

Technikai és szervezési intézkedések

Adatbiztonság és adatvédelem

Tartalom

1.	**Bevezetés**	**3**
2.	**Adatbiztonsági és adatvédelmi intézkedések**	**4**
2.1.	Irányítási és működési modell	4
2.2.	Irányelvek, folyamatok és iránymutatások	4
2.3.	Adatvédelem terv szerint	4
2.4.	Adatkörnyezet	4
2.5.	Információs életciklus-kezelés	4
2.6.	Az érintett jogai	5
2.7.	Határon átnyúló adattovábbítás	5
2.8.	Szabályozás	5
2.9.	Képzés és tudatosság	5
2.10.	A személyes adatok biztonsága	6
2.11.	Az adatvédelmi incidensre való reagálás és bejelentés	6
2.12.	Harmadik felek kezelése	6
3.	**Információbiztonsági intézkedések**	**7**
3.1.	Információbiztonsági szerepek és felelősségi körök	7
3.2.	Információbiztonsági irányelvek	7
3.3.	Mobil készülékek kezelése	7
3.4.	Emberi erőforrások	7
3.5.	Elfogadható használat	7
3.6.	Hozzáférés kezelése	8
3.7.	Vagyonkezelés és osztályozás	8
3.8.	Fizikai és környezeti biztonság	8
3.9.	A működés biztonsága	9
3.10.	A rendszer beszerzése, fejlesztése és karbantartása	9
3.11.	Harmadik felek kezelése	9
3.12.	Információbiztonsági eseménykezelés	9
3.13.	Üzletmenet-folytonosság	9
3.14.	Megfelelés	9

Bevezetés

Az NTT DATA a stratégiai tanácsadástól a csúcstechnológiákig terjedő tevékenységével olyan tapasztalatokat nyújt, amelyek sikerre viszik a szervezeteket, jó irányba terelik az iparágakat, és amelyek mindenki számára lehetővé teszik egy jobb társadalom kialakítását.

Technikai és szervezési intézkedéseinkben azt ismertetjük, hogy milyen módon biztosítjuk a személyes adatok átlátható, tisztességes, etikus és jogszerű védelmét. Ezek az iparágban bevált gyakorlaton és az azon joghatóságok alkalmazandó jogi követelményein alapulnak, ahol működünk, melynek során figyelembe vesszük az általunk feldolgozott adatok jellegét és a végrehajtás költségeit is.

Ha bármilyen kérdése van ezekkel a technikai és szervezési intézkedésekkel kapcsolatban, illetve arra vonatkozóan, hogy ezek hogyan kapcsolódnak termékeinkhez, szolgáltatásainkhoz és megoldásainkhoz, kérjük, forduljon az ügyfélszolgálati képviselőjéhez.



Technikai és szervezési intézkedéseinkben azt ismertetjük, hogy milyen módon biztosítjuk a személyes adatok átlátható, tisztességes, etikus és jogszerű védelmét.

Adatbiztonsági és adatvédelmi intézkedések

2.1. Irányítási és működési modell

Az NTT DATA elkötelezett amellett, hogy a személyes adatok általa végzett feldolgozása során elszámoltathatósága mindvégig fennmaradjon. A személyes adatok kezelésének irányításához és felügyeletéhez megfelelő szervezeti struktúrákkal, szerep-, és felelősségi körökkel rendelkezünk.

A különböző joghatóságokban működő szervezeti egységeink kötelesek a helyben alkalmazandó adatvédelmi törvényeknek való megfeleléshez illeszkedő erőforrásokat biztosítani. Ez magában foglalja a megfelelőség felügyeletére szakképzett adatvédelmi erőforrások kinevezését, valamint a megfelelő bejelentési struktúrák létrehozását.

Az NTT DATA az adatbiztonsági és adatvédelmi tevékenységek kialakításáról és működési hatékonyságáról rendszeres jelentést készít a felső vezetésnek.

2.2. Irányelvek, folyamatok és iránymutatások

Az NTT DATA végrehajtotta és kommunikálta mindazokat az irányelveket, folyamatokat, szabványokat és iránymutatásokat, amelyek részletesen leírják, hogy az NTT DATA munkavállalói hogyan kötelesek feldolgozni a személyes adatokat.

Az NTT DATA meghatározta és közzétette az adatkezelési tájékoztatókat, amelyek a munkavállalók, az ügyfelek és más érdekelt felek számára nyújtanak tájékoztatást a személyes adatok feldolgozásának módjáról.

Az NTT DATA az alkalmazandó adatvédelmi jogszabályokkal összhangban folyamatokat és mintadokumentumokat vezetett be a kockázatértékelések elvégzésére, így például az adatvédelmi hatásvizsgálatokat (DPIA), a jogos érdekek értékelését (LIA) és az adattovábbítási kockázatértékeléseket.

2.3. Adatvédelem terv szerint

Az NTT DATA elkötelezett olyan ésszerű intézkedések végrehajtása mellett, amelyekkel támogatja ügyfelei adatvédelmi jogszabályok betartására vonatkozó képességét. Az NTT DATA a termékeinek, szolgáltatásainak és megoldásainak fejlesztése során a lehető legnagyobb mértékben a beépített és alapértelmezett adatvédelem elveit alkalmazza.

2.4. Adatkörnyezet

Az NTT DATA folyamatokat vezetett be az általa kezelt személyes adatok azonosítására, nyilvántartására, értékelésére és megértésére.

Az NTT DATA az alkalmazandó adatvédelmi jogszabályoknak megfelelő nyilvántartást vezet a kezelt személyes adatokról.

2.5. Információs életciklus-kezelés

Az NTT DATA irányelveket és folyamatokat vezetett be annak biztosítására, hogy a személyes adatokat az életciklusuk során (a gyűjtéstől a felhasználáson, megőrzésen, közlésen keresztül a megsemmisítésig) megfelelően kezeljék.

Az NTT DATA az alkalmazandó jogszabályokhoz igazodó adatmegőrzési irányelvekkel és ütemtervekkel rendelkezik. Az NTT DATA csak akkor őrzi meg a személyes adatokat, ha erre jogos üzleti okból, valamint jogszabályi kötelezettségeinek megfelelően van szükség.
Az NTT DATA megsemmisíti, törli vagy azonosíthatatlanná teszi a személyes adatokat, ha a megőrzési időszak lejár, és nincs jogos üzleti érdeke a személyes adatok hosszabb ideig történő megőrzésére.

Az NTT DATA az ügyfelei nevében kezelt személyes adatokat az ügyfél kérésének és az alkalmazandó jogszabályoknak megfelelően őrzi meg, és kérésre, illetve amennyiben az alkalmazandó jogszabályok alapján nincs további kötelezettség a személyes adatok megőrzésére, a személyes adatokat biztonságosan megsemmisíti, törli, azonosíthatatlanná teszi vagy visszajuttatja.

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

2.6. Az érintett jogai

Egyes országok adatvédelmi jogszabályai az érintettek számára különleges jogokat biztosítanak személyes adataikkal kapcsolatban. Az NTT DATA kötelezettséget vállal e jogok tiszteletben tartására és arra, hogy az érintettek kérelmeire időben, átlátható, tisztességes, etikus és jogszerű módon válaszol.

Az érintettek jogainak védelme érdekében az NTT DATA az alkalmazandó adatvédelmi jogszabályokkal összhangban megfelelő irányelveket és eljárásokat vezetett be.

Az NTT DATA az alábbi érintetti jogokat támogatja:

- Tájékoztatáshoz való jog
- Hozzáféréshez való jog
- A helyesbítéshez való jog
- Az elfeledtetéshez való jog
- Az adathordozhatósághoz való jog
- Az adatkezelés korlátozásához való jog
- A tiltakozáshoz való jog (beleértve a közvetlen üzletszerzés és a személyes adatok értékesítésének elutasításához való jogot)
- Az automatizált döntések megtámadásához való jog
- A hátrányos megkülönböztetéstől való mentességhez való jog
- Panaszjog

Az NTT DATA biztosítja, hogy az érintettek számára megfelelő csatornák álljanak rendelkezésre, hogy gyakorolhassák jogaikat az NTT DATA által velük kapcsolatban kezelt személyes adatok vonatkozásában.

Az NTT DATA nyilvántartja az érintettek részéről beérkezett összes kérelmet és az ezekre válaszul tett intézkedéseket.

Az NTT DATA a fennálló megállapodásokkal összhangban minden ésszerű támogatást megad az ügyfeleknek az érintettek kérelmeinek megválaszolásához.

Az NTT DATA a hatóságoktól érkező, a személyes adatokhoz való hozzáférésre irányuló kérelmekre történő válaszadáshoz az alkalmazandó jogszabályokkal és szerződéses követelményekkel összhangban álló irányelveket és eljárásokat hozott létre. Az NTT DATA nyilvántartja ezeket a kérelmeket és azok eredményeit.

2.7. Határon átnyúló adattovábbítás

Határokon átnyúló adattovábbításban történő részvétel esetére az NTT DATA megfelelő garanciákat hoz létre (például megfelelőségi határozatokat, szabványos szerződési záradékokat és az alkalmazandó jogszabályokban meghatározott egyéb eszközöket).

A személyes adatok határokon átnyúló továbbítása esetén az NTT DATA adattovábbítási hatásvizsgálatokat (TIA) végez annak biztosítása érdekében, hogy a célország az érintettek jogai és szabadságai tekintetében ugyanolyan szintű védelmet nyújtson, mint az az ország, ahol az adatokat eredetileg gyűjtötték. Amennyiben ilyen egyenértékűség nem áll fenn, felmérjük és elfogadjuk az érintettek jogait támogató, az irányelveinkkel és a jogszabályi követelményekkel összhangban álló kiegészítő intézkedéseket.

Amennyiben e kiegészítő intézkedések nem hajthatók végre, az NTT DATA leállítja a személyes adatok továbbítását.

Az NTT DATA a személyes adatoknak az eredeti gyűjtés helye szerinti országon kívül történő jogszerű továbbítása érdekében szabványos szerződéses záradékokra támaszkodik. Az ilyen jellegű adattovábbítások támogatása érdekében az NTT DATA leányvállalataival, csoportvállalataival, kapcsolt vállalkozásaival, adatfeldolgozóival, alfeldolgozóival és ügyfeleivel megfelelő megállapodások vannak érvényben.

2.8. Szabályozás

Azokban az országokban, ahol működik és a megfelelés támogatására folyamatokat és eszközöket vezetett be, az NTT DATA figyelemmel kíséri az adatvédelmi jogszabályok változásait.

2.9. Képzés és tudatosság

Az NTT DATA folyamatos képzések és tudatosságnövelő kezdeményezések révén elkötelezett a tudatosság és a megfelelés kultúrájának megvalósítása mellett. Minden munkavállalótól megköveteljük a kötelező adatbiztonsági és adatvédelmi képzésen való rendszeres részvételt. A képzési anyagok és a kapcsolódó irányelvek, folyamatok, szabványok és iránymutatások a munkavállalók rendelkezésére állnak, és azokat rendszeresen közöljük. Szükség esetén helyi, regionális vagy funkcionális képzéseket biztosítunk annak érdekében, hogy az egyes országokban, régiókban vagy üzleti funkciókban dolgozó munkavállalók a követelményeknek megfelelően tudjanak eljárni.

2.10. A személyes adatok biztonsága

Az NTT DATA megfelelő technikai és szervezési intézkedéseket hajtott végre a személyes adatok bizalmas kezelésének, integritásának és hozzáférhetőségének biztosítása érdekében, figyelembe véve a technika állását, a megvalósítás költségeit, a személyes adatok kezelésének jellegét, terjedelmét, összefüggéseit és célját, valamint az érintettek jogait és szabadságait érintő kockázatokat.

Az NTT DATA biztonsági módszerei az ISO 27001 és a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) szabványokhoz igazodnak.

2.11. Az adatvédelmi incidensre való reagálás és bejelentés

Az NTT DATA rendelkezik azokkal az irányelvekkel, folyamatokkal és eljárásokkal, amelyek az adatvédelmi incidensek azonosítására, felderítésére, az azokra való reagálásra és az azokból való helyreállításra, valamint az ilyen incidensek esetén a megfelelő érdekelt felek felé történő bejelentére vonatkoznak. Ezek között szerepelnek a kiváltó okok elemzésének elvégzésére és a korrekciós intézkedések megtételére szolgáló mechanizmusok.

Az NTT DATA elkötelezett annak biztosítása mellett, hogy a személyes adatok sérelme esetén az alkalmazandó adatvédelmi jogszabályoknak és a szerződéses kötelezettségeknek megfelelően értesítse az adott adatvédelmi hatóságokat, az érintett ügyfeleket és az érintetteket.

Az NTT DATA nyilvántartja a személyes adatok sérelmével járó összes esetet és az ezekre válaszul tett intézkedéseket.

„3. fejezet: Az információbiztonsági intézkedések” című rész ismerteti az információbiztonsági incidensek azonosítására, felderítésére, reagálásra és helyreállítására irányuló eseménykezelési intézkedéseinket.

2.12. Harmadik felek kezelése

Az NTT DATA elszámoltatható a személyes adatokat a nevünkben alfeldolgozóként működők tevékenységéért. A kiválasztáskor és azt követően rendszeresen értékeljük, hogy az adatfeldolgozók és alfeldolgozók képesek-e a személyes adatoknak az NTT DATA szabványainak megfelelő védelmére.

Az NTT DATA adatfeldolgozói és alfeldolgozói kötelesek olyan megállapodások aláírására, amelyek a személyes adatok feldolgozását és védelmét megfelelően szabályozzák. Ezek a megállapodások olyan követelményeket tartalmaznak, amelyek biztosítják, hogy ugyanezek a kötelezettségek a személyes adatokat esetleg feldolgozó más adatfeldolgozókra is vonatkozzanak.



Információbiztonsági intézkedések

Az NTT DATA elkötelezett amellett, hogy a személyes adatok bizalmas jellegének, integritásának és rendelkezésre állásának védelme érdekében információbiztonságot valósítson meg és azt megfelelően kezelje.

Az NTT DATA megfelelő irányelveket, folyamatokat, eljárásokat, szabványokat és iránymutatásokat hozott létre az általa feldolgozott adatok biztonságának biztosítása érdekében. Az NTT DATA biztonsági módszerei az ISO 27001 és egyéb iparági bevált gyakorlatok szabványaihoz igazodnak.

3.1. Információbiztonsági szerepek és felelősségi körök

Az információbiztonsággal kapcsolatos szerepeket és felelősségi köröket, beleértve az információbiztonsági vezetőt és a szervezeten belüli információbiztonsági felelősöket, hivatalosan kijelöltük, és ezen szereplők a funkciók függetlenségét biztosító jelentéstételi útvonalak betartására kötelezettek.

Az NTT DATA munkavállalói felelősek azért, hogy mindennapi üzleti tevékenységeik során az információbiztonsági irányelveinkkel, folyamatainkkal, szabványainkkal és iránymutatásainkkal összhangban járjanak el.

3.2. Információbiztonsági irányelvek

Az NTT DATA számos információbiztonsági irányelvet dokumentált és tett közzé. Ezeket az irányelveket és az ezeket alátámasztó dokumentációt rendszeresen felülvizsgáljuk.

3.3. Mobil készülékek kezelése

Az NTT DATA a “Zero Trust” biztonsági keretrendszert alkalmazza az NTT DATA rendszereihez és információs vagyonelemeihez való hozzáférésekhez és interakciókhoz kapcsolódó védelmi intézkedéseinek megvalósítására és fenntartására:

- Végfelhasználói eszközkezelési (EDM) irányelvek és támogató eljárások.
- Ellenőrzések és eszközök a biztonság fenntartásához.
- A vállalati adatok bizalmas jellege, rendelkezésre állása és integritása. Ezek az adatok a végponti felhasználói eszközökön (beleértve a mobiltelefonokat, táblagépeket és a távoli hozzáférést lehetővé tevő eszközöket) tárolhatók, vagy azokon keresztül hozzáférhetők.

3.4. Emberi erőforrások

Az NTT DATA a vonatkozó jogszabályok által megengedett mértékben háttér- és foglalkoztatási szűrést végez munkavállalói esetében, hogy ellenőrizze alkalmasságukat mind a felvételük tekintetében, mind a vállalati és ügyféladatok (beleértve a személyes adatokat is) kezelése vonatkozásában. A szűrés mértéke arányos az üzleti követelményekkel és azon információk osztályozásával, amelyekhez a munkavállaló hozzáférhet.

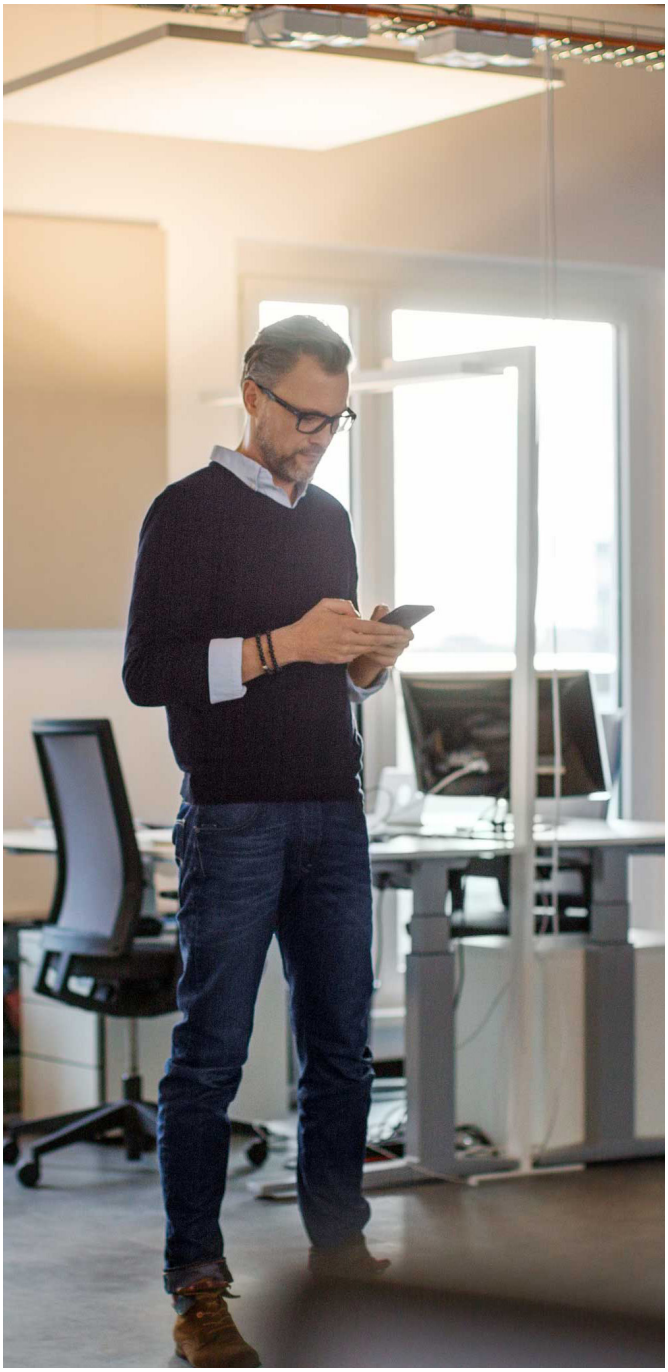
Az NTT DATA megköveteli minden munkavállalótól (beleértve a szerződéses és ideiglenes foglalkoztatottat is), hogy vállalja a vállalati és ügyféladatok (beleértve a személyes adatokat is) bizalmas kezelését.

Az NTT DATA alkalmazottai kötelesek elvégezni az információbiztonsági tudatosságra vonatkozó képzést és az időszakos ismétlő képzéseket. Az információbiztonsági irányelvek és az azokat támogató eljárások, folyamatok és iránymutatások a munkavállalók rendelkezésére állnak. Az alkalmazottak releváns információkat kapnak a trendekről, fenyegetésekről és a bevált gyakorlatról is. A tudatosság folyamatos biztosítása érdekében rendszeres időközönként biztonságtudatossági kampányokat is szervezünk.

3.5. Elfogadható használat

Az NTT DATA létrehozott olyan irányelveket, amelyek az információs vagyonelemeink megfelelő és hatékony használatát támogatják, idetartoznak a számítógépes és távközlési erőforrások, termékek, szolgáltatások, megoldások és informatikai infrastruktúra.

Az NTT DATA olyan információosztályozási irányelveket hozott létre, amelyek az információk kezelésének, azok minősítése alapján történő megfelelő ellenőrzését támogatják. Az információkat és a vagyonelemeket az osztályozási címkének megfelelően kell védeni.



“Az NTT DATA biztonsági módszerei az ISO 27001 és egyéb iparági bevált gyakorlatok szabványaihoz igazodnak.”

3.6. Hozzáférés kezelése

Az NTT DATA hozzáférés-kezelési irányelveket, támogató eljárásokat, valamint logikai és fizikai hozzáférési intézkedéseket hozott létre annak biztosítása érdekében, hogy a legkisebb jogosultság elve alapján, csak az arra jogosult személyek férjenek hozzá az információkhoz.

Adott esetben az NTT DATA az iparági szabványoknak megfelelő titkosítást alkalmaz nyugalmi állapotban és szállítás közben, hogy biztosítsa a személyes adatok védelmét a jogosulatlan hozzáféréssel vagy közzététellel szemben.

Rendszeresen végzünk hozzáférési felülvizsgálatokat annak biztosítása érdekében, hogy csak az arra jogosult személyek férjenek hozzá az NTT DATA rendszereihez és információs vagyonelemeihez.

Az NTT DATA ésszerű erőfeszítéseket tett annak érdekében, hogy korlátozza azon felhasználók számát, akik kiemelt hozzáféréssel rendelkeznek az NTT DATA rendszereihez és információs vagyonelemeihez.

Az NTT DATA nem engedélyezi a fiókok vagy hitelesítő adatok megosztását, kivéve, ha azt a vonatkozó kivételkezelési folyamaton során jóváhagyták.

3.7. Vagyonelemek kezelése és osztályozása

Az NTT DATA olyan irányelveket hozott létre, amelyek szabályozzák a fizikai és információs vagyonelemek osztályozását és kezelését, beleértve ezek biztonságos megsemmisítését is, annak érdekében, hogy az információk megfelelő szintű védelme biztosított legyen.

A bizalmas jellegre vonatkozó követelmények a vagyonelemek üzleti kritikussága alapján kerülnek meghatározásra. A személyes adatok kezelésére vonatkozó ágazati iránymutatások biztosítják a technikai, szervezési és fizikai garanciák keretét. Ezek a garanciák magukban foglalhatnak olyan kontrollokat, mint a hozzáférés kezelése, titkosítás, naplózás és nyomon követés, valamint az adatok megsemmisítése.

3.8. Fizikai és környezeti biztonság

Az NTT DATA a fizikai biztonsági irányelveivel összhangban ésszerű és megfelelő intézkedéseket hajtott végre, annak érdekében, hogy megakadályozza az információkhoz, alkalmazásokhoz, rendszerekhez, adatbázisokhoz és infrastruktúrához való jogosulatlan fizikai hozzáférést, illetve azok károsodását vagy megzavarását. Ide tartoznak:

- Fizikai hozzáférés kezelése
- Fizikai hozzáférés nyomon követése és auditálása
- Környezeti veszélyek elleni védelem
- Fizikai eszközök biztosítása
- Fizikai eszközök kezelése
- Fizikai eszközök karbantartása és eltávolítása
- Tiszta asztal és képernyő gyakorlata
- Látogatók hozzáférése és felügyelete

3.9. A működés biztonsága

Az NTT DATA az információs rendszereinek és infrastruktúrájának kezelésére és védelmére megfelelő szakértői csoportokat hozott létre.

Az NTT DATA szabályzatokat és támogató eljárásokat hozott létre az üzleti folyamatok, az információs rendszerek és az infrastruktúra változásainak kezelésére. Az NTT DATA többféle irányítási struktúrát hozott létre a változások felülvizsgálatára és jóváhagyására a változás mérete és terjedelme, valamint a stratégiai célok alapján. Minden kérelmet és azok eredményeit naplózzuk és dokumentáljuk.

Az NTT DATA iparági szabványos eszközökkel támogatott fenyegetés- és sérülékenység-kezelési programokat hozott létre a vállalati információkat, köztük a munkavállalókat és az ügyfelek személyes adatait érintő kockázatok azonosítására, kezelésére és csökkentésére. Ez magában foglalja a legkorszerűbb végponti észlelést és reagálást (EDR) a vírusirtó és rosszindulatú szoftverek elleni eszközök számára, a környezetek rendszeres vizsgálatát, a javítási protokollokat, valamint a javítási és fejlesztési tevékenységek irányítását.

A kapacitásigényeket folyamatosan nyomon követjük és rendszeresen felülvizsgáljuk. A rendszereket és hálózatokat e felülvizsgálatoknak megfelelően kezeljük és méretezzük.

A rendszer rendelkezésre állása magában foglalja az architektúrát, valamint az egyes rendszerekre vonatkozó kockázati és rendelkezésre állási követelmények alapján a magas rendelkezésre állásra hivatott tervezést, a katasztrófa utáni helyreállítást és/vagy a biztonsági mentéseket. A rendszer rendelkezésre állásának vagy helyreállításának módszerét, beleértve a biztonsági mentések terjedelmét és gyakoriságát, az NTT DATA üzleti követelményei – beleértve az ügyfél elvárásait, valamint az információ kritikusságát is – határozzák meg. A katasztrófa utáni helyreállítási terveket rendszeresen teszteljük. A biztonsági mentési folyamatok felügyelete biztosítja a biztonsági mentések sikeres teljesítését, valamint a biztonsági mentési problémák, kivételek vagy hibák kezelését.

Az NTT DATA ésszerű erőfeszítéseket tesz az alkalmazások és rendszerek audit naplózásának fenntartására. A naplókat rendszeresen felülvizsgáljuk, és azok vizsgálati célokra rendelkezésre állnak. A naplókhoz való hozzáférés szigorúan csak az arra felhatalmazott személyzetre korlátozódik.

3.10. A rendszer beszerzése, fejlesztése és karbantartása

Az NTT DATA a “Zero Trust” biztonsági keretrendszert alkalmazza az NTT DATA rendszereihez és információs vagyonelemeihez való hozzáférésekhez és interakciókhoz kapcsolódó védelmi intézkedéseinek megvalósítására és fenntartására.

Az architektúra- és tervezési irányelvek, valamint a támogató szabványok és eljárások biztosítják, hogy a tervezésen alapuló biztonság elveit a szoftverfejlesztés életciklusa során alkalmazzuk.

3.11. Harmadik felek kezelése

Az NTT DATA a harmadik felek kezelésére vonatkozó irányelveket és gyakorlatot hozott létre annak érdekében, hogy biztosítsa az információs vagyonelemek védelmét, akkor, amikor az NTT DATA harmadik fél szolgáltatókat és/vagy adatfeldolgozókat vesz igénybe. Ezek között szerepelnek az információbiztonsági átvilágításra és az információbiztonsági kockázatértékelésre vonatkozó követelmények, amelyekkel biztosítani kell:

- az információbiztonsági követelményeknek a megállapodásokban történő, az NTT DATA információbiztonsági szabványainak megfelelő világos megfogalmazását és dokumentálását,
- az NTT DATA szolgáltatók és adatfeldolgozók általi, az NTT DATA-val azonos szintű védelem és ellenőrzés alkalmazását,
- a szolgáltatók és adatfeldolgozók általi, minden feltételezett vagy tényleges információbiztonsági incidens NTT DATA felé időben történő bejelentését.

3.12. Információbiztonsági eseménykezelés

Az NTT DATA rendelkezik azokkal az irányelvekkel, folyamatokkal és eljárásokkal, amelyek az információbiztonsági események – ideértve a személyes adatok megsértését – azonosítására, felderítésére, az azokra való reagálásra és az azokból való helyreállításra, valamint az ilyen események esetén a megfelelő érdekelt felek felé történő bejelentére vonatkoznak. Ezek között szerepelnek a kiváltó okok elemzésének elvégzésére és a korrekciós intézkedések megtételére szolgáló mechanizmusok, amelyek célja az orvoslás és az újabb előfordulás megelőzése.

Az NTT DATA az egész vállalatra kiterjedő biztonsági műveleteket hozott létre az összes hálózati és számítástechnikai eszköz proaktív nyomon követése és kezelése érdekében. Ezeket a műveleteket az információbiztonsági eseményekre való reagálás és helyreállítás technikai eszközei támogatják.

3.13. Üzletmenet-folytonosság

Az NTT DATA rendelkezik üzletmenet-folytonossági és katasztrófa-helyreállítási tervekkel. Az NTT DATA a rendszerek és adatok rendelkezésre állásának biztosítása érdekében többszintű megközelítést alkalmaz az üzletmenet-folytonosság terén.

3.14. Megfelelés

Az NTT DATA meghatározta az üzleti tevékenységünket érintő jogszabályok és előírások azonosítására vonatkozó szerepeket és felelősségi köröket. A jogszabályoknak és előírásoknak való megfelelésért csoport- és regionális szinten állapítottuk meg a felelősségi köröket annak biztosítása érdekében, hogy az NTT DATA megfeleljen a globális és helyi követelményeknek.


NTT DATA