Technická a organizační opatření

Naší vizí v NTT je zajistit **bezpečnou a propojenou budoucnost prostřednictvím technologií a inovací**. Zavedli jsme naše technická a organizační opatření („TOO“), která popisují, jak zajišťujeme ochranu osobních údajů transparentním, spravedlivým, etickým a zákonným způsobem.

Naše TOO jsou založena na osvědčených postupech v oboru a požadavcích stanovených platnými právními předpisy v jurisdikcích, ve kterých působíme, s přihlédnutím k povaze zpracovávaných údajů a nákladům na jejich zavedení.

Obsah

(A) Opatření na ochranu osobních údajů

1 Model řízení a provozu

1.1 NTT se zavázalo nést odpovědnost za zpracování osobních údajů, zavedla organizační strukturu a přiřadila role a povinnosti pro správu a dohled nad zpracováním osobních údajů.

1.2 Byla zavedena řada řídicích struktur, které zajišťují přezkum otázek ochrany osobních údajů příslušným vedením NTT. Konečnou odpovědnost za ochranu osobních údajů nese představenstvo společnosti NTT Ltd., přičemž příslušnou podporu poskytují určené role v rámci celé skupiny, včetně jmenovaných pověřenců pro ochranu osobních údajů nebo podobných funkcí, pokud to vyžadují právní předpisy o ochraně osobních údajů.

2 Zásady, postupy a pokyny

2.1 NTT zavedla a oznámila své zásady, procesy, normy a pokyny, které podrobně popisují, jak mají její zaměstnanci zpracovávat osobní údaje.
Jedná se o následující zásady:

2.1.1 Zásady ochrany osobních údajů;

2.1.2 Zásady práv subjektů údajů; a

2.1.3 Zásady oznamování porušení zabezpečení osobních údajů.

2.2 NTT definovala a zveřejnila oznámení o ochraně osobních údajů, která poskytují zaměstnancům, klientům a dalším zúčastněným stranám informace o tom, jak NTT zpracovává osobní údaje.

2.3 NTT má zaveden Proces pro provádění posuzování vlivu na ochranu osobních údajů (Data Protection Impact Assessment – DPIA) a v případě potřeby DPIA provádí v souladu s právními předpisy o ochraně osobních údajů.

3 Záměrná ochrana osobních údajů

3.1 NTT se zavazuje zavést přiměřená opatření na podporu schopnosti svých klientů dodržovat platné právní předpisy o ochraně osobních údajů. Při vývoji a poskytování produktů, služeb a řešení NTT v maximální možné míře uplatňuje zásady záměrné a standardní ochrany osobních údajů.

4 Datové prostředí

4.1 NTT zavedlo procesy pro identifikaci, zaznamenávání, vyhodnocování a udržování přehledu o osobních údajích, které zpracovává.

4.2 NTT vede záznamy o zpracovávaných osobních údajích v souladu s platnými právními předpisy o ochraně osobních údajů.

5 Správa životního cyklu informací

5.1 NTT má zavedeny zásady a postupy, které zajišťují, že osobní údaje jsou zpracovávány náležitým způsobem po celou dobu jejich životního cyklu (od shromáždění přes používání, uchovávání, zpřístupňování, až po jejich zničení).

5.2 Platné právní předpisy o ochraně osobních údajů v některých zemích poskytují subjektům údajů zvláštní práva v souvislosti s jejich osobními údaji. NTT se zavazuje tato práva dodržovat a reagovat na žádosti subjektů údajů transparentně, spravedlivě, eticky a v souladu se zákonem.

5.3 NTT má zavedeny Zásady pro uplatňování práv subjektů údajů a Proces vyřizování žádostí subjektů údajů s cílem prosazovat práva subjektů údajů v souladu s platnými právními předpisy o ochraně osobních údajů.

5.4 NTT vede záznamy o všech obdržených žádostech subjektů údajů a opatřeních přijatých v reakci na tyto žádosti. Svým klientům poskytne NTT přiměřenou podporu při reakci na žádosti subjektů údajů, pokud o to požádají, v souladu s uzavřenými smlouvami.

5.5 NTT dodržuje Zásady a harmonogram uchovávání údajů, které jsou v souladu s platnými právními předpisy. Osobní údaje NTT uchovává pouze, pokud existuje legitimní obchodní účel a v souladu se svými povinnostmi stanovenými právními předpisy. NTT osobní údaje zničí, vymaže nebo anonymizuje poté, co uplyne doba jejich uchovávání a pokud neexistuje žádný legitimní obchodní důvod pro uchovávání těchto osobních údajů po delší dobu.

5.6 NTT zpracovává osobní údaje pro své klienty v souladu s požadavky klienta a na jeho žádost osobní údaje zničí, vymaže, anonymizuje nebo mu je vrátí, pokud podle platných právních předpisů neexistuje žádná další povinnost tyto osobní údaje uchovávat.

5.7 NTT vyvíjí veškeré přiměřené úsilí s cílem zajistit přesnost, úplnost a aktuálnost osobních údajů.

5.8 NTT se opírá o standardní smluvní doložky, aby byla zajištěna zákonnost předávání osobních údajů mimo zemi, kde byly původně shromážděny, a za tímto účelem má také uzavřeny příslušné smlouvy s dceřinými společnostmi, ostatními společnostmi, které jsou součástí skupiny, se zpracovateli, dílčími zpracovateli a klienty.

6 Školení a informovanost o ochraně osobních údajů

6.1 NTT od svých zaměstnanců vyžaduje každoročně absolvovat školení o ochraně osobních údajů. Všechny zásady, procesy, normy a pokyny týkající se ochrany osobních údajů jsou zaměstnancům k dispozici a zaměstnanci jsou s nimi pravidelně seznamováni. V případě potřeby jsou také poskytovány školení na místní, nebo regionální úrovni nebo v souvislosti s určitými funkcemi, která zaměstnance podporují v jednání, které je v souladu s požadavky na ochranu osobních údajů v konkrétních zemích, regionech nebo obchodních funkcích.

7 Zabezpečení osobních údajů

7.1 Týmy v NTT pro ochranu osobních údajů a bezpečnost informací spolupracují s cílem zavést vhodnou správu a opatření na ochranu osobních údajů, aby byla chráněna jejich důvěrnost, integrita a dostupnost.

Naše bezpečnostní metodiky jsou v souladu s normami ISO27001 a Rámcem pro kybernetickou bezpečnost („CSF“) Národního institutu standardů a technologie (NIST).

8 Reakce na porušení zabezpečení osobních údajů a jejich oznamování

8.1 NTT má zavedeny zásady, procesy a postupy pro identifikaci, odhalení, reakci, obnovu a informování příslušných zainteresovaných stran v případě porušení zabezpečení osobních údajů. Jedná se o mechanismy pro provádění analýzy kořenových příčin a přijímání nápravných opatření.

8.2 NTT se zavazuje, že v případě porušení zabezpečení osobních údajů bude informovat příslušné orgány pro ochranu osobních údajů, dotčené klienty a dotčené subjekty údajů v souladu s platnými právními předpisy o ochraně osobních údajů a veškerými smluvními závazky.

8.3 NTT vede záznamy o všech případech porušení zabezpečení osobních údajů a o opatřeních přijatých v reakci na tyto události.

8.4 Opatření NTT pro řízení incidentů, která slouží k identifikaci, odhalování, reakci a obnově po incidentech v oblasti bezpečnosti informací, jsou popsána v oddíle B (Bezpečnost informací) těchto TOO.

9 Řízení třetích stran

9.1 NTT je odpovědná za činnost svých zpracovatelů (tj. dílčích zpracovatelů), kteří zpracovávají osobní údaje pro NTT, a posuzuje schopnost svých zpracovatelů chránit osobní údaje v době jejich výběru a poté pravidelně v souladu se svými zásadami.

9.2 Zpracovatelé NTT jsou povinni podepsat příslušné smlouvy, které upravují zpracování a ochranu osobních údajů a NTT vyžaduje přenos stejných povinností, které jsou uvedeny ve smlouvě o zpracování osobních údajů, na další zpracovatele, jejichž služby NTT využívá. NTT vyvíjí veškeré přiměřené úsilí k tomu, aby bylo zajištěno, že smlouvy o zpracování osobních údajů se zpracovateli jsou uzavřeny.

10 Monitorování a hodnocení

10.1 NTT pravidelně informuje Výbor pro audit a rizika NTT Ltd o koncepci a provozní účinnosti svých činností v oblasti ochrany osobních údajů. Součástí výše uvedeného je podávání zpráv, sebehodnocení managementu, certifikace, přezkoumání interním auditem a nezávislé audity a hodnocení.

(B) Opatření pro bezpečnost informací

NTT se zavazuje, že zavede a bude řádně řídit systém kontroly bezpečnosti informací s cílem chránit důvěrnost, integritu a dostupnost osobních údajů zpracovávaných pro své klienty a dle jejich pokynů.

NTT zavedla v rámci celé skupiny Systém řízení bezpečnosti informací („ISMS“), který je v souladu s předními světovými postupy a normami v oblasti bezpečnosti informací, včetně řady ISO27000 a Rámce kybernetické bezpečnosti („CSF“) Národního institutu standardů a technologie (NIST).

11 Bezpečnost informací

11.1 NTT formálně přiřadila role a odpovědnosti za bezpečnost informací s příslušnými kanály pro hlášení, které zajišťují nezávislost daných funkcí, včetně vedoucího bezpečnostního pracovníka (Chief Security Officer – CSO), vedoucích pracovníků pro bezpečnost informací (Chief Information Security Officers – CISO) a pracovníků pro bezpečnost informací (Information Security Officers, ISO).

11.2 Zaměstnanci NTT jsou odpovědní za to, že při svých každodenních obchodních činnostech jednají v souladu se zásadami, procesy, normami a pokyny

pro bezpečnost informací.

11.3 NTT zdokumentovala a zveřejnila soubor zásad bezpečnosti informací, které podporují požadavky systému ISMS. Zásady a související dokumentace se pravidelně revidují.

11.4 NTT zavedla opatření zajišťující ochranu mobilních zařízení (včetně notebooků, mobilních telefonů, tabletů, zařízení umožňujících vzdálený přístup a programů „Přines si své zařízení“) a jejich obsahu. Vyvíjí přiměřené úsilí při instalaci softwaru pro správu mobilních zařízení (mobile device management – „MDM“) na všech mobilních zařízeních s přístupem do podnikové sítě NTT.

11.5 Pracovníci pracující na dálku mají v případě potřeby vzdálený přístup k infrastruktuře NTT pouze prostřednictvím služeb virtuální privátní sítě (VPN).

12 Lidské zdroje

12.1 NTT provádí u svých zaměstnanců prověrky uváděných údajů a zaměstnání v rozsahu povoleném platnými právními předpisy s cílem ujistit se o jejich vhodnosti k zaměstnání a nakládání s informacemi NTT a klientů (včetně osobních údajů). Rozsah prověrky je úměrný obchodním požadavkům a úrovni utajení informací, ke kterým má mít zaměstnanec přístup.

12.2 NTT po svých zaměstnancích (včetně smluvních partnerů a dočasných zaměstnanců) vyžaduje zachování mlčenlivosti, a to jak ve vztahu k interním údajům, tak ve vztahu k údajům klientů (včetně osobních údajů).

12.3 Zaměstnanci NTT každoročně absolvují školení o povědomí o bezpečnosti informací. Zaměstnancům jsou k dispozici zásady bezpečnosti informací a podpůrné postupy, procesy a směrnice a prostřednictvím komunikačních platforem NTT dostávají relevantní informace o trendech, hrozbách a osvědčených postupech.

13 Řízení přístupu

13.1 NTT dodržuje Zásady přijatelného užívání (Acceptable Use Policy), které podporují správné a účinné používání a ochranu podnikových aktiv NTT, včetně počítačových a telekomunikačních zdrojů, produktů, služeb, řešení a IT infrastruktury.

13.2 NTT se řídí Zásadami klasifikace informací, které popisují vhodné technické a organizační opatření pro nakládání s informacemi na základě jejich klasifikace. Informace a aktiva jsou chráněny v souladu s označením stupně utajení.

14 Správa aktiv

14.1 NTT uplatňuje Zásady řízení přístupu, podpůrné postupy a opatření logického a fyzického přístupu s cílem zajistit, aby k informacím, u nichž je uplatňován princip nejnižších privilegií, měly přístup pouze oprávněné osoby.

14.2 U IT aktiv, aplikací, systémů a databází se pravidelně provádí kontroly přístupu s cílem zajistit, že přístup budou mít pouze oprávněné osoby.

14.3 Zpracovatelé NTT (tj. dílčí zpracovatelé) musí k přístupu k systémům NTT využívat jmenné účty. Společné účty a/nebo sdílení pověření jsou zakázány, pokud vedení nebo klienti výslovně nepovolí výjimku.

14.4 NTT vyvinula přiměřené úsilí, aby přísně omezila počet uživatelů svých aplikací, systémů a databází s vyšším oprávněním („správců“).

15 Fyzická a environmentální bezpečnost

15.1 NTT zavedla přiměřená a vhodná opatření v souladu se Zásadami fyzické bezpečnosti s cílem zabránit neoprávněnému fyzickému přístupu, poškození nebo narušení informací, aplikací, systémů, databází a infrastruktury NTT v následujících oblastech:

15.1.1 řízení fyzického přístupu;

15.1.2 monitorování a auditování fyzického přístupu;

15.1.3 oblasti ochrany před environmentálním nebezpečím;

15.1.4 zabezpečení fyzických aktiv;

15.1.5 zabezpečení kabeláže;

15.1.6 oblasti manipulace s fyzickými a informačními aktivy;

15.1.7 oblasti údržby a likvidace hmotného majetku;

15.1.8 oblasti principu čistého stolu a obrazovky;

15.1.9 přístupu návštěvníků a dohledu nad nimi; a

15.1.10 oblasti opatření pro bezpečnost a ochranu zdraví při práci.

16 Provozní bezpečnost

16.1 Oddělení NTT pro informace a technologie („I&T“) je odpovědné za správu aplikací, systémů, databází a infrastruktury NTT. I&T dokumentuje, udržuje a zavádí všechny provozní zásady a postupy v oblasti IT, které

jsou v souladu s normami COBIT a ITIL.

16.2 NTT má zavedeny zásady a podpůrné postupy pro řízení změn obchodních procesů, aplikací, systémů, databází a infrastruktury. NTT zavedlo několik řídicích struktur, které přezkoumávají a schvalují veškeré změny v závislosti na velikosti a rozsahu změny a strategických cílech. Všechny žádosti a jejich výsledky se zaznamenávají a dokumentují.

16.3 NTT má zaveden program řízení hrozeb a zranitelností podporovaný standardními odvětvovými nástroji pro identifikaci, řízení a zmírňování rizik pro firemní informace včetně osobních údajů zaměstnanců a klientů. Jedná se o novou generaci Detekce a reakce na kybernetické útoky (Endpoint Detection and response - „EDR“) pro nástroje antivirové antimalwarové ochrany, pravidelné skenování prostředí, opravné protokoly a řízení činností pro zjednání nápravy a zlepšení.

16.4 Požadavky na kapacitu jsou průběžně sledovány a pravidelně přezkoumávány. Systémy a sítě se budou spravovat a rozšiřovat v souladu s těmito přezkumy.

16.5 Dostupnost systému zahrnuje architekturu, návrh vysoké dostupnosti a/nebo zálohování na základě požadavků na riziko a dostupnost každého systému. O metodě správy dostupnosti nebo obnovy systému, včetně rozsahu a četnosti zálohování rozhodují obchodní požadavky NTT, včetně požadavků klienta, a kritičnosti informací. Monitorování záloh se provádí k zajištění úspěšného dokončení zálohování, stejně jako pro správu případných problémů se zálohováním, výjimky nebo selhání.

16.6 NTT vynakládá přiměřené úsilí na uchovávání auditních protokolů v aplikacích a systémech. Tyto protokoly jsou pravidelně kontrolovány a jsou k dispozici pro účely vyšetřování. Přístup k těmto protokolům je přísně omezen pouze na oprávněné pracovníky.

17 Pořizování, vývoj a údržba systému

17.1 NTT se řídí Zásadami bezpečnosti architektury a návrhu a podpůrnými normami a postupy, které zajišťují použití zásad bezpečnosti od fáze návrhu v rámci životního cyklu vývoje softwaru.

17.2 NTT nedovoluje používat údaje z produkčního prostředí, údaje klientů, osobní údaje ani žádné důvěrné informace pro účely testování. Ve výjimečných případech mohou být použity údaje z produkčního prostředí nebo údaje klientů se souhlasem příslušného klienta nebo vlastníka projektu.

18 Řízení třetích stran

18.1 NTT se řídí Zásadami bezpečnosti třetích stran a podpůrnými postupy, které zajišťují ochranu informačních aktiv v případech, kdy NTT využívá služeb třetích stran a/nebo zpracovatelů. Součástí výše uvedeného jsou požadavky na hloubkovou prověrku bezpečnosti informací a hodnocení rizik bezpečnosti informací, které je třeba provést k zajištění následujícího:

18.1.1 požadavky na bezpečnost informací jsou jasně formulovány a zdokumentovány ve smlouvách se zpracovateli NTT;

18.2 zpracovatelé NTT zajišťují stejnou úroveň ochrany a kontroly jako NTT;

18.3 zpracovatelé jsou povinni NTT včas hlásit jakékoli podezření nebo skutečně vzniklé incidenty v oblasti bezpečnosti informací.

18.4 NTT vyvinulo přiměřené úsilí a uzavřelo příslušné smlouvy se zpracovateli, kteří mají přístup k informacím, aplikacím, systémům, databázím a infrastruktuře NTT. Tyto smlouvy zahrnují standardy NTT pro bezpečnost informací, aby byla zajištěna důvěrnost, integrita a dostupnost informací NTT.

19 Řízení incidentů v oblasti bezpečnosti informací

19.1 NTT má zavedeny zásady, procesy a postupy pro identifikaci, odhalování, reakci, obnovu a informování příslušných zúčastněných stran v případě incidentu v oblasti bezpečnosti informací, včetně porušení zabezpečení osobních údajů. Součástí výše uvedeného jsou mimo jiné mechanismy pro provádění analýzy kořenových příčin a přijímání opatření ke zjednání nápravy.

19.2 NTT zavedlo bezpečnostní operace v rámci celé skupiny a proaktivně monitoruje a spravuje všechny síťové a počítačové prostředky. To je podporováno technickými nástroji pro reakce na incidenty v oblasti bezpečnosti informací a obnovu po takových incidentech.

20 Kontinuita podnikatelské činnosti

20.1 NTT zavedlo plány kontinuity podnikatelské činnosti a obnovy po havárii. NTT přijalo vrstvený přístup k

zajištění dostupnosti svých systémů a dat.	**21**	**Dodržování právních předpisů**	
	21.1	NTT stanovilo role a odpovědnosti za identifikaci právních předpisů, které mají dopad na naši podnikatelskou činnost. Odpovědnost za dodržování právních předpisů je stanovena na úrovni skupiny a rovněž na úrovni regionů, aby bylo zajištěno, že NTT splňuje požadavky stanovené právními předpisy globálně i na místní úrovni.	
			21.2 NTT prosazuje důsledný přístup k bezpečnosti informací napříč svými obchodními operacemi. Produkty, služby a řešení NTT jsou v souladu s normou ISO 27001 a v případě, že jsou certifikovány (pokud tak je uvedeno ve smlouvě s klientem), jsou v souladu s touto normou každoročně auditovány.

V případě jakýchkoli dotazů se obraťte na oddělení pro ochranu osobních údajů na adrese **privacyoffice@global.ntt**

Together we do great things