

Technická a organizační opatření

Ochrana soukromí a osobních údajů

Obsah

1.	**Úvod**	**3**
2.	**Ochrana osobních údajů a opatření na ochranu**	**4**
2.1.	Model řízení a provozu	4
2.2.	Zásady, postupy a pokyny	4
2.3.	Záměrná ochrana osobních údajů	4
2.4.	Datové prostředí	4
2.5.	Správa životního cyklu informací	4
2.6.	Práva subjektů údajů	5
2.7.	Přeshraniční předávání	5
2.8.	Právní úprava	5
2.9.	Školení a informovanost o ochraně osobních údajů	5
2.10.	Zabezpečení osobních údajů	6
2.11.	Reakce na porušení zabezpečení osobních údajů a jejich oznamování	6
2.12.	Řízení třetích stran	6
3.	**Opatření pro bezpečnost informací**	**7**
3.1.	Role a odpovědnosti v oblasti bezpečnosti informací	7
3.2.	Pravidla pro bezpečnost informací	7
3.3.	Řízení mobilních zařízení	7
3.4.	Lidské zdroje	7
3.5.	Přijatelné užívání	7
3.6.	Řízení přístupů	8
3.7.	Správa a klasifikace informací	8
3.8.	Fyzická a environmentální bezpečnost	8
3.9.	Provozní bezpečnost	9
3.10.	Pořizování, vývoj a údržba systému	9
3.11.	Řízení třetích stran	9
3.12.	Řízení incidentů v oblasti bezpečnosti informací	9
3.13.	Kontinuita podnikatelské činnosti	9
3.14.	Dodržování právních předpisů	9

Úvod

Od strategického poradenství až po špičkové technologie, NTT DATA umožňuje zkušenosti, které transformují společnosti k úspěchu, mění průmyslová odvětví a formují lepší společnost pro všechny.

Naše technická a organizační opatření popisují, jak zajišťujeme ochranu osobních údajů transparentním, férovým, etickým a zákonným způsobem.

Jsou založena na osvědčených postupech v oboru a plnění požadavků stanovených právními předpisy v jurisdikcích, ve kterých působíme, přičemž jsme brali v úvahu povahu osobních údajů, které zpracováváme a náklady na jejich zavedení.

V případě jakýchkoli dotazů ohledně našich technických a organizačních opatřeních nebo jak se týkají našich produktů, služeb nebo řešení, prosím kontaktujte Vašeho servisního zástupce v NTT DATA.



Naše technická a organizační opatření popisují, jak zajišťujeme ochranu osobních údajů transparentním, férovým, etickým a zákonným způsobem.

Ochrana osobních údajů a opatření na ochranu

2.1. Model řízení a provozu

NTT DATA se zavázala nést odpovědnost za zpracování osobních údajů. Máme odpovídající organizační strukturu, role a povinnosti pro správu a dohled nad zpracováním osobních údajů.

V každé jurisdikci, kde působíme, jsou organizační jednotky povinny vyčlenit vhodné zdroje, aby byly v souladu s platnými právními předpisy o ochraně osobních údajů. To zahrnuje jmenování pracovních pozicí kvalifikovaných pro ochranu osobních údajů, na kterých budou zaměstnanci dohlížet na zajištění souladu s platnými právními předpisy o ochraně osobních údajů a také stanovení vhodných reportovacích struktur.

NTT DATA pravidelně informuje top management o koncepci a provozní účinnosti svých činností v oblasti ochrany osobních údajů.

2.2. Zásady, postupy a pokyny

NTT DATA zavedla a oznámila svá pravidla, procesy, normy a pokyny, které podrobně popisují, jak mají zaměstnanci NTT DATA zpracovávat osobní údaje.
NTT DATA definovala a zveřejnila prohlášení o ochraně osobních údajů, která poskytují zaměstnancům, klientům a dalším zúčastněným stranám informace o tom, jak NTT DATA zpracovává osobní údaje.

NTT DATA zavedla procesy a šablony pro provádění hodnocení rizik, včetně posuzování vlivu na ochranu osobních údajů (Data Protection Impact Assessment – DPIA), posouzení oprávněného zájmu (LIA) a posouzení rizik předávání osobních údajů, v souladu s platnými právními předpisy o ochraně osobních údajů.

2.3. Záměrná ochrana osobních údajů

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

2.4. Datové prostředí

NTT DATA zavedla procesy pro identifikaci, zaznamenávání, vyhodnocování osobních údajů a rozumí osobním údajům, které zpracovává.

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

2.5. Správa životního cyklu informací

NTT DATA 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).

NTT DATA má svá pravidla a harmonogramy pro uchovávání osobních údajů, které jsou v souladu s právními předpisy. NTT DATA uchovává osobní údaje pouze pokud k tomu existuje legitimní obchodní účel a pouze v souladu se svými závazky podle právních předpisů. NTT DATA zničí, vymaže nebo anonymizuje osobní údaje poté, co uběhne doba jejich uchovávání nebo pokud již neexistuje legitimní obchodní důvod, na základě kterého by byly osobní údaje uchovávány po delší dobu.

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

NTT vynakládá veškeré přiměřené úsilí, aby zajistila, že osobní údaje jsou přesné, kompletní a aktuální.

2.6. Práva subjektů údajů

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

NTT DATA má zavedena odpovídající pravidla a postupy pro vyřizování žádostí subjektů údajů s cílem prosazovat práva subjektů údajů v souladu s platnými právními předpisy o ochraně osobních údajů.

NTT DATA podporuje následující práva subjektů údajů:

- Právo být informován
- Právo přístupu k osobním údajům
- Právo na opravu
- Právo být zapomenut
- Právo na přenos osobních údajů
- Právo na omezení přístupu
- Právo vznést námitku (včetně práva vnést námitku proti zpracování osobních údajů pro účely přímého marketingu, kdy osobní údaje nebudou pro tento účel dále zpracovány, a proti prodeji osobních údajů)
- Právo vznést námitku proti automatizovanému rozhodování
- Právo na nediskriminaci
- Právo podat stížnost

NTT DATA zajišťuje, aby byly subjektům údajů k dispozici vhodné kanály, aby mohly uplatnit svá práva ve vztahu k osobním údajům, které o nich může NTT DATA zpracovávat.

NTT DATA vede záznamy o všech obdržených žádostech subjektů údajů a opatřeních přijatých v reakci na tyto žádosti.

NTT DATA svým klientům poskytne přiměřenou podporu při reakci na žádosti subjektů údajů, pokud o to požádají, v souladu s uzavřenými smlouvami.

NTT DATA zavedla pravidla a postupy, které zajistí, že odpovíme na veškeré žádosti od orgánů veřejné moci o zpřístupnění osobních údajů v souladu s platnými právními předpisy a smluvními požadavky. NTT DATA vede záznamy o těchto žádostech a a o jejich výsledcích.

2.7. Přeshraniční předávání

NTT DATA zavádí vhodné záruky (jako jsou rozhodnutí o přiměřenosti, standardní smluvní doložky a další nástroje stanovené v platných právních předpisech) při přeshraničním předávání osobních údajů.

V případech, kdy dochází k přeshraničnímu předání osobních údajů, NTT DATA provádí posouzení vlivu převodu na ochranu osobních údajů (transfer impact assesment) (TIA), aby zajistila, že země, do které jsou osobní údaje předávány, poskytuje odpovídající míru ochrany právům a svobodám subjektů údajů, jako země, kde byly osobní údaje původně shromážděny. Jestliže odpovídající míra ochrany neexistuje, NTT DATA zavádí dodatečná opatření, aby podpořila práva subjektů údajů v souladu se svými interními pravidly a v souladu s požadavky právních předpisů. Pokud taková dodatečná opatření nelze provést, NTT DATA ukončí předávání osobních údajů.

NTT DATA se spoléhá na standardní smluvní doložky na podporu zákonného přenosu osobních údajů mimo zemi, kde byly osobní údaje původně shromážděny. Na podporu takových převodů jsou uzavřeny příslušné smlouvy s dceřinými společnostmi NTT DATA, společnostmi skupiny, přidruženými společnostmi, zpracovateli, dílčími zpracovateli a klienty.

2.8. Právní úprava

NTT DATA monitoruje změny v právní úpravě na ochranu osobních údajů v zemích, kde NTT DATA působí a zavedla procesy a nástroje, aby zajistila soulad s právními předpisy.

2.9. Školení a informovanost o ochraně osobních údajů

NTT DATA je odhodlána zavádět kulturu povědomí a dodržování předpisů prostřednictvím průběžných školení a iniciativ na zvyšování povědomí. NTT DATA od svých zaměstnanců vyžaduje pravidelně absolvovat povinné školení o ochraně osobních údajů. Školící materiály a související směrnice, standardy, pokyny a postupy 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.

2.10. Zabezpečení osobních údajů

Společnost NTT DATA zavedla vhodná technická a organizační opatření, aby zajistila důvěrnost, integritu a dostupnost osobních údajů, přičemž bere v úvahu stav technologií, náklady na implementaci a povahu, rozsah, kontext a účel zpracování osobních údajů, stejně jako rizika pro práva a svobody subjektů údajů.

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

2.11. Reakce na porušení zabezpečení osobních údajů a jejich oznamování

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

NTT DATA se zavazuje, že v případě porušení zabezpečení osobních údajů budou příslušné orgány pro ochranu osobních údajů, dotčení klienti a dotčené subjekty údajů informováni v souladu s platnými právními předpisy o ochraně osobních údajů a veškerými smluvními závazky.

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

Část 3: Opatření pro bezpečnost informací popisuje naše opatření pro řízení incidentů, která slouží k identifikaci, odhalování, reakci a obnově po incidentech v oblasti bezpečnosti informací.

2.12. Řízení třetích stran

NTT DATA je odpovědná za činnost zpracovatelů a dílčích zpracovatelů, kteří pro nás zpracovávají osobní údaje. Posuzujeme schopnost těchto zpracovatelů a dílčích zpracovatelů chránit osobní údaje v souladu se standardy NTT DATA, a to jednak v době jejich výběru a dále pravidelně poté.

Zpracovatelé a dílčí zpracovatelé NTT DATA jsou povinni podepsat odpovídající smlouvy, které upravují zpracování a ochranu osobních údajů. Tyto smlouvy zahrnují požadavky na zajištění toho, aby stejné povinnosti byly přeneseny na jakékoli další zpracovatele, kteří mohou osobní údaje zpracovávat.



Opatření pro bezpečnost informací

NTT DATA se zavazuje zajistit, že systém kontroly bezpečnosti informací je implementován a řádně spravován s cílem chránit důvěrnost, integritu a dostupnost osobních údajů.

Společnost NTT DATA zavedla vhodné zásady, procesy, postupy, standardy a směrnice k zajištění bezpečnosti dat, která zpracovává. Bezpečnostní metodiky NTT DATA jsou v souladu s ISO 27001 a dalšími osvědčenými postupy v oboru.

3.1. Role a odpovědnosti v oblasti bezpečnosti informací

V rámci své organizační struktury NTT DATA 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).

Zaměstnanci NTT DATA jsou odpovědní za to, že při svých každodenních obchodních činnostech jednají v souladu s našimi zásadami, procesy, normami a pokyny pro bezpečnost informací.

3.2. Pravidla pro bezpečnost informací

NTT DATA zdokumentovala a zveřejnila soubor pravidel pro bezpečnost informací. Tyto pravidlá a související dokumentace se pravidelně revidují.

3.3. Řízení mobilních zařízení

NTT DATA vytvořila rámec nulové důvěryhodnosti pro implementaci a udržování bezpečnostních kontrol pro přístup a interakci s NTT DATA systémy a informačními aktivy. Tento rámec zahrnuje:

- Zásady a podpůrné postupy pro správu koncových zařízení (EDM).
- Ovládací prvky a nástroje pro udržení bezpečnosti.
- Důvěrnost, dostupnost a integrita podnikových dat. Tato data mohou být uložena na místě nebo mohou být dostupná prostřednictvím koncových uživatelských zařízení (včetně notebooků, mobilních telefonů, tabletů a zařízení umožňujících vzdálený přístup).

3.4. Lidské zdroje

NTT DATA 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 DATA a klientů (včetně osobních údajů). Rozsah prověrky je úměrný obchodním požadavkům a úrovni utajení informací, ke kterým má mít zaměstnanec přístup.

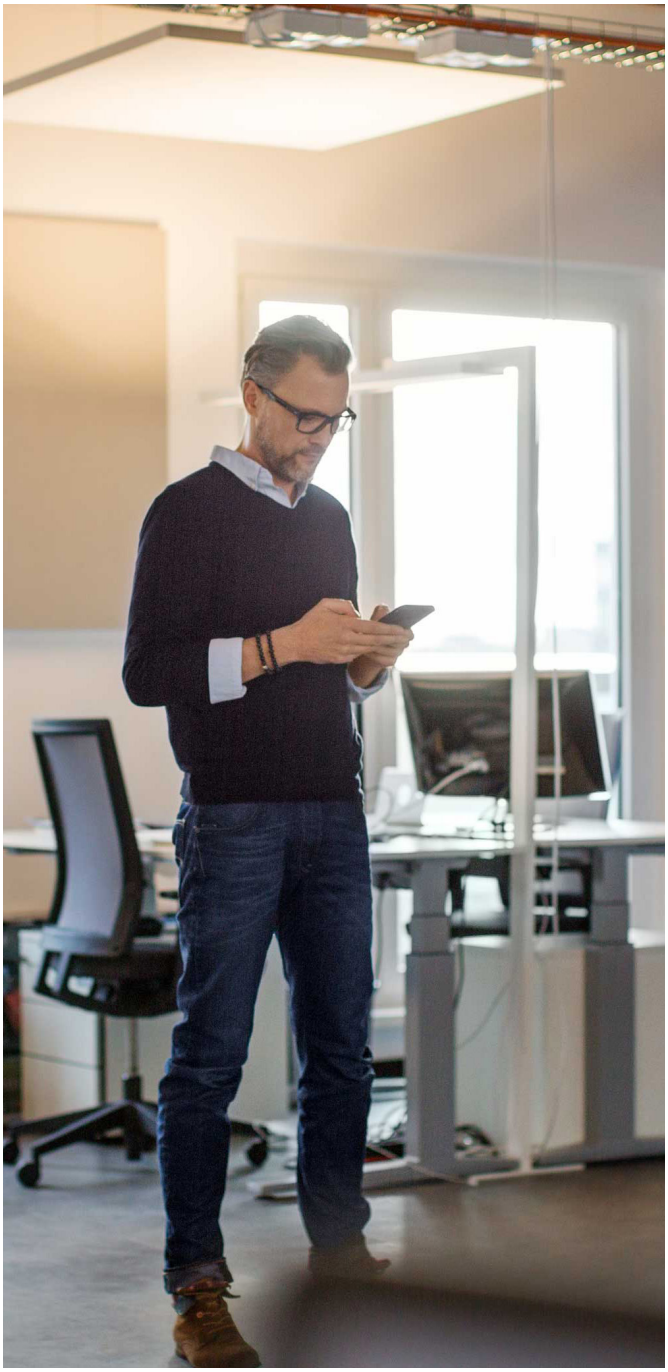
NTT DATA po svých zaměstnancích (včetně smluvních partnerů a dočasných zaměstnanců) vyžaduje zachování mlčenlivosti, a to jak ve vztahu k informacím NTT DATA, tak ve vztahu k informacím klientů (včetně osobních údajů).

Zaměstnanci NTT DATA každoročně absolvují školení o bezpečnosti informací a pravidelné opakující se školení. Zaměstnancům jsou pravidelně poskytovány a komunikovány pravidla pro bezpečnost informací a rovněž podpůrné postupy, procesy a směrnice.

Zaměstnanci NTT DATA dostávají relevantní informace o trendech, hrozbách a osvědčených postupech.

3.5. Přijatelné užívání

NTT DATA zavedla postupy, které podporují správné a účinné používání a ochranu našich podnikových aktiv, včetně počítačových a telekomunikačních zdrojů, produktů, služeb, řešení a IT infrastruktury.



“

Bezpečnostní metodiky NTT DATA jsou v souladu s ISO 27001 a dalšími osvědčenými postupy v oboru.”

3.6. Řízení přístupů

NTT DATA zavedla pravidla a postupy pro 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.

V případech, kde je to vhodné, společnost NTT DATA zavedla šifrování při ukládání a při přenosu (encryption at-rest and in-transit), které je v oboru standardní, aby zajistila, že osobní údaje jsou chráněny proti neoprávněnému přístupu nebo zveřejnění. Pravidelně se provádí kontroly přístupu s cílem zajistit, že k systémům NTT DATA a k informacím budou mít přístup pouze oprávněné osoby.

NTT DATA vyvinula přiměřené úsilí, aby omezila počet uživatelů, kteří mají vyšší oprávnění na přístup k systémům NTT DATA a informacím. NTT DATA neumožňuje společné účty nebo přihlašovací údaje, pokud management nebo klienti výslovně nepovolí výjimku.

3.7. Správa a klasifikace informací

NTT DATA zavedla zásady, které řídí klasifikaci a manipulaci s informacemi, včetně bezpečné likvidace dat, aby bylo zajištěno, že informace jsou chráněny na odpovídající úrovni.

Data jsou založena na obchodní kritickosti pro stanovení požadavků na důvěrnost. Odvětvové pokyny pro nakládání s osobními údaji poskytují rámec pro technická, organizační a fyzická zabezpečení. Tato ochranná opatření mohou zahrnovat kontroly, jako je správa přístupu, šifrování, protokolování a monitorování a zničení dat.

3.8. Fyzická a environmentální bezpečnost

NTT DATA implementovala přiměřená a vhodná opatření v souladu s našimi pravidly fyzické bezpečnosti s cílem zabránit neoprávněnému fyzickému přístupu, poškození nebo narušení našich informací, aplikací, systémů, databází a infrastruktury. Tyto zahrňují:

- řízení fyzického přístupu
- monitorování a auditování fyzického přístupu
- oblasti ochrany před environmentálním nebezpečím
- zabezpečení fyzických aktiv
- oblasti manipulace s fyzickými aktivy
- oblasti údržby a likvidace hmotného majetku
- oblasti principu čistého stolu a obrazovky
- řízení přístupu návštěvníků a dohledu nad nimi

3.9. Provozní bezpečnost

NTT DATA vytvořila specializované týmy, které jsou odpovědné za správu a ochranu informačních systémů a infrastruktury NTT DATA. NTT DATA zavedla zásady a podpůrné postupy pro řízení změn obchodních procesů, informačních systémů a infrastruktury. NTT DATA zavedlo několik řídicích struktur, které přezkoumávají a schvalují jakékoli změny v závislosti na velikosti a rozsahu změny a strategických cílech. Všechny žádosti a jejich výsledky se zaznamenávají a dokumentují.

NTT DATA 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.

Požadavky na kapacitu jsou průběžně sledovány a pravidelně přezkoumávány. Systémy a sítě jsou spravovány a rozšiřovány v souladu s těmito přezkumy.

Dostupnost systému zahrnuje architekturu, návrh vysoké dostupnosti, plány obnovy po havárii (Disaster Recovery plány) 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 DATA, včetně požadavků klienta, a kritičnosti informací. Plány obnovy po havárii jsou pravidelně testovány. Procesy zálohování jsou monitorovány, aby bylo zajištěno úspěšné dokončení zálohování, stejně jako pro správu případných problémů se zálohováním, výjimky nebo selhání.

NTT DATA 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.

3.10. Pořizování, vývoj a údržba systému

NTT DATA vytvořila rámec bezpečnosti architektury, který řídí návrh, akvizici a údržbu informačních systémů a infrastruktury. Máme zavedenou architekturu, návrh designu a podpůrné normy a postupy, které zajišťují použití zásad bezpečnosti od fáze návrhu v rámci životního cyklu vývoje softwaru.

3.11. Řízení třetích stran

NTT DATA zavedla pravidla pro informační bezpečnost třetích stran a podpůrné postupy, které zajišťují ochranu informačních aktiv v případech, kdy NTT DATA využívá služby 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:

- požadavky na bezpečnost informací jsou jasně formulovány a zdokumentovány ve smlouvách v souladu se standardy NTT DATA pro informační bezpečnost;
- poskytovatelé služeb pro NTT DATA a zpracovatelé zajišťují stejnou úroveň ochrany a kontroly jako NTT DATA;
- poskytovatelé služeb pro NTT DATA a zpracovatelé jsou povinni NTT DATA včas hlásit jakékoli podezření nebo skutečně vzniklé incidenty v oblasti bezpečnosti informací.

3.12. Řízení incidentů v oblasti bezpečnosti informací

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

NTT DATA zavedlo bezpečnostní operace v rámci celé skupiny a proaktivně monitoruje a spravuje všechny síťové a počítačové prostředky. Tyto operace jsou podporovány technickými nástroji pro reakce na incidenty v oblasti bezpečnosti informací a obnovu po takových incidentech.

3.13. Kontinuita podnikatelské činnosti

NTT DATA zavedlo plány kontinuity podnikatelské činnosti a obnovy po havárii. NTT DATA přijalo vrstvený přístup ke kontinuitě podnikatelské činnosti k zajištění dostupnosti systémů a dat.

3.14. Dodržování právních předpisů

NTT DATA 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 DATA splňuje požadavky stanovené právními předpisy globálně i na místní úrovni.


NTT DATA