Technikai és szervezési intézkedések

Az NTT-nél az a jövőképünk, hogy a **technológia és az innováció révén biztonságos és összekapcsolt jövőt** teremtsünk **.** Az NTT technikai és szervezési intézkedéseket állított össze, amelyek leírják, hogyan biztosítjuk a személyes adatok védelmét átlátható, tisztességes, etikus és jogszerű módon.

A technikai és szervezési intézkedések az iparági legjobb gyakorlatokon és azon joghatóságok alkalmazandó jogi követelményein alapulnak, ahol működünk, figyelembe véve az általunk kezelt adatok jellegét és a végrehajtás költségeit.

Tartalom

(A) Adatvédelmi intézkedések

1 Irányítási és működési modell

1.1 Az NTT elkötelezett az elszámoltathatóság mellett, amikor az NTT személyes adatokat dolgoz fel, és szervezeti struktúrát, valamint szerepeket és felelősségi köröket határozott meg a személyes adatok kezelésének irányítása és felügyelete céljából.

1.2 Az NTT számos irányítási struktúrát vezetett be annak biztosítása érdekében, hogy az adatvédelmi kérdéseket az NTT-n belül a megfelelő vezetőség felülvizsgálja. Az adatvédelemmel kapcsolatos végső elszámoltathatóságot az NTT Ltd. igazgatótanácsa képviseli, amelyet az egész vállalaton belül kijelölt szerepkörök támogatnak, beleértve a kijelölt adatvédelmi tisztviselőket vagy ezzel egyenértékű szerepköröket, ahol az adatvédelmi jogszabályok ezt megkövetelik.

2 Szabályzatok, folyamatok és iránymutatások

2.1 Az NTT bevezett és kommunikált olyan szabályzatokat, folyamatokat, szabványokat és iránymutatásokat, amelyek részletesen leírják, hogy az NTT alkalmazottai hogyan kezelhetik a személyes adatokat.
Ez a következő szabályzatokat érinti:

2.1.1 Adatvédelemi szabályzat;

2.1.2 Az érintettek jogaira vonatkozó szabályzat; és

2.1.3 Adatvédelmi incidens értesítési szabályzat.

2.2 Az NTT adatvédelmi tájékoztatót fogalmazott meg és tett közzé, amely tájékoztatást nyújt az alkalmazottak, az ügyfelek és más érdekelt felek számára a személyes adatok kezelésének módjáról.

2.3 Az NTT adatvédelmi hatásvizsgálati folyamatot (DPIA) állított össze, és szükség esetén, valamint az adatvédelmi jogszabályoknak megfelelően adatvédelmi hatásvizsgálatot végez.

3 Beépített adatvédelem

3.1 Az NTT elkötelezett az ésszerű intézkedések végrehajtása mellett, hogy támogassa ügyfeleit az adatvédelmi jogszabályok betartása során. Amennyire lehetséges, az NTT termékeinek, szolgáltatásainak és megoldásainak fejlesztése és szállítása során a lehető legnagyobb mértékben alkalmazza a beépített és alapértelmezett adatvédelem elveit.

4 Adattérkép

4.1 Az NTT folyamatokat vezetett be az általa kezelt személyes adatok azonosítása, nyilvántartása, értékelése és értelmezése céljából.

4.2 Az NTT az általa kezelt személyes adatokról az alkalmazandó adatvédelmi jogszabályoknak megfelelően nyilvántartást vezet.

5 Adat életciklus menedzsment

5.1 Az NTT szabályzatokat és folyamatokat vezetett be annak biztosítása érdekében, hogy a személyes adatok kezelése az adatok teljes életciklusa alatt (a gyűjtéstől a felhasználáson, megőrzésen, nyilvánosságra hozatalon és megsemmisítésen át) megfelelő módon történjen.

5.2 Az adatvédelmi jogszabályok egyes országokban az érintettek számára különleges jogokat biztosítanak a személyes adataikkal kapcsolatban. Az NTT elkötelezett ezen jogok fenntartása mellett, és biztosítja, hogy az NTT az érintettek kérelmeire átlátható, tisztességes, etikus, és törvényes módon reagáljon.

5.3 Az alkalmazandó adatvédelmi jogszabályokkal összhangban az NTT az érintettek jogaira vonatkozó szabályzatot és az érintettek kérelmére vonatkozó eljárást vezetett be az érintettek jogainak védelme érdekében.

5.4 Az NTT nyilvántartást vezet az érintettektől beérkezett kérelmekről, és az adott kérelmek esetén tett intézkedésekről. Az NTT minden ésszerű támogatást biztosít ügyfelei részére az érintettek kérelmére adott válasz során, amennyiben erre igényt tartanak, a velük kötött megállapodásokkal összhangban.

5.5 Az NTT az alkalmazandó jogszabályokkal összhangban adatmegőrzési szabályzatot és ütemtervet tart fenn. Az NTT csak akkor őrzi meg a személyes adatokat, ha jogos üzleti céljai alapján erre szüksége van, valamint a jogszabályi kötelezettségeivel összhangban. Az NTT megsemmisíti, törli vagy személyazonosításra alkalmatlanná teszi a személyes adatokat, amikor a megőrzési időszak lejár, és nem áll fenn jogos üzleti érdeke a személyes adatok hosszabb ideig történő megőrzésére.

5.6 Az NTT az ügyfelei nevében kezelt személyes adatokat az ügyfél követelményeinek megfelelően őrzi meg, és kérésre megsemmisíti, törli, személyazonosításra alkalmatlanná teszi, vagy visszaküldi a személyes adatokat az ügyfél részére, illetve ha az alkalmazandó jog alapján nem áll fenn további

kötelezettsége a személyes adatok megőrzésére.

5.7 Az NTT minden ésszerű erőfeszítést megtett annak biztosítása érdekében, hogy a személyes adatok pontosak, teljesek és naprakészek legyenek.

5.8 Az NTT az általános szerződési feltételekre támaszkodik a személyes adatok jogszerű továbbítása érdekében azon országon kívülre, ahol a személyes adatokat eredetileg gyűjtötték és az NTT leányvállalataival, kapcsolt vállalkozásaival, adatfeldolgozóival, további feldolgozóival és ügyfeleivel megfelelő megállapodást kötött a határokon átnyúló adattovábbítás támogatása érdekében.

6 Adatvédelmi képzés és tudatosság

6.1 Az NTT minden alkalmazottjától megköveteli, hogy évente adatvédelmi képzésen vegyenek részt. Minden adatvédelmi szabályzatot, folyamatot, szabványt és iránymutatást elérhetővé teszünk a munkavállalók számára, és rendszeresen tájékoztatjuk őket ezekről. Szükség esetén helyi, regionális vagy funkcionális képzéseket is biztosítunk számukra annak érdekében, hogy a munkavállalók az egyes országokban, régiókban vagy üzleti funkciókban az adatvédelmi követelményeknek megfelelően tudjanak eljárni.

7 Adatbiztonság

7.1 Az NTT adatvédelmi és információbiztonsági csapatai együttműködnek annak érdekében, hogy a személyes adatok bizalmas jellegének, sértetlenségének és rendelkezésre állásának védelme érdekében megfelelő adatvédelmi irányítást és ellenőrzést hajtsanak végre.

Biztonsági módszereink az ISO27001 és a NIST kiberbiztonsági keretrendszer („CSF") szabványaihoz igazodnak.

8 Adatvédelmi incidensek elhárítása és bejelentése

8.1 Az NTT rendelkezik szabályzatokkal, folyamatokkal és eljárásokkal az adatvédelmi incidens esetén történő azonosítás, felderítés, reagálás, helyreállítás és a megfelelő érdekelt felek értesítése céljából.
Ez magában foglalja a kiváltó okok elemzésének elvégzésére és a korrekciós intézkedések megtételére szolgáló mechanizmusokat.

8.2 Az NTT elkötelezett annak biztosítása mellett, hogy az NTT a vonatkozó adatvédelmi jogszabályok és a szerződéses kötelezettségei értelmében értesítse az illetékes adatvédelmi hatóságokat, az érintett ügyfeleket és az érintetteket adatvédelmi incidens esetén.

8.3 Az NTT nyilvántartást vezet az adatvédelmi incidensekről és az adott incidensek esetén tett intézkedésekről

8.4 Az NTT incidenskezelési intézkedéseit az információbiztonsági incidensek azonosítására, felderítésére, megválaszolására és helyreállítására a jelen technikai és szervezési intézkedések B. szakasza (Információbiztonság) tartalmazza.

9 Harmadik felek kezelése

9.1 Az NTT felelős adatfeldolgozói (azaz további feldolgozói) tevékenységéért, akik az NTT nevében személyes adatokat dolgoznak fel, és kiválasztásuk során, valamint azt követően rendszeresen értékeli, hogy adatfeldolgozói képesek-e a személyes adatok védelmét biztosítani az NTT szabályzataival összhangban.

9.2 Az NTT adatfeldolgozóinak megfelelő megállapodásokat kell aláírniuk, amelyek szabályozzák a személyes adatok feldolgozását és védelmét, és előírják, hogy az adatfeldolgozási megállapodásban meghatározott kötelezettségek az NTT által esetlegesen megbízott további adatfeldolgozókra is átruházásra kerülnek.

Az NTT minden ésszerű erőfeszítést megtett annak biztosítása érdekében, hogy adatfeldolgozóival adatfeldolgozási megállapodásokat kössön.

10 Monitorozás és értékelés

10.1 Az NTT rendszeres

időközönként jelentést tesz az adatvédelmi tevékenységeinek kialakításáról és működési hatékonyságáról az NTT Ltd. Ellenőrzési és Kockázati Bizottsága és a felső vezetés felé.

Ez magában foglalja az egyoldalas jelentéseket, a vezetőségi önértékeléseket, a tanúsításokat, a belső ellenőrzési felülvizsgálatokat, valamint a független ellenőrzéseket és értékeléseket.

(B) Információbiztonsági intézkedések

Az NTT elkötelezett amellett, hogy biztosítsa az információbiztonsági ellenőrzés végrehajtását és megfelelő irányítását az ügyfelei nevében és utasítására kezelt személyes adatok bizalmas jellegének, integritásának és rendelkezésre állásának védelme érdekében.

Az NTT a csoport egészére kiterjedő információbiztonsági irányítási rendszert („ISMS") hozott létre, amely a világ vezető információbiztonsági gyakorlataihoz és szabványaihoz igazodik, beleértve az ISO27000 sorozatot és a NIST kiberbiztonsági keretrendszert („CSF").

11 Információbiztonság

11.1 Az információbiztonsággal kapcsolatos szerepeket és felelősségi köröket hivatalosan kijelölték, a funkció függetlenségét biztosító jelentéstételi vonalakkal, beleértve a biztonsági igazgatót („CSO"), az információbiztonsági igazgatókat („CISO") és az információbiztonsági tisztviselőket („ISO").

11.2 Az NTT alkalmazottai felelősek azért, hogy az információbiztonsági szabályzatoknak, folyamatoknak, szabványoknak és iránymutatásoknak megfelelően járjanak el mindennapi üzleti tevékenységük során.

11.3 Az NTT olyan információbiztonsági szabályzatokat dokumentált és tett közzé, amelyek támogatják az ISMS követelményeit. A szabályzatokat és az alátámasztó dokumentációt rendszeresen felülvizsgálják.

11.4 Az NTT intézkedéseket hozott annak biztosítására, hogy a mobil eszközök (beleértve a laptopokat, mobiltelefonokat, táblagépeket, a távoli hozzáférést lehetővé tevő eszközöket és a „Hozd a saját eszközödet" égisze alatt használt eszközök) és azok tartalma védett legyen. Az NTT ésszerű erőfeszítéseket tett annak biztosítása érdekében, hogy az NTT vállalati hálózatához hozzáférő valamennyi mobileszközön mobileszköz-kezelő („MDM") szoftverek legyenek telepítve.

11.5 A távmunkások csak virtuális magánhálózati ("VPN") szolgáltatások igénybevételével férhetnek hozzá az NTT infrastruktúrájához távolról, amennyiben ez lehetséges.

12 Humán erőforrások

12.1 Az NTT a vonatkozó jogszabályok által megengedett mértékben háttér- és foglalkoztatási átvilágítást végez alkalmazottai esetében, hogy biztosítsa felvételi alkalmasságukat a felvételre, valamint a vállalati és ügyféladatok (beleértve a személyes adatokat is) feldolgozására. Az átvilágítás mértéke az üzleti követelményekkel és azon adatok besorolásával arányos, amelyekhez az alkalmazott hozzáférhet.

12.2 Az NTT megköveteli, hogy az NTT alkalmazottai (beleértve az alvállalkozókat és kölcsönzött munkavállalókat is) vállalják az NTT belső és ügyféladatainak (beleértve a személyes adatokat is) bizalmas kezelését.

12.3 Az NTT alkalmazottai évente kötelesek elvégezni az információbiztonsági tudatosságnövelő képzést. Az információbiztonsági szabályzatokat és az azokat támogató eljárásokat, folyamatokat és iránymutatásokat az alkalmazottak rendelkezésére bocsátják, és az alkalmazottak az NTT kommunikációs platformjain keresztül releváns információkat kapnak a trendekről, fenyegetésekről és a legjobb gyakorlatokról.

13 Hozzáférés ellenőrzése

13.1 Az NTT rendelkezik egy elfogadható használati szabályzattal, amely támogatja az NTT vállalati eszközeinek, beleértve a számítógépes és távközlési erőforrások, termékek, szolgáltatások, megoldások és az informatikai infrastruktúra, megfelelő és hatékony használatát és védelmét.

13.2 Az NTT információ besorolási szabályzatot tart fenn, amely leírja az információk kezelésének megfelelő technikai és szervezési ellenőrzését azok besorolása alapján. Az információk és eszközök a besorolási címkének megfelelő védelmet élveznek.

14 Eszközkezelés

14.1 Az NTT rendelkezik hozzáférés-szabályozási szabályzattal, támogató eljárásokkal, valamint logikai és fizikai hozzáférési intézkedésekkel annak biztosítása érdekében, hogy az adatokhoz a legkisebb kiváltság elve alapján csak az arra jogosult személyek férjenek hozzá.

14.2 Az informatikai eszközök, alkalmazások, rendszerek és adatbázisok hozzáférésének rendszeres időközönként történő felülvizsgálata biztosítja, hogy azokhoz csak az arra jogosult személyek férjenek hozzá.

14.3 Az NTT-feldolgozók (azaz a további feldolgozók) névre szóló fiókok használatával férnek hozzá az NTT rendszereihez. Az általános fiókok használata és/vagy a hitelesítő adatok megosztása tilos, kivéve, ha a kivételt a vezetőség vagy az ügyfelek kifejezetten engedélyezik.

14.4 Az NTT ésszerű erőfeszítéseket tett annak érdekében, hogy szigorúan korlátozza a kiváltságos („Admin") felhasználók számát alkalmazásaiban, rendszereiben és adatbázisaiban.

15 Fizikai és környezeti biztonság

15.1 Az NTT ésszerű és megfelelő intézkedéseket hozott a fizikai biztonsági szabályzattal összhangban az NTT információihoz, alkalmazásaihoz, rendszereihez, adatbázisaihoz és infrastruktúrájához való jogosulatlan fizikai hozzáférés, azok károsítása vagy megzavarása megelőzése érdekében az alábbi területeken:

15.1.1 Fizikai hozzáférés ellenőrzése:

15.1.2 A fizikai hozzáférés ellenőrzése és auditálása;

15.1.3 Védelem a Környezeti veszélyek ellen;

15.1.4 Fizikai eszközök biztosítása;

15.1.5 Kábelezés biztonsága;

15.1.6 Fizikai és információs eszközök kezelése;

15.1.7 A fizikai eszközök karbantartása és ártalmatlanítása;

15.1.8 Tiszta íróasztal és képernyő szabályzat;

15.1.9 Látogatók bejutása és felügyelete; és

15.1.10 Egészségi és biztonsági eljárásrend.

16 Működési biztonság

16.1 Az NTT IT részlege felelős az NTT alkalmazásainak, rendszereinek, adatbázisainak és infrastruktúrájának kezeléséért.
Az IT dokumentálja, karbantartja és végrehajtja a COBIT és az ITIL szabványokhoz igazodó összes informatikai működési szabályzatot és eljárást.

16.2 Az NTT rendelkezik az üzleti folyamatok, alkalmazások, rendszerek, adatbázisok és infrastruktúra változásainak kezelésére vonatkozó szabályzattal és támogató eljárásokkal.
Az NTT többféle irányítási struktúrát hozott létre a változások felülvizsgálatára és jóváhagyására a változás nagysága és terjedelme, valamint a stratégiai célok alapján.
Minden kérelem és annak eredménye naplózásra és dokumentálásra kerül.

16.3 Az NTT iparági szabványos eszközökkel támogatott fenyegetés- és sebezhetőségkezelési programot hozott létre a vállalati információkat, köztük az alkalmazottak és az ügyfelek személyes adatait érintő kockázatok azonosítása, kezelése és csökkentése érdekében.

Ez magában foglalja a vírus- és malware-ellenes rendszerek következő generációs végpont-érzékelési és -reagálási („EDR”) eszközeit, a környezetek rendszeres ellenőrzését, a patching protokollokat, valamint a javítási és fejlesztési tevékenységek irányítását.

16.4 A kapacitásigényeket folyamatosan nyomon követik és rendszeresen felülvizsgálják.
A rendszereket és hálózatokat e felülvizsgálatokkal összhangban kezelik és méretezik.

16.5 A rendszer rendelkezésre állása magában foglalja az architektúrát, a nagy rendelkezésre állású tervezést és/vagy a biztonsági mentéseket az egyes rendszerekre vonatkozó kockázati és rendelkezésre állási követelmények alapján. A rendszer rendelkezésre állásának vagy helyreállításának módszerét, beleértve a biztonsági mentések terjedelmét és gyakoriságát az NTT üzleti követelményeit, illetve az ügyfél követelményeit, és az információk kritikussága alapján határozzák meg.

A biztonsági mentések figyelemmel kísérése a mentés sikeres befejezésének biztosítása, valamint az esetleges biztonsági mentési problémák, kivételek vagy hibák kezelése érdekében.

16.6 Az NTT ésszerű erőfeszítéseket tesz az alkalmazások és rendszerek ellenőrzési naplózásának fenntartására. A naplókat rendszeresen felülvizsgálják, és vizsgálati célokra rendelkezésre állnak.
A naplókhoz való hozzáférés szigorúan csak az arra jogosult személyzetre korlátozódik.

17 Rendszerbeszerzés, fejlesztés és karbantartás

17.1 Az NTT rendelkezik egy biztonsági architektúra- és tervezési szabályzattal, valamint támogató szabványokkal és eljárásokkal, amelyek biztosítják, hogy a szoftverfejlesztés életciklusa során a beépített biztonsági elveket alkalmazzák.

17.2 Az NTT nem engedélyezi, hogy a gyártási, ügyfél-, személyes adatokat vagy bármilyen bizalmas információt tesztelési célokra használjanak.
Kivételes esetekben a gyártási vagy ügyféladatok az érintett ügyfél vagy cégtulajdonos jóváhagyásával felhasználhatók.

18 Harmadik felek kezelése

18.1 Az NTT rendelkezik harmadik félre vonatkozó biztonsági szabályzattal és támogató eljárásokkal, amelyek biztosítják az információs eszközök védelmét, amikor az NTT harmadik fél szolgáltatókat és/vagy adatfeldolgozókat vesz igénybe. Ez magában foglalja az információbiztonsági átvilágításra vonatkozó követelményeket, valamint információbiztonsági

kockázatértékelést kell végezni a következők biztosítása érdekében:

18.1.1 Az információbiztonsági követelményeket egyértelműen megfogalmazzák és dokumentálják az NTT adatfeldolgozóival kötött megállapodásokban.

18.1.2 Az NTT adatfeldolgozói az NTT-vel azonos szintű védelmet és ellenőrzést valósítanak meg;

18.1.3 A feldolgozók kötelesek minden feltételezett vagy tényleges információbiztonsági incidenst időben jelenteni az NTT felé.

18.2 Az NTT ésszerű erőfeszítéseket tett annak biztosítására, hogy megfelelő megállapodások legyenek érvényben azokkal a feldolgozókkal, akik hozzáférnek az NTT adataihoz, alkalmazásaihoz, rendszereihez, adatbázisaihoz és infrastruktúráihoz. Ezek a megállapodások tartalmazzák az NTT információbiztonsági szabványait, amelyek biztosítják az NTT adatainak bizalmas jellegét, integritását és elérhetőségét.

19 Információbiztonsági incidensek kezelése

19.1 Az NTT szabályzatokat, folyamatokat és eljárásokat léptetett életbe az információbiztonsági incidensek, beleértve az adatvédelmi incidenseket is, azonosítása, felderítése, kezelése, helyreállítása és a megfelelő érdekelt felek értesítése céljából.

Ez magában foglalja a kiváltó okok elemzésének elvégzésére és a korrekciós intézkedések megtételére szolgáló mechanizmusokat.

19.2 Az NTT csoportos biztonsági műveleteket hozott létre az összes hálózati és számítástechnikai eszköz proaktív figyelemmel kísérése és kezelése érdekében. Ezt az információbiztonsági incidensekre való reagálás és helyreállítás technikai eszközei is támogatják.

20 Üzletmenet-folytonosság

20.1 Az NTT üzletmenet-folytonossági és katasztrófa-helyreállítási terveket dolgozott ki. Az NTT többszintű megközelítést alkalmaz rendszereink és adataink rendelkezésre állásának biztosítása érdekében.

21 Megfelelőség

21.1 Az NTT meghatározta az NTT üzleti tevékenységét érintő jogszabályok és rendeletek azonosítására vonatkozó szerepeket és felelősségi köröket. A jogszabályok és rendeletek betartásának felelőssége csoportos és regionális szinten kerül szabályozásra annak érdekében, hogy az NTT megfeleljen a globális és helyi követelményeknek.

21.2 Az NTT egységes információbiztonsági megközelítést alkalmaz minden üzleti tevékenysége során. Az NTT termékei, szolgáltatásai és megoldásai az ISO 27001 szabványhoz igazodnak, és amennyiben az ügyfélmegállapodásban foglaltak szerint tanúsítottak, évente auditálják őket e szabványnak megfelelően.

Amennyiben bármilyen kérdése merülne fel, forduljon az Adatvédelmi Hivatalhoz a következő címen:
privacyoffice@global.ntt

Together we do great things