nebo o kterých lze i bez označení předpokládat, že na jejich utajení má Poskytovatel zájem.

1.3. Za důvěrné není nutné informace výslovně označovat. Za Důvěrné informace je nutné považovat i veškeré úpravy, které na základě výše uvedeného Příjemce připraví či vytvoří nebo k nimž má přístup.

1.4. Informace přestává být důvěrná jejím oprávněným zveřejněním.

2. Práva a povinnosti

2.1. Příjemce se zavazuje, že:

2.1.1. bude nakládat s Důvěrnými informacemi poctivým způsobem, v souladu s účelem této Smlouvy tak, aby při nakládání s Důvěrnými informacemi byla zajištěna jejich ochrana a šetřeny práva a zájmy Poskytovatele;

2.1.2. používat bezpečnostní opatření, které jsou obvyklá při ukládání a přenášení Důvěrných informací, zejména používat zabezpečené komunikační aplikace (např. Signal), zabezpečené připojení a dvoufázové ověření svého účtu

(např. heslo potvrzené kódem zaslaným v sms či v autentizační aplikaci), pokud používá pro přihlášení jiný než osobní počítač a tento způsob zabezpečení je dostupný, či přístupu k jakékoliv využívané aplikaci obsahující Důvěrné informace; Příjemce potvrzuje, že se s přehledem bezpečnostních opatření seznámil před podpisem této smlouvy;

2.1.3. zachová Důvěrné informace obdržené od Poskytovatele v důvěrnosti a omezí přístup k těmto Důvěrným informacím jen Poskytovatelem určeným osobám;

2.1.4. nepoužije obdržené Důvěrné informace pro vlastní potřebu nebo za jiným účelem než ke spolupráci Smluvních stran;

2.1.5. bez předchozího písemného souhlasu Poskytovatele neposkytne Důvěrné informace třetí osobě;

2.1.6. bez předchozího písemného souhlasu Poskytovatele nebude pořizovat kopie obdržených Důvěrných informací na vlastní nosiče nebo vzdálená úložiště mimo kontrolu Poskytovatele, nebude-li to nutné pro aktivní spolupráci s Poskytovatelem, tedy pro plnění úkolů;

2.1.7. zajistí, aby osoby, kterým je nutné sdělit Důvěrné informace, byly zavázány k mlčenlivosti na obdobné úrovni, jako stanoví tato Smlouva;

2.1.8. bude dodržovat vnitřní předpisy Poskytovatele.

2.2. Povinnosti a zákazy uvedené v článku 2.1 výše neplatí pro informace:

2.2.1. pokud je Příjemce povinen předat Důvěrné informace podle právních předpisů nebo podle nařízení soudu či jiného státního orgánu oprávněného regulovat fungování Příjemce,

2.2.2. Příjemcem prokazatelně vytvořené nezávisle na jednání Smluvních stran a bez jakékoliv souvislosti se vzájemnou spoluprací Smluvních stran, nebo

2.2.3. zpřístupněné Příjemci třetí stranou, nikoli však porušením této Smlouvy, povinností mlčenlivosti této třetí strany nebo jiné smluvní či zákonné povinnosti Příjemce nebo této třetí strany.

2.3. Příjemce nezískává v důsledku této Smlouvy či jinak žádné právo, titul ani licenci k Důvěrným informacím, a to ani po skončení spolupráce Smluvních stran.

2.4. Příjemce se zavazuje na písemnou žádost Poskytovatele vrátit bezodkladně Poskytovateli veškeré Důvěrné informace a vlastní kopie nevratným způsobem smazat.

2.5. V případě, že došlo nebo může dojít k prozrazení Důvěrných informací neoprávněné osobě, zavazuje se Příjemce o této skutečnosti neprodleně informovat technický odbor Poskytovatele a přijmout všechna opatření nezbytná k zabránění vzniku škody nebo omezení rozsahu škody již vzniklé a dále k dalšímu šíření Důvěrných informací.

2.6. Za výkon činností a za závazky stanovené v této smlouvě náleží Příjemci odměna, je-li ujednána v jiné smlouvě (například v pracovní smlouvě, smlouvě o dílo či ve smlouvě o výkonu funkce). Tato Smlouva o zachování důvěrnosti informací sama o sobě úplatná není.

3. Náhrada škody a obohacení

Poskytovatel je oprávněn v případě porušení této Smlouvy Příjemcem požadovat plnou náhradu škody vzniklou z důvodu tohoto porušení, ledaže Příjemce prokáže, že ani při zachování potřebné péče nebylo možno škodě předejít. Tímto není dotčena povinnost Příjemce uhradit Poskytovateli smluvní pokutu. Poskytovatel je oprávněn taktéž požadovat vydání veškerého obohacení, které Příjemce v důsledku porušení povinnosti dle této Smlouvy získal.

4. **Smluvní pokuta**

Poskytovatel je oprávněn v případě porušení této Smlouvy Příjemcem požadovat vůči Příjemci smluvní pokutu do výše 250.000,- Kč (slovy: dvěstěpadesát tisíc korun českých) za každý jednotlivý incident (časově ohraničený skutek) porušení povinnosti Příjemce sjednané v čl. 2.1, 2.4 a 2.5. této Smlouvy. Tímto ujednáním není dotčeno právo Poskytovatele požadovat náhradu škody vzniklou z důvodu tohoto porušení.

5. **Rozhodné právo**

Tato Smlouva se řídí právním řádem České republiky.

6. **Závěrečná ustanovení**

6.1. Veškeré dodatky a změny této Smlouvy musí být činěny v písemné formě a musí být schváleny a podepsány oběma Smluvními stranami, jinak jsou neplatné.

6.2. Tato Smlouva je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží jeden stejnopis.

6.3. Příjemce souhlasí s tím, aby Poskytovatel kopii této smlouvy včetně jeho údajů zveřejnil, přičemž údaje Poskytovatele, který je fyzickou osobou, mohou být zveřejněny jen v rozsahu jména a příjmení, obce bydliště a roku narození.

6.4. Tato Smlouva obsahuje úplný konsensus Smluvních stran o jejím obsahu a v tomto smyslu také nahrazuje všechny předchozí dohody, ujednání, sliby anebo prohlášení.

6.5. V této Smlouvě, pokud z kontextu jasně nevyplývá jinak, zahrnuje význam slova v jednotném čísle rovněž význam daného slova v množném čísle a naopak, význam slova vyjadřujícího určitý rod zahrnuje rovněž ostatní rody. Nadpisy jsou uváděny pouze pro přehlednost a nemají vliv na výklad této Smlouvy.

6.6. Nevymahatelnost či neplatnost kteréhokoliv ustanovení této Smlouvy nemá vliv na vymahatelnost či platnost zbývajících ustanovení této Smlouvy, pokud z povahy nebo obsahu takového ustanovení nevyplývá, že nemůže být odděleno od ostatního obsahu této Smlouvy.

6.7. Tato Smlouva se stává platnou a účinnou ke dni jejího podpisu poslední ze Smluvních stran a uzavírá se na dobu neurčitou.

6.8. Povinnosti dle této Smlouvy k Důvěrným informacím nabytých v době trvání spolupráce Smluvních stran a v době trvání této Smlouvy přetrvávají ve stejném rozsahu i po zániku spolupráce Smluvních stran. Příjemce se tedy zavazuje dodržovat povinnosti dle této Smlouvy i po skončení vzájemné spolupráce Smluvních stran. Ukončením vzájemné spolupráce Smluvních stran není dotčeno především právo Poskytovatele na smluvní pokutu dle čl. 4 této Smlouvy.

6.9. Smluvní strany nejsou oprávněny tuto Smlouvu jednostranně ukončit.

V Praze dne 27. 7. 2021

.....

Česká pirátská strana
Poskytovatel

.....

Příjemce

Poučení o bezpečnostních opatřeních – příklady porušení smlouvy o zachování důvěrnosti informací („NDA")

Projděte si následující seznam, abyste si byli jisti, že jste pro dodržení NDA udělali vše, co bylo ve vašich silách:

- Mám nastavené dvoufázové ověření všude, kde je to možné (není nutné u osobních zařízení).
- Nenechávám svůj počítač/telefon bez dozoru zapnutý a neuzamčený.
- Nenechávám počítač, telefon ani dokumenty v autě bez dozoru.
- Chráním svá hesla a další přístupové údaje, nezapisuju je na papírky u souvisejícího zařízení.
- Nezveřejňuji chráněné osobní údaje (GDPR).
- Neposkytuji nikomu informace (či zápisy) z uzavřených jednání
- Skartuji dokumenty, které obsahují osobní údaje nebo utajované informace.
- Uvědomuji si, že Piráty reprezentuji 24/7 (i večer na pivu) a podle toho se chovám.
- Nemluvím o konkrétních projektech a vztazích na pracovišti na veřejnosti (lidé poslouchají a riziko zneužití informací je všude).
- Nezadávejte hesla na zařízeních, kde hrozí odposlech hesel (key logger), zejména pokud nejsou chráněna dvoufázovým ověřením.

Pár tipů, jak se vyhnout nepříjemnostem (doporučená, nikoliv povinná opatření):

- Nepoužívejte počítače, které neznáte a a neukládejte data na pochybná zařízení.
- Zašifrujte si disk.
- Mám aktualizovaný antivirus na svých zařízeních.
- Počítejte s tím, že co říkáte do telefonů, může být odposlechnuto či nahráno; to stejné platí i pro počítače s mikrofonem a webkamerou (pozor, platí to i v případě, že jsou přístroje vypnuté).
- "Clean desk" princip je nejlepší způsob, jak předejít ztrátě dokumentů či citlivých dat - jednoduše, když odcházím z práce, vše uklidím a ideálně uzamknu.
- Whistleblower není lobbistický kontakt, naopak, jeho identitu je třeba chránit.
- Pokud se dostanu do střetu zájmů, který může mít vliv na důvěrnost informací, proberu to s neutrálním členem strany a nechám o tomto vyhotovit záznam.

Zde uvádíme konkrétní příklady situací, kdy půjde o porušení NDA. Samozřejmě tento výčet není vyčerpávající a mohou nastat i další dnes i obtížně představitelné situace.

Poskytnutí soukromých zpráv, e-mailů a jiných informací uživatelů uložené na spravovaném zařízení

Tohoto porušení se např. jako správce serveru dopustíš, pokud třetím osobám přepošleš soukromé zprávy či jejich obsah bez odpovídajícího důvodu (např. technický problém se sítí může odůvodňovat takovou zprávu přeposlat kolegovi, aby se zjistilo, proč systém nefunguje). Uživatelé systémů spoléhají na to, že zajišťujeme ochranu jejich soukromým datům.

Identifikace whistleblowerů

Tohoto porušení se jako příjemce údajů dopustíš, pokud jakýmkoliv způsobem třeba i nepřímo označíš konkrétního whistleblowera. Tedy např. člověka, který anonymně upozornil na nějaký nešvar ve státní správě. Nemusí jít o přímé označení jménem např. na webu či při rozhovoru s novinářem. K porušení stačí i poskytnutí jasného vodítka. Např. informace, kdy a kde se bude daný člověk nacházet, nebo označení jeho konkrétní funkce a dalších údajů, které vedou k jeho „dopadení". Whistleblowerem Transparency International je bývalý nebo stávající zaměstnanec, který je na svém pracovišti svědkem závažných nelegitimních, neetických nebo nezákonných praktik, prováděných se souhlasem nadřízených, a informuje o nich osoby nebo instituce, které mohou sjednat nápravu.

Poskytnutí tabulek lidí a jiných chráněných osobních údajů

Tohoto porušení se jako příjemce údajů dopustíš pokud např. na blogu či na plakátu zveřejníš telefonní číslo na nějakého kolegu či spolupracovníka, případně jeho adresu či jiný údaj bez jeho souhlasu (může jít třeba i o sexuální orientaci). Je zde však potřeba připomenout, že se to samozřejmě netýká informací, které jsou již veřejné známé, nebo je zná daná osoba, které to sděluješ. Pak o porušení nejde. Opravdu si nemůžeme dovolit, aby například unikly tabulky osobních údajů našich členů, jak se to stalo ODS.

Poskytnutí záznamů, zápisů a jiné informace z uzavřených jednání.

Tohoto porušení se jako příjemce údajů dopustíš pokud např. novinářům, nakladatelům či dokonce politické konkurenci vyzradíš záznamy a poznámky z uzavřených jednání. Může jít třeba o průzkumy veřejného mínění, různé verze strategií či prostě jen hodnocení konkrétních osob. Nezapomeň, že informace jsou nebezpečná zbraň. Informace vytržené z kontextu mohou pak být ještě nebezpečnější. Poskytnutí je však možné, pokud tuto informaci cíleně a řízeně uvolňuje pověřená osoba např. při vyjednání či mediálních výstupech.

Poskytnutí přístupových údajů

V neposlední řadě je samozřejmě potřeba chránit přístupové údaje do různých zařízení. Vyzrazení hesla svého kolegy třetí straně může vést k značnému narušení jeho soukromí a poškození celé strany, v případě, že disponuš administrátorskými či moderátorskými oprávněními může kompromitace hesel vést i ke změně dat v systému a ohrožení integrity dat. Opět zde však samozřejmě platí, že pokud je potřeba s danými údaji pracovat z technických důvodů, nemusí o porušení povinností jít. Důležitý je úmysl.