BINDING CORPORATE RULES PRIVACY (BCRP)

KÖTELEZŐ EREJŰ VÁLLALATI SZABÁLYOK A SZEMÉLYISÉGI JOGOK VÉDELMÉRE A DEUTSCHE TELEKOM CÉGCSOPORTON BELÜLI ADATKEZELÉS FOLYAMÁN

Deutsche Telekom AG, Group Privacy

Verziószám: 3.0 végleges
Felülvizsgálat dátuma: 2023. december 29.
Nyilvános

Connecting your world.

Copyright © Error! Reference source not found. Error! Reference source not found., Error! Reference source not found.
Minden jog fenntartva, beleértve kivonatolt részek újranyomtatását, a fotomechanikus sokszorosítást (többek között a mikrofilmre másolást), valamint az adatbázisokban és hasonló rendszerekben történő felhasználás jogát is.

Kiadás részletei

Kiadta

Deutsche Telekom AG
Group Privacy
Friedrich-Ebert-Allee 140, 53113 Bonn, Germany

File név	Dokumentum szám	Dukumentum név
[Binding Corporate Rules Privacy DTAG.docx]	[2.9]	[Binding Corporate Rules Privacy]

Verzió	Utolsó felülvizsgálat	Állapot
3.0 final	29.12.2023	

Szerkesztő	Tartalom felülvizsgálva	Elfogadta
Dr. Jörg Friedrichs	Jan Lichtenberg, Strategy & Steering	Dr. Claus-Dieter Ulmer, Group Privacy Officer
Bonn, 27.10.2023	[Bonn, 30.102023]	[Bonn, 31.10.2023]

Rövid összefoglaló
Szabályzat vállalatcsoporton belüli személyes adatok kezeléséről

Változások

Verzió	Utolsó felülvizsgálat	Szerkesztette	Változások/megjegyzések
2.2	20.01.2013	Sonjy Klauck	Az adatvédelmi magatartási kódex felülvizsgált változata, német nyelvű, 2.1-es verzió
2.3	08.02.2013	Dr. Claus-Dieter Ulmer	Teljes átdolgozás
2.4	14.02.2013	Dr. Claus-Dieter Ulmer	Adattovábbítás és felelősség
2.5	21.03.2013	Marcus Schmitz Dr. Claus-Dieter Ulmer	Felülvizsgálat a német adatvédelemért és információszabadságért felelős szövetségi biztos megjegyzéseivel
2.6	09.04.2013	Daniel Hoff	Felülvizsgálat a német adatvédelemért és információszabadságért felelős szövetségi biztos megjegyzéseivel
2.7	05.12.2013	Daniel Hoff Marcus Schmitz	Felülvizsgálat az osztrák adatvédelmi hatóság megjegyzéseivel
2.8	19.02.2019	Dr. Jörg Friedrichs Christina Kreft-Spallek	Az általános adatvédelmi rendelethez való igazodás a WP 256 rev.01 alapján
3.0	29.12.2023	Dr. Jörg Friedrichs	Az 1/2022. számú ajánláshoz való igazodás a jóváhagyási kérelemről, valamint az adatkezelői kötelező érvényű vállalati szabályok elemeiről és elveiről (GDPR 47. cikk)

Megjegyzés: Előfordulhat, hogy a Cégcsoport jelen szabályzata kinyomtatott formájában a megtekintés pillanatában már elavult. Kérjük, mindig ellenőrizze a Deutsche Telekom AG Corporate Rule Base oldalán (http://policies.telekom.de), hogy a Cégcsoport Szabályzatának aktuális verziójával rendelkezik-e.

Tartalomjegyzék

Bevezetés

(1) Az ügyfelek, alkalmazottak és a Deutsche Telekom Cégcsoporttal kapcsolatban lévő egyéb személyek személyes adatainak védelme kiemelt fontosságú a Deutsche Telekom Cégcsoport összes vállalata számára.

(2) A Deutsche Telekom Cégcsoport vállalatai számára nyilvánvaló, hogy a Deutsche Telekom Cégcsoport egészének sikere nem csak az információáramlás globális hálózatának, hanem a személyes adatok megbízható és biztonságos kezelésének is függvénye.

(3) Számos területen a Deutsche Telekom Cégcsoport egyetlen egységnek látszik, elsősorban az ügyfelei és a nyilvánosság számára. Éppen ezért a Deutsche Telekom Cégcsoport vállalatainak közös feladata, hogy a jelen Binding Corporate Rules Privacy Szabályzat alkalmazásával hozzájáruljanak a vállalat közös sikeréhez, és támogassák a Deutsche Telekom Cégcsoport azon törekvését, hogy jó minőségi termékeket és innovatív szolgáltatásokat nyújtson.

(4) A Deutsche Telekom Cégcsoport jelen Binding Corporate Rules Privacy Szabályzatának célja az, hogy egységes, magas szintű, globális adatvédelmi rendszert hozzon létre a személyes adatoknak az egyes vállalatokon belüli és a vállalatok közötti kezelésére, illetve a Németországon belüli, illetve nemzetközi adatátvitelre. A Deutsche Telekom Cégcsoporton belül a fogadó félnek a megkapott személyes adatokat a küldő félre érvényes adatvédelmi jogszabályi előírásoknak megfelelően kell feldolgoznia.

Első rész
Hatály

1. § A Binding Corporate Rules Privacy szabályzat jogi természete

A Binding Corporate Rules Privacy szabályzat kötelező érvényű a személyes adatok feldolgozása (az Európai Adatvédelmi Testület 1/2022 munkaanyag értelmezése szerint) a Deutsche Telekom Cégcsoport összes olyan vállalatára nézve, amelyek azt kötelező érvénnyel elfogadták.

2. § Felhasználási terület

A Binding Corporate Rules Privacy szabályzat az adatgyűjtés helyétől függetlenül alkalmazandó a Deutsche Telekom Cégcsoporton belül az összes típusú személyes adat kezelésére. A személyes adatok kezelése a Deutsche Telekom Cégcsoporton belül konkrétan a következő célokra történhet:

a) Alkalmazottak adatainak kezelése a munkaszerződések megkötése, végrehajtása és feldolgozása során, valamint az alkalmazottak megkeresésére a Deutsche Telekom Cégcsoport vagy harmadik fél által számukra kínált termékek és szolgáltatások kapcsán.

b) Üzleti ügyfelek és fogyasztók szerződéseinek megkötése, végrehajtása és feldolgozása, valamint a Deutsche Telekom Cégcsoport vagy harmadik felek (értelemszerűen) által kínált termékekkel és szolgáltatásokkal kapcsolatban ügyfelek és érdeklődő harmadik felek tájékoztatására szolgáló hirdetési és piackutatási tevékenységek végrehajtása.

c) Szerződések megkötése és végrehajtása a Deutsche Telekom Cégcsoport szolgáltatóival a Deutsche Telekom Cégcsoport által nyújtott szolgáltatások részeként.

d) Más külső felek – speciálisan részvényesek, partnerek vagy látogatók – megfelelő kezelésének lehetővé tétele, a kötelező erejű jogi szabályozások betartása.

Az adatok kezelésének a Deutsche Telekom Cégcsoport vállalatainak aktuális és jövőbeli üzleti céljaival összhangban kell történnie. Ilyen cél többek között a távközlési szolgáltatások, digitális szolgáltatások nyújtása fogyasztók és üzleti ügyfelek számára, informatikai (például adatközponti) és tanácsadási szolgáltatások nyújtása.

3. § Kapcsolódás más jogi rendelkezésekhez

(1) A Binding Corporate Rules Privacy rendelkezéseinek kialakítása úgy történt, hogy a személyes adatok védelmét magas szinten és standard módon biztosítsák a Deutsche Telekom Cégcsoport egészében. A személyes adatok feldolgozása tekintetében az egyes vállalatok számára a jelen Binding Corporate Rules Privacy szabályzatban meghatározott elveken túlmenő, a betartandó, illetve további megkötéseket tartalmazó jogi kötelezettségeket és előírásokat a jelen szabályzat nem befolyásolja.

(2) Az Európai Gazdasági Térségben gyűjtött adatokat általánosságban az adatkezelés helyétől függetlenül annak az országnak a jogi előírásainak megfelelően kell kezelni, ahol az adatok gyűjtése történt, minimális követelményként a jelen Binding Corporate Rules Privacy szabályzat követelményeit kell teljesíteni.

(3) Az állambiztonsági, nemzetvédelmi vagy közbiztonsági okokból, bűncselekmények megelőzése és kiderítése, illetve a bűnözők elleni vádemelés céljából nemzeti szinten megalkotott jogszabályok alkalmazandó voltát a jelen Binding Corporate Rules Privacy szabályzat rendelkezései nem befolyásolják.

(4) Amennyiben egy vállalat számára kiderül, hogy jelen Szabályzat jelentős fejezetei, részei ellenkeznek a nemzeti adatvédelmi rendelkezésekkel, és ez megakadályozza, hogy a felek betartsák a jelen Szabályzatot, haladéktalanul értesíteni kell a Deutsche Telekom Cégcsoport csoportszintű adatvédelmi tisztviselőjét. A vállalat illetékes felügyeleti hatóságát közvetítői minőségben be kell vonni.

4. § Lejárat és megszűnés

A jelen Binding Corporate Rules Privacy szabályzat megszűnik kötelező erejűnek lenni egy vállalatra nézve, ha az adott vállalat már nem a Deutsche Telekom Cégcsoport tagja, illetve ha érvényteleníti a jelen Szabályzatot. Ugyanakkor a Binding Corporate Rules Privacy érvényességének megszűnése vagy érvénytelenítése nem mentesíti a vállalatot a már átvitt adatok kezelését szabályozó Binding Corporate Rules Privacy kötelezettségei és/vagy rendelkezései alól. Az ilyen vállalathoz vagy vállalattól további adatátvitelre abban az esetben kerülhet sor, ha az európai jog követelményeinek megfelelő egyéb megfelelő eljárási garanciákat biztosít.

Második rész
Alapelvek

1. szakasz
Az adatkezelés átláthatósága

5. § Tájékoztatási kötelezettség

Az érintetteket a vonatkozó jogszabályoknak és a következő feltételeknek megfelelően tájékoztatni kell arról, hogyan történik személyes adataik kezelése.

6. § A tájékoztatás tartalmi és formai jellemzői

(1) A vállalat az érintetteket köteles megfelelő módon tájékoztatni a következőkről:

a) az adatkezelő(k) személye és elérhetősége.

b) az adatvédelmi tisztviselő elérhetőségei

c) az adatok kezelésének céljai; valamint az adatkezelés jogalapja időtartama.

d) Amennyiben harmadik félnek átadnak vagy továbbítanak személyes adatokat, a fogadó fél, valamint az ilyen jellegű átadás/továbbítás hatásköre és célja (vagy céljai).

e) törvényes jogaik.

(2) Az érintetteknek ezt a tájékoztatást a választott kommunikációs médiumtól függetlenül világos és könnyen érthető módon kell biztosítani.

7. § A tájékoztatás elérhetősége

Az érintettek számára az adatok első begyűjtésekor, valamint azt követően kérésükre bármikor tájékoztatást kell nyújtani.

8.§ Adatkezelési tevékenységek nyilvántartása

A vállalatok az általuk végzett adatkezelési tevékenységekről (ideértve az adatfeldolgozási tevékenységet is) nyilvántartást vezetnek. A nyilvántartásnak a következő információkat kell tartalmaznia:

a) a vállalatnak, a vállalat képviselőjének és adatvédelmi tisztviselőjének (DPO-jánakÖ neve és kontakt adatatai;

b) az adatkezelési tevékenységek kategóriáinak és az adatkezelés céljának leírása;

c) a címzettek és harmadik felek kategóriái akik számára az adatokat továbbítják vagy akikkel az adatokat közlik;

d) a harmadik országok megnevezése és a megfelelő biztosítékok dokumentációja ha a jelen Binding Corporate Rules nem alkalmazható;

e) ahol lehetséges, a törlésre előírt határidők, és

f) ahol lehetséges, a technikai és szervezeti biztonsági intézkedések általános leírása.

2. szakasz
A személyes adatok kezelésének elfogadhatósága

9. § Alapelv

Személyes adatokat csak az alábbi feltételek teljesülése mellett lehet kezelni, és kizárólag az adatgyűjtés eredeti céljának megfelelően.

A gyűjtött adatok egyéb célra történő kezelése csak abban az esetben megengedhető, ha az alábbi követelményeknek megfelelően az elfogadhatóság feltételei megvalósulnak (célhoz kötöttség).

10. § A személyes adatok kezelésének jogszerűsége

Személyes adatok a következő feltételek legalább egyikének teljesülése esetén kezelhetők:

a) Az adatok kezelése a szándéknak megfelelő módon jogilag egyértelműen elfogadható.

b) Az érintett hozzájárult adatainak kezeléséhez.

c) A vállalat számára az adatok ilyen módon történő kezelése szükséges ahhoz, hogy az érintettel meglévő szerződésének értelmében létrejött kötelezettségeit teljesíteni tudja, ideértve szerződéses tájékoztatási kötelezettségének és/vagy másodlagos kötelezettségeinek teljesítését is. Illetve ahhoz, hogy a vállalat az érintett által igényelt szerződés megkötéséhez vagy feldolgozásához szükséges szerződéskötés előtti vagy utáni intézkedéseket végre tudja hajtani.

d) Az adatkezelésre a vállalat jogi kötelezettségének teljesítése érdekében kerül sor.

e) Az adatok kezelése az érintett létfontosságú érdekeinek védelmében szükséges.

f) Az adatok kezelése közérdekű feladat végrehajtásához szükséges, illetve olyan közfeladat végrehajtásának részét képezi, amellyel a vállalatot vagy az olyan harmadik felet bíztak meg, aki az átvitt adatokat megkapja.

g) Az adatok kezelése az adatátvitelt fogadó vállalat vagy harmadik fél/felek jogos érdekeinek megvalósításához szükséges, feltéve, hogy ezeket az érdekeket nem sértik az érintett jogos érdekeit.

11. § Az érintett hozzájárulása

A Binding Corporate Rules Privacy szabályzat 10. § (1), b) bekezdése értelmében a következő feltételek teljesülése esetén úgy kell tekinteni, hogy az érintett hozzájárulását megadta:

a. Megfelelő tájékoztatást követően, mely az adatkezelés alanya számára pontosan megjelöli, hogy mihez adja a hozzájárulását, az érintett kifejezett, önkéntes beleegyezése szükséges. A hozzájárulásról szóló nyilatkozat szövegének pontosnak, világosnak kell lennie, és az érintettet tájékoztatnia kell arról, hogy bármikor joga van visszavonni a hozzájárulását. Olyan üzleti modellek esetében, amelyeknél a visszavonás szerződéses kötelezettségek nem teljesítéséhez vezet, az érintettet tájékoztatni kell.

b) A hozzájárulást a körülményeknek megfelelő formában (írásban) kell beszerezni. A hozzájárulást kivételes esetben szóban is meg lehet szerezni, amennyiben a hozzájárulás tényét, illetve a szóbeli hozzájárulás elégséges voltát indokoló körülményeket megfelelő módon dokumentálják.

12. § Automatizált egyedi döntések, a profilalkotást is ideértve

(1) Az adatkezelésben érintett személyek tulajdonságait értékelő (profilalkotás), illetve számukra jogi következményekkel vagy komoly hátránnyal járó döntéseket nem lehet kizárólagosan automatizált adatkezelésre alapozni. Ide tartoznak az olyan döntések,

amelyek meghozatalához fontosak az adatkezelés alanyának hitelképességével, szakmai megfelelőségével vagy egészségi állapotával kapcsolatos adatok.

(2) Ha egyedi esetekben objektív módon automatizált döntéshozatalra van szükség, az adatkezelés alanyát haladéktalanul értesíteni kell az automatizált döntés eredményéről és lehetőséget kell neki adni arra, hogy azt megfelelő időn belül észrevételezze. Az érintett észrevételeit megfelelő módon figyelembe kell venni a végső döntés meghozatala előtt.

13. § Személyes adatkezelés direkt marketing célokra

Amennyiben az adatok kezelése direkt marketing céljára történik, az érintetteknek:

a) tájékoztatást kell kapniuk arról, hogy adataikat milyen módon használják fel direkt marketing céljára;

b) tájékoztatást kell kapniuk arról, hogy bármikor joguk van tiltakozni személyes adataik direkt marketing kommunikációban történő kezelése ellen;

c) megfelelő eszközöket kell kapniuk, hogy a kommunikáció visszautasításához való jogukat gyakorolják. Tájékoztatást kell kapniuk elsősorban arról a vállalatról, amelynél tiltakozni tudnak.

14. § Személyes adatok különleges kategóriái

(1) A különleges adatok kezeléséhez kifejezett jogi felhatalmazás, vagy az adatkezelés alanyának előzetes és kifejezett hozzájárulása szükséges. Különleges adat akkor is kezelhető, ha az munkajogi szempontból a felelős szervezet jogainak és kötelezettségeinek gyakorlása céljából szükséges, ennek azonban a megfelelő garanciákat biztosító nemzeti törvények alapján kell történnie.

(2) Az ilyen adatgyűjtés, -feldolgozás vagy kezelés megkezdése előtt az összes szükséges esetben írásban kell konzultálni a kérdéses vállalat Adatvédelmi Tisztviselőjével és dokumentálni az adatfelhasználást. Az elfogadhatóság kiértékelésekor különös figyelmet kell fordítani az adatfelhasználás jellegére, hatáskörére, céljára, szükségességére és jogalapjára.

15. § Adat minimalizálás, az adatelkerülés, anonomizálás korlátozott tárolhatóság és álnevesítés

(1) A személyes adatoknak megfelelőeknek, relevánsaknak és nem túlzó mértékűnek kell lenniük az adatok adott célra történő felhasználása tekintetében (az adatok minimalizálása). Az adatot csak egy adott alkalmazáshoz lehet felhasználni, amikor arra szükség van (adatelkerülés).). Az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (korlátozott tárolhatóság).

(2) Ahol lehetséges és gazdaságilag ésszerű, eljárásokat kell alkalmazni az érintetteket azonosító jellemzők törlésére (anonimizálás) vagy azok egyéb jellemzőkkel való helyettesítésére (álnevesítés).

16. § Büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó adatok kezelése

Az Európai Gazdasági Térség területén gyűjtött, büntetőjogi felelősség megállapításával és bűncselekményekkel vagy a Kötelező Erejű Vállalati Adatvédelmi Szabályok 10. szakasza alapján kapcsolódó biztonsági intézkedésekkel összefüggő személyes adatok feldolgozása kizárólag hatósági felügyelet mellett történhet, illetve akkor, ha az adatkezelést az érintettek jogainak és szabadságainak megfelelő garanciáit biztosító uniós vagy tagállami jog engedélyezi. A büntetőjogi felelősség megállapítására vonatkozó átfogó nyilvántartás kizárólag hatósági felügyelet mellett vezethető.

17. § Az árukapcsolás tilalma

A termékek és/vagy szolgáltatások igénybevételének, az azokhoz való hozzájutásnak nem lehet feltétele az adatkezelés alanyának az adatok más célra történő felhasználásához való hozzájárulása. Az adatok csak egy szerződéses viszony kezdeményezéséhez vagy teljesítéséhez használhatóak fel. Árukapcsolás csak akkor alkalmazható, ha az érintett egyáltalán nem, vagy az ésszerűség határain belül nem tud hasonló szolgáltatást igénybe venni vagy hasonló terméket megvásárolni.

3. szakasz
Személyes adatok továbbítása

18. § A személyes adatok továbbításának jellege és célja

(1) A személyes adatok továbbítása abban az esetben történhet, ha a címzett meghatározza az adatkezelés céljait és eszközeit, vagy ha a címzett kizárólag az adatkezelő nevében kezeli az adatokat.
(2) A személyes adatok kizárólag a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok 10. szakaszában foglaltak szerinti engedélyezett célokból, a vállalat üzleti tevékenysége vagy jogi kötelezettségei keretében, illetve az érintettek hozzájárulását követően továbbíthatók.
(3) Személyes adatok továbbítására kizárólag abban az esetben kerülhet sor, ha az adatok továbbítását megelőzően a megfelelő adatvédelmi és adatbiztonsági követelményekről megállapodás jött létre a címzett féllel.

19. § Az adatok továbbítása, beleértve az újbóli továbbítást is

(1) Személyes adatok, amelyek az Európai Gazdasági Térség területén kerültek összegyűjtésre, kizárólag akkor továbbíthatók harmadik országbeli adatkezelőknek vagy adatfeldolgozóknak, ha a Kötelező Erejű Vállalati Adatvédelmi Szabályok vagy más megfelelő adatvédelmi biztosítékok alkalmazásával biztosított a megfelelő szintű adatvédelem, mint például az uniós általános szerződési feltételek vagy egyedi szerződéses megállapodások, amelyek az európai jog vonatkozó követelményeinek megfelelnek, és hogy az érintettek számára a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok 5. része értelmében végrehajtható érintettek jogai és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

(2) Ez magában foglalja azt is, hogy a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok kizárólag abban az esetben használhatóak továbbítási eszközként a továbbítás hatásvizsgálatát követően, ha a vállalat úgy értékelte, hogy a célország harmadik országának a személyes adatok címzett általi feldolgozására alkalmazandó joga és gyakorlata nem akadályozza a címzettet abban, hogy teljesítse a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok szerinti kötelezettségeit. A felülvizsgálat során az állami hatóságok számára a személyes adatok nyilvánosságra hozatalára vonatkozó követelményeket vagy a hozzáférést engedélyező intézkedéseket is figyelembe kell venni. Ez vonatkozik az Európai Gazdasági Térségen kívüli vállalatoknak továbbított valamennyi személyes adatra, valamint a harmadik országbeli vállalatoktól ugyanazon vagy más harmadik országbeli vállalatoknak történő újbóli továbbításra.

(3) A személyes adatokat továbbító vállalat köteles felfüggeszteni az adattovábbítást, ha úgy ítéli meg, hogy a kötelező erejű vállalati szabályok nem teljesíthetők, vagy ha az illetékes felügyeleti hatóság erre utasítja. A vállalat köteles az adattovábbítást vagy az adattovábbítások sorozatát megszüntetni, ha a Kötelező erejű Vállalati Adatvédelmi

Szabályok betartása a felfüggesztést követő egy hónapon belül nem kerül helyreállításra. Ebben az esetben a felfüggesztést megelőzően továbbított személyes adatokat és azok másolatait a személyes adatokat továbbító vállalat választása szerint vissza kell szolgáltatni vagy teljes egészében meg kell semmisíteni.

(4) A Deutsche Telekom Csoport követelményei és az általánosan elismert technikai és szervezési szabványok alapján a személyes adatok biztonságának garantálása érdekében - beleértve a személyes adatok más félnek történő továbbítását is - megfelelő technikai és szervezési intézkedésekre van szükség.

20. § A címzett kötelezettségei hatóságok általi hozzáférés esetén

(1) A címzett kötelezettséget vállal arra, hogy haladéktalanul értesíti a személyes adatok továbbítását végző vállalatot, amennyiben:

a) a célország jogszabályai szerinti hatóságtól, beleértve az igazságügyi hatóságokat is, jogilag kötelező erejű megkeresést kap a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok alapján továbbított személyes adatok nyilvánosságra hozatalára vonatkozóan; az értesítésnek tartalmaznia kell a kért személyes adatokra, a megkereső hatóságra, a megkeresés jogalapjára és a válaszra vonatkozó információkat; vagy

b) tudomást szerez a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok alapján továbbított személyes adatokhoz való közvetlen hatósági hozzáférésről a célország jogszabályaival összhangban; az értesítésnek tartalmaznia kell a címzett számára rendelkezésre álló valamennyi információt.

(2) Abban az esetben, ha a címzett a célország jogszabályai értelmében nem jogosult a személyes adatokat továbbító vállalatot értesíteni, a címzett vállalja, hogy a lehető leghamarabb minden tőle telhetőt megtesz a korlátozás alóli felmentés megszerzése érdekében, a lehető legtöbb információ közlése érdekében. A címzett vállalja, hogy minden erőfeszítését dokumentálja annak érdekében, hogy a személyes adatokat továbbító vállalat kérésére bizonyítani tudja azokat.

(3) Amennyiben a rendeltetési ország jogszabályai lehetővé teszik, a címzett vállalja, hogy a szerződés időtartama alatt a személyes adatokat továbbító vállalatnak rendszeres időközönként a lehető legtöbb lényeges információt közli a beérkezett kérelmekről (különösen a kérelmek száma, a kért adatok típusa, a kérelmező hatóság/hatóságok, a kérelmek megtámadása és a megtámadás eredménye stb.)

(4) A címzett vállalja, hogy az (1)-(3) bekezdés szerinti információkat a szerződés időtartama alatt megőrzi, és kérésre az illetékes felügyeleti hatóság rendelkezésére bocsátja.

(5) Az (1)-(3) bekezdések alkalmazása nem érinti az átvevő azon kötelezettségét, hogy haladéktalanul tájékoztassa a személyes adatokat továbbító vállalatot, ha az nem képes megfelelni a Kötelező Erejű Vállalati Adatvédelmi Szabályoknak.

(6) A címzett vállalja, hogy a közlésre irányuló kérelem jogszerűségét felülvizsgálja, különösen arra vonatkozóan, hogy az a megkereső hatóság által biztosított hatáskörbe tartozik-e, és megtámadja a kérelmet, ha körültekintő vizsgálatot követően arra a következtetésre jut, hogy alapos okkal feltételezi, hogy a kérelem a célország jogszabályai, a nemzetközi jog szerinti alkalmazandó kötelezettségek és a nemzetközi udvariasság elve alapján jogellenes. A címzett ugyanilyen feltételek mellett élhet a jogorvoslati lehetőségekkel. A megkeresés megtámadása esetén a címzett ideiglenes intézkedéseket kér a megkeresés hatásainak felfüggesztése érdekében, amíg az illetékes igazságügyi hatóság érdemben nem dönt. A

címzett nem jogosult a kért személyes adatokat nyilvánosságra hozni, amíg az alkalmazandó eljárási szabályok alapján erre nem kötelezhető. Ezek a követelmények nem érintik a címzettnek a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok szerinti egyéb kötelezettségeit.

(7) A címzett vállalja, hogy dokumentálja jogi vizsgálatát és a nyilvánosságra hozatal iránti kérelemmel szembeni esetleges kifogását, valamint a célország jogszabályai által megengedett mértékben a dokumentációt a személyes adatokat továbbító vállalat rendelkezésére bocsátja. Kérésre ezeket az illetékes felügyeleti hatóság rendelkezésére bocsátja.

(8) A címzett vállalja, hogy a közlésre irányuló kérelemre adott válaszában a kérelem ésszerű értelmezése alapján a megengedett minimális mennyiségű információt adja meg.

21. § Adatkezelő nevében végzett adatfeldolgozás[1]

(1) Abban az esetben, ha egy vállalat (adatkezelő) megbíz egy harmadik felet (adatfeldolgozó), hogy utasításai szerint a nevében szolgáltatásokat nyújtson, akkor az elvégzendő munkát tartalmazó szolgáltatási megállapodáson túlmenően a megállapodásnak tartalmaznia kell az adatfeldolgozónak, mint az adatfeldolgozással megbízott félnek a kötelezettségeit is. Az említett kötelezettségek meghatározzák az adatkezelő utasításait a személyes adatok feldolgozásának típusára és módjára, az adatkezelés céljára, valamint az adatvédelemhez szükséges technikai és szervezési intézkedésekre vonatkozóan.

(2) A (megbízás teljesítése érdekében rábízott) személyes adatokat az adatfeldolgozó saját vagy harmadik fél általi feldolgozás céljából az adatkezelő előzetes hozzájárulása nélkül nem kezelheti. Az adatfeldolgozó köteles előzetesen tájékoztatni az adatkezelőt minden olyan tervéről, amely szerint a szerződéses kötelezettségeinek teljesítése érdekében a munkát más harmadik félnek kívánja alvállalkozásba adni. Az adatkezelőnek joga van kifogást emelni az alfeldolgozók ilyen jellegű igénybevétele ellen. Amennyiben az alfeldolgozók alkalmazása engedélyezett módon történik, az adatkezelő kötelezi őket az adatfeldolgozó és az adatkezelő között létrejött megállapodásokban foglalt követelmények betartására.

(3) Az adatfeldolgozóként eljáró vállalatok kötelesek indokolatlan késedelem nélkül értesíteni az adatkezelőt, miután tudomást szereztek egy incidensről.

(4) Az alfeldolgozók kiválasztása a fent említett követelmények teljesítésére való képességük alapján történik.

[1] Ez a § nem rendelkezés a 29. Európai Bizottság munkacsoportja által kibocsátott 195-ös munkaanyag értelmében

4. szakasz
Az adatok minősége és biztonsága

22. § Adatminőség

(1) A személyes adatoknak mindig pontosnak kell lenniük, és amennyiben szükséges, azokat naprakészen kell tartani (adatpontosság).

(2) Az adatkezelés célja ismeretében, megfelelő intézkedéseket kell tenni annak érdekében, hogy a helytelen vagy hiányos információk törlésre, zárolásra, illetve szükség esetén kijavításra kerüljenek.

23. § Adatbiztonság – műszaki és szervezeti óvintézkedések (beépített és alapértelmezett adatvédelem)

A vállalatnak megfelelő műszaki és szervezeti óvintézkedéseket kell tennie az adatok védelmére olyan vállalati folyamatok, informatikai rendszerek és platformok tekintetében melyeket adatok gyűjtését, feldolgozását vagy felhasználását végzi, melyek hatékonysága rendszeresen értékelésre kerül.

Ezeknek az intézkedéseknek a következőket kell tartalmazniuk:

a) jogosulatlan személyek személyes adatokat feldolgozó vagy felhasználó adatfeldolgozó rendszerekhez történő hozzáférésének megakadályozása (fizikai hozzáférés kontroll);

b) annak biztosítása, hogy az adatfeldolgozó rendszereket jogosulatlan személyek ne használhassák (használat megtagadása kontroll);

c) annak biztosítása, hogy az adatfeldolgozó rendszerekhez hozzáférő személyek csak azon adatokhoz jussanak hozzá, amelyeknek elérésére jogosultságuk van (adat hozzáférési kontroll), valamint hogy a személyes adatokat jogosulatlan személyek a feldolgozás, használat során, illetve a rögzítést követően ne tudják olvasni, másolni, módosítani vagy törölni (pl. titkosítással).

d) annak biztosítása, hogy az elektronikus átadás, szállítás vagy adathordozóra való rögzítés során a személyes adat ne legyen jogosulatlan személyek által olvasható, másolható, módosítható vagy törölhető, és hogy meg lehessen vizsgálni és ki lehessen deríteni, hogy a személyes adatot hol adták át az adatátviteli berendezés segítségével (adatátviteli kontroll);

e) annak biztosítása, hogy visszamenőleg meg lehessen vizsgálni és ki lehessen deríteni, hogy a személyes adatot ki vitte be, illetve ki módosította vagy törölte az adatfeldolgozó rendszerben (adatbeviteli kontroll);

f) annak biztosítása, hogy a vállalkozók által feldolgozott személyes adatot csak a megrendelő fél utasításainak megfelelően lehessen feldolgozni (adatfeldolgozói kontroll);

g) annak biztosítása, hogy a személyes adat védett legyen a véletlenszerű megsemmisüléssel vagy adatvesztéssel szemben (rendelkezésre állási kontroll);

h) annak biztosítása, hogy a különböző célból gyűjtött adatok feldolgozása egymástól elkülönített módon történjen (szétválasztási szabály).

Harmadik rész
Az érintettek jogai

24. § A hozzáférési jog

(1) Az érintettek jogosultak bármikor az adataikat használó bármely vállalathoz fordulni, és kérni a következőkről tájékoztatást:

a) a róluk tárolt személyes adatokról, azok forrásával és fogadó feleivel együtt;

b) az adatkezelés céljáról;

c) a címzettek, akik felé az adataikat rendszeresen továbbítják, vagy továbbították, különösképpen, ha az adattovábbítás harmadik országba történik;

d) jelen Binding Corporate Rules Privacy szabályzat rendelkezéseiről.

(2) Érthető formában, ésszerű időn belül megfelelő tájékoztatást kell adni az érintett számára. Ezt általában írásban vagy elektronikus úton kell biztosítani. Az érintettet a kérelem kézhezvételétől számított egy hónapon belül kell tájékoztatni. Ez az időtartam két további hónappal meghosszabbítható ha szükséges, a kérelem komplexitását és a kérelmek számát figyelembe véve. Erről a meghosszabbításról a kérelmezőt tájékoztatni kell. Jelen Binding Corporate Rules Privacy szabályzat nyomtatott példányának biztosítása megfelelő tájékoztatást jelent a követelményekre vonatkozóan.

(3) Amennyiben a vonatkozó nemzeti jogszabályok ezt lehetővé teszik, a vállalat díjat számíthat fel az érintett által kért tájékoztatás további másolataiért.

25. § Tiltakozáshoz, adattörléshez, zároláshoz, helyesbítéshez való jog

(1) Az érintettek bármikor tiltakozhatnak adataik felhasználásával szemben, ha az adatokat nem törvényileg kötelező célokra használják fel.

(2) A tiltakozás joga akkor is megilleti, ha az adatkezelés alanya korábban hozzájárult adatai használatához.

(3) A jogos adattörlési vagy korlátozási kéréseket azonnal teljesíteni kell. Az ilyen kérés különösen jogos akkor, ha az adathasználat jogalapja megszűnt. A kötelező retenciós időszakra azonban figyelemmel kell lenni.

(4) Az érintettek bármikor kérhetik a vállalattól a róluk tárolt személyes adatok helyesbítését, amennyiben az adatok hiányosak és/vagy nem pontosak.

(5) Olyan üzleti modellek esetében, amelyeknél a visszavonás vagy a törlés szerződéses kötelezettségek nem teljesítéséhez vezet, az érintettet tájékoztatni kell.

26. § A tisztázáshoz, és az észrevételezéshez való jog

(1) Ha az adatkezelés alanya azt állítja, hogy jogszabályellenes adatkezelés kapcsán sérültek a jogai, különösen, ha bizonyítékot szolgáltat jelen Eljárási Szabályzat igazolható megsértésére, a felelős vállalat késedelem nélkül köteles tisztázni a tényeket. Különösképpen az Európai Unión kívüli vállalatoknak továbbított adatok esetében az Európai Unión belüli székhelyű vállalat köteles a tények tisztázására, és bizonyítania kell, hogy a fogadó fél nem sértette meg a jelen Binding Corporate Rules Privacy adatvédelmi szabályokat, vagy felelős bármilyen okozott kárért. A vállalatoknak szorosan együtt kell működniük egymással a tények tisztázása érdekében, és az ehhez szükséges információkhoz kötelesek egymás számára hozzáférést biztosítani.

(2) Az érintett a Deutsche Telekom Cégcsoport Holding ellen panaszt nyújthat be, ha az a gyanúja, hogy a Deutsche Telekom Cégcsoporthoz tartozó valamelyik vállalat nem a jogi előírásoknak vagy jelen Binding Corporate Rules Privacy szabályzatnak megfelelően végzi személyes adatai feldolgozását. A megalapozott panaszt megfelelő időn belül kezelni kell, és az érintettet az adatkezelési helyzettől számított egy hónapon belül megfelelően tájékoztatni kell. Ez az időtartam további két hónappal meghosszabbítható ha szükséges, a kérelem komplexitását és a kérelmek számát figyelembe véve, a meghosszabbításról a kérelmezőt megfelelően tájékoztatni kell.

(3) Amennyiben egy panasz több vállalatot érint, a panasz tárgyát legjobban ismerő vállalat Adatvédelmi Tisztviselőjének kell összehangolnia az érintettel a témában folytatott minden levelezést. A Cégcsoport Adatvédelmi Tisztviselője bármikor gyakorolhatja a helyettesítésre és átvételre vonatkozó jogát.

(4) A személyes adatokkal kapcsolatos incidensek bejelentésére megfelelő csatornáknak kell rendelkezésre állniuk (például Adatvédelmi Tisztviselő vagy közvetlen kontaktszemély, aki online elérhető).

(5) Az érintett vállalat Adatvédelmi Tisztviselője a megfelelő jelentési folyamatokon keresztül köteles haladéktalanul tájékoztatni a Cégcsoport Adatvédelmi Tisztviselőjét az adatvédelmi incidensről, és biztosítani az adatvédelmi incidens dokumentációját, ami kérelemre a felügyelő hatóság számára elérhetővé tehető.

(6) Az érintettek a jelen Binding Corporate Rules Privacy szabályzat ötödik részének értelmében panasszal élhetnek, ha jogaik sérültek vagy veszteséget szenvedtek el.

27. § Kérdéshez és panaszhoz való jog

Valamennyi érintettnek bármikor jogában áll felvenni a kapcsolatot annak a vállalatnak az Adatvédelmi Tisztviselőjével, ahol a kérdéses személyes adatait feldoglozzák, ha kérdése vagy kifogása vannak a jelen Binding Corporate Rules Privacy szabályzat alkalmazásával kapcsolatban. A kérdés/panasz tárgyát legjobban ismerő vagy az érintett adatait gyűjtő vállalat köteles biztosítani, hogy az érintett jogait a többi felelős vállalat megfelelő módon tiszteletben tartsa.

28. § Az érintettek jogainak gyakorlása

Az érintetteket az itt ismertetett jogok gyakorlása miatt semmilyen hátrány nem érheti. Az érintettel folytatott kommunikáció formájának – pl. telefon, e-mail vagy levél – figyelembe kell vennie az érintett kívánságát, amennyiben lehetséges.

29. § A Binding Corporate Rules Privacy szabályzat hozzáférhetősége

Ezen kötelező erejű vállalati adatvédelmi szabályok aktuális változatát és az azokat jogilag kötelező jelleggel elfogadó vállalatok listáját a www.telekom.com oldalon teszik közzé.

Negyedik rész
Az adatvédelmi szervezet

30. § Felelősség az adatkezelésért

A vállalatok kötelesek biztosítani az adatok védelmével kapcsolatos jogi rendelkezések és jelen Binding Corporate Rules Privacy szabályzat betartását.

31. § Adatvédelmi Tisztviselő

(1) Minden vállalatnak ki kell jelölnie egy független Adatvédelmi Tisztviselőt, akinek feladata biztosítani, hogy az adott vállalat egyes szervezeti egységei tájékoztatás kapjanak az adatok védelmével kapcsolatos törvényi, illetve a vállalat/cégcsoport szintjén meghatározott előírásokról, és különösképpen a jelen Binding Corporate Rules Privacy szabályzatról. Az Adatvédelmi Tisztviselőnek megfelelő intézkedésekkel, különösképpen véletlenszerű ellenőrzésekkel kell figyelemmel kísérnie az adatvédelmi rendelkezéseknek való megfelelőséget.

(2) A vállalatnak az Adatvédelmi Tisztviselő kinevezése előtt egyeztetnie kell a Cégcsoport Adatvédelmi Tisztviselőjével.

(3) A vállalat gondoskodik arról, hogy az Adatvédelmi Tisztviselő feladatai és kötelezettségei ne eredményezzenek összeférhetetlenséget.

(4) A vállalatnak biztosítania kell, hogy az Adatvédelmi Tisztviselő rendelkezzen az adatvédelmi intézkedések jogi, műszaki és szervezeti szempontjainak értékeléséhez szükséges megfelelő szakértelemmel.

(5) A vállalatnak az Adatvédelmi Tisztviselő számára biztosítania kell a feladatának ellátásához szükséges pénzügyi és személyi erőforrásokat

(6) Az Adatvédelmi Tisztviselőnek meg kell adni a jogot, hogy közvetlenül a vállalat vezetésének tartozzon beszámolással, és szervezetileg a vállalatvezetéshez kell kapcsolódnia.

(7) Az egyes vállalatok Adatvédelmi Tisztviselői tartoznak felelősséggel a Cégcsoport Adatvédelmi Tisztviselője és a Deutsche Telekom Cégcsoport adatvédelmi stratégiája által meghatározott követelmények teljesüléséért.

(8) Minden vállalat minden egyes részlege köteles tájékoztatni vállalatának Adatvédelmi Tisztviselőjét az informatikai infrastruktúra, a hálózati infrastruktúra, az üzleti modellek, a termékek, a személyi állomány adatainak feldolgozása és a megfelelő stratégiai tervek szempontjából bekövetkező mindennemű változásról. Az Adatvédelmi Tisztviselőt az új fejlesztésekkel kapcsolatban a fejlesztésnek már a korai szakaszában be kell vonni, hogy biztosítható legyen az adatvédelmi szempontok figyelembe vétele és kiértékelése.

32. § A Cégcsoport Adatvédelmi Tisztviselője

(1) A Cégcsoport Adatvédelmi Tisztviselője koordinálja a Deutsche Telekom Cégcsoporton belül az adatvédelemmel kapcsolatos minden jelentős kérdésben az együttműködési és egyeztetési folyamatokat. A Deutsche Telekom Cégcsoport Holding vezérigazgatóját tájékoztatja az aktuális fejleményekről, illetve a tervezett ajánlásokról, amennyiben ez szükséges.

(2) A Cégcsoport Adatvédelmi Tisztviselőjének kötelessége a Deutsche Telekom Cégcsoport adatvédelemmel kapcsolatos szabályainak kidolgozása és fejlesztése, adott esetben a Cégcsoporthoz tartozó vállalatok Adatvédelmi Tisztviselőivel egyeztetve. Ezek az Adatvédelmi Tisztviselők dolgozzák ki a Cégcsoport adatvédelmi szabályzatával összhangban saját vállalatuk adatvédelmi szabályzatát. A Cégcsoport Adatvédelmi Tisztviselője és a nemzeti vállalatok Adatvédelmi Tisztviselői évenkénti találkozókon, a nemzetközi adatvédelmi vezetők értekezletein tájékoztatják egymást (személyes találkozás).

33. § A szabályok megsértésével és a vállalatra vonatkozó jogszabályi változásokkal kapcsolatos tájékoztatási kötelezettség

Az érintett vállalat köteles haladéktalanul tájékoztatni adatvédelmi tisztviselőjét az adatvédelmi szabályok, különösen a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok megsértéséről vagy annak egyértelmű jeléről. Ha az esemény potenciális hatással lehet a nyilvánosságra, egynél több vállalatot érint, vagy 500 000 eurónál nagyobb potenciális veszteséggel jár, az adatvédelmi tisztviselő ezt követően haladéktalanul tájékoztatja a Csoport Adatvédelmi Biztosát. A Csoport Adatvédelmi Biztosának tájékoztatása minden esetben kötelező, ha az illetékes felügyeleti hatóság közigazgatási bírságot szabott ki a vállalatra.

Ezen túlmenően a Vállalat Adatvédelmi Biztosa köteles tájékoztatni a Csoport Adatvédelmi Biztosát, ha a vállalatra vonatkozó jogszabályokban és gyakorlatban olyan változások következnek be, amelyek jelentősen kedvezőtlenek a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok betartása szempontjából.

Az adatkezelőként eljáró vállalatok indokolatlan késedelem nélkül tájékoztatják az érintetteket, ha egy esemény valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

34. § Az adatvédelem szintjének felülvizsgálata

(1) A vonatkozó éves ellenőrzési terv elkészítése során a Kötelező Erejű Vállalati Adatvédelmi Szabályok hatálya alá tartozó feldolgozási tevékenységek által jelentett kockázatokra is figyelemmel kell lenni. A Csoport Adatvédelmi Biztosának ellenőrzését a belső és külső ellenőrök végzik. Rendszeres önértékelésekre is sor kerülhet a Deutsche Telekom Csoporton belül, amelyeket a Csoport Adatvédelmi Biztosa koordinál.

(2) A vizsgálatok lefolytatásával megbízott vállalatok vagy más szervezeti egységek Adatvédelmi Biztosai külön írásban dokumentált ellenőrzési tervek alapján is végeznek ellenőrzéseket annak megállapítására, hogy a vállalatok megfelelnek-e az adatvédelmi követelményeknek. Az Adatvédelmi Biztosok a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok betartásának ellenőrzésére nem jogosultak, amennyiben ez a helyzet összeférhetetlenséget eredményezhet.

(3) A vállalat köteles megfelelő intézkedéseket tenni az ellenőrzés során feltárt bármely hiányosság orvoslására, a Cégcsoport Adatvédelmi Tisztviselőjének pedig figyelemmel kell kísérnie az ilyen intézkedések végrehajtását. Amennyiben a vállalat elfogadható indok nélkül nem hajtja végre az intézkedéseket, a Cégcsoport Adatvédelmi Tisztviselője felméri az adatvédelemre való kihatásokat, és megteszi a megfelelő intézkedéseket, szükség esetén felsőbb szintre viszi tovább az ügyet.

(4) A vállalatok Adatvédelmi Tisztviselői vagy az ellenőrzések végrehajtásával megbízott egyéb szervezeti egységek külön e célra írásban elkészített auditterv alapján azt is ellenőrzik, hogy a vállalatok megfelelnek-e az adatvédelmi követelményeknek.

(5) A Cégcsoport Adatvédelmi Tisztviselője a Cégcsoportnál, az Adatvédelmi Tisztviselők saját vállalatuknál jogosultak ellenőrizni, hogy a személyes adatok felhasználása megfelelő módon történik-e, amennyiben nincsenek jogi korlátozások. Az érintett vállalatoknak a Cégcsoport Adatvédelmi Tisztviselője és az Adatvédelmi Tisztviselők számára teljes körű hozzáférést kell biztosítaniuk az összes olyan információhoz, mely a helyzet tisztázásához és kiértékeléséhez számukra szükséges. A Cégcsoport Adatvédelmi Felelőse és az Adatvédelmi Tisztviselők jogosultak e tekintetben utasításokat adni.

(6) A vállalatok Adatvédelmi Tisztviselőinek az ellenőrzések során a teljes Cégcsoportra érvényes, standard eljárásokat kell alkalmazniuk, például az általános adatvédelmi auditok eljárásait, amennyiben lehetséges. Az ilyen eljárásokat a Cégcsoport Adatvédelmi Tisztviselője teszi elérhetővé.

35. § Az adatvédelemi hatásvizsgálat

A vállalatok a személyes adatok feldolgozására vonatkozóan strukturált és dokumentált adatvédelmi hatásvizsgálatot végeznek. A Deutsche Telekom Group Holding központilag elérhetővé teszi az Adatvédelmi és biztonsági értékelés (Privacy and Security Assessment, PSA) nevű folyamatot, amelyet a jelenlegi változatában egységesen alkalmazandók minden vállalatnál. A PSA-folyamat alkalmazásától a csoport adatvédelmi biztosával konzultálva és annak előzetes jóváhagyásával lehet eltérni, abban az esetben, ha a vállalatok rendkívül kis méretűek, vagy nem végeznek jelentős mértékű adatfeldolgozást.

36. § Az alkalmazottak kötelezettségei és oktatása

(1) A vállalatoknak alkalmazottaikat kötelezniük kell legkésőbb a foglalkoztatásuk megkezdésekor az adatok és a telekommunikáció bizalmasságának, titkosságának fenntartására. Az alkalmazottakat e kötelezettségvállalás részeként megfelelő oktatásban kell részesíteni az adatvédelemre vonatkozóan. A vállalatnak ehhez megfelelő folyamatokat kell bevezetnie, és biztosítania kell a szükséges erőforrásokat.

(2) Az alkalmazottaknak az adatvédelem alapjairól rendszeresen, de legalább kétévente oktatást kell kapniuk. A vállalatok jogosultak saját alkalmazottaik számára speciális tanfolyamokat kidolgozni és megvalósítani. Minden vállalat Adatvédelmi Tisztviselőjének dokumentálnia a tanfolyamok megvalósulását, és ezekről évenként tájékoztatni a Cégcsoport Adatvédelmi Tisztviselőjét ~~Felelősét~~.

(3) A Cégcsoport Adatvédelmi Tisztviselője központilag teheti elérhetővé a Deutsche Telekom Cégcsoport alkalmazottainak kötelezettségeivel és oktatásával kapcsolatos erőforrásokat és folyamatokat.

37. § Együttműködés a felügyeleti hatóságokkal

(1) A vállalatoknak az ő tevékenységüket vagy az adatok továbbítását végző vállalat tevékenységét felügyelő illetékes hatóságokkal való együttműködést bizalmi alapon kell folytatniuk, különösképpen a kérdésekre történő válaszadás és az ajánlások követése tekintetében.

(2) Amennyiben a vállalatra vonatkozó jogszabályok változása jelentős mértékű negatív hatással lehet a jelen Binding Corporate Rules Privacy szabályzat által biztosított garanciákra, az érintett vállalatnak értesítenie kell a változásról az illetékes adatvédelmi hatóságot.

(3) Az illetékes felügyeleti hatóságok által a jelen Kötelező Erejű Vállalati Adatvédelmi Szabályok betartásának felügyeletével kapcsolatos bármely jogvitát a felügyeleti hatóság tagállamának bíróságai rendezik, az adott tagállam eljárási jogának megfelelően. A vállalatok vállalják, hogy alávetik magukat ezen bíróságok joghatóságának.

38. § A felmerülő kérdések tekintetében felelős kontaktszemélyek

A vállalatok Adatvédelmi Tisztviselői, illetve a Cégcsoport Adatvédelmi Tisztviselője a kijelölt kontaktszemélyek a jelen Binding Corporate Rules Privacy szabályzattal kapcsolatban felmerülő kérések és kérdések megválaszolására. A Cégcsoport Adatvédelmi Tisztviselője kérésre megadja a vállalatok Adatvédelmi Tisztviselők elérhetőségi adatait.

A Cégcsoport Adatvédelmi Tisztviselőjének elérhetősége:

datenschutz@telekom.de

privacy@telekom.de

Firedrich-Ebert-Allee 140,

53113 Bonn

Ötödik rész
Kártérítési felelősség

39. § A kártérítésért való felelősségi szabályok alkalmazási területe

(1) A jelen Binding Corporate Rules Privacy szabályzat ötödik része kizárólag a 679/2016 általános adatvédelmi rendelet (GDPR) hatálya alá tartozó adatkezelésekre vonatkozik.

(2) Az Európai Gazdasági Térégterületén belül annak az országnak a kártérítési felelősségre vonatkozó jogi rendelkezéseit kell alkalmazni, ahol a vállalat bejegyzett központi székhelye található. A Binding Corporate Rules Privacy szabályzat § 1. szakaszának hatálya alá nem tartozó adatok tekintetében annak az országnak a kártérítési felelősségre vonatkozó jogi rendelkezéseit alkalmazandók, amelyben az adatokat gyűjtő vállalat bejegyzett székhelye található. Jogi rendelkezések hiányában az adatgyűjtést végző vállalat követelményei, feltételei és kikötései alkalmazandóak.

(3) A kár tényleges összegét meghaladó bármilyen kártérítést kifejezetten ki kell zárni.

40. § Kártérítés nyújtása

(1) Bármely érintett, aki veszteséget szenvedett amiatt, mert a Binding Corporate Rules Privacy szabályzatban foglalt egy vagy több kötelességét a Deutsche Telekom Cégcsoport valamelyik vállalata megsértette, vagy a fogadó fél sértette meg, akinek Deutsche Telekom Cégcsoport valamelyik vállalata átadta vagy továbbította az adatokat, jogosult a Deutsche Telekom Cégcsoport érintett vállalatával szemben kártérítési igénnyel fellépni.

(2) Az érintett a Deutsche Telekom Cégcsoport Holdinggal szemben is jogosult kártérítési igénnyel fellépni. Amennyiben a Holding fizeti meg a kártérítést, jogosult a veszteségért felelős, vagy az azt okozó harmadik felet megbízó vállalattól annak megtérítését kérni. .

(3) Az érintettnek első fokon az adatokat átadó vagy továbbító vállalattal szemben kell kártérítési igénnyel fellépnie. Amennyiben az adatokat átadó cég jogilag vagy tényszerűen nem felelős, az érintett jogosult az adatok fogadó vállalattal szemben kártérítési igénnyel fellépni. Az adatok fogadó vállalat nem jogosult a felelősséget a szabályokat megsértő alvállalkozó felelősségére hivatkozva elhárítani.

(4) Az érintett bármikor jogosult a lakhelye, szokásos tartózkodási helye, munkavégzésének helye vagy az állítólagos jogsértés helye szerint illetékes felügyeleti hatóságnak, vagy a Deutsche Telekom Cégcsoport Holding illetékes felügyeleti hatóságának panaszt benyújtani.

(5) Az érintett jogosult panasszal élni az Európai Gazdasági Térség illetékes bíróságainál, ha úgy véli, hogy a jelen Kötelező erejű vállalati szabályok alapján fennálló jogait megsértették személyes adatainak a jelen Kötelező erejű vállalati szabályokkal nem összhangban történő feldolgozása következtében.

(6) Az érintett jogosult egy nonprofit szervet, szervezetet vagy egyesületet megbízni a fent említett jogok saját nevében történő gyakorlásával.

41. § Bizonyítási kényszer

Az érintett adatainak megfelelő kezelésével kapcsolatos bizonyítási kényszer a felelős vállalatot terheli.

42. § Érintettek jogai harmadik félként

Amennyiben az érintett nem rendelkezik közvetlen jogokkal, a jelen Binding Corporate Rules Privacy szabályzat rendelkezései alapján jogosult harmadik félként kártérítési igénnyel fellépni a szerződéses kötelezettségeit nem teljesítő vállalatokkal szemben.

43. § Az Illetékesség helye

A kártérítési igény érvényesítésének illetékességi helye az adott személy döntése alapján lehet

a) ahol természetes személy az érintett, ott a tartózkodás helye,
b) az a joghatóság ahol a Cégcsoportnak szervezete található, vagy
c) a Cégcsoport azon európai tagjának európai uniós központja szerinti, amelyhez az adatvédelmi feladatokat delegálták.

44. § Az igazságszolgáltatáson kívüli megállapodás

(1) Amennyiben egy harmadik fél véleménye szerint személyes adatainak tényleges vagy vélt kezelése miatt sérült a magánélet tiszteletben tartásához fűződő joga, jogosult az érintett vállalat Adatvédelmi Tisztviselőjétől az ügyben eljárást kérni. Az Adatvédelmi Tisztviselő köteles a panaszt kivizsgálni és az érintettet a jogairól tájékoztatni. Ennek során az Adatvédelmi Tisztviselő köteles a panaszos egyéb személyes adatainak bizalmasságát megőrizni, kivéve, ha a panaszos az Adatvédelmi Tisztviselőt felmenti ezen kötelezettsége alól. Az érintett személy kérésére az érintett személy és az Adatvédelmi Tisztviselő bevonásával meg kell kísérelni a panasszal kapcsolatban megegyezést elérni. Az ilyen megegyezésnek része lehet az érintett magánélet tiszteletben tartásához fűződő jogának megsértéséből adódóan elszenvedett veszteségekre vonatkozó ellentételezésre vonatkozó felajánlás is. Ez a felajánlás kötelező érvényű az érintett vállalatokra vonatkozóan, amennyiben a felek kölcsönösen elfogadják.

(2) A panasz benyújtásának joga a lakhely, szokásos tartózkodási hely, munkavégzés helye vagy az állítólagos jogsértés helye szerint illetékes illetékes felügyeleti hatósághoz, illetve a jogi kereset lehetősége változatlan marad.

Hatodik rész
Záró rendelkezések

45. § A jelen Binding Corporate Rules Privacy szabályok felülvizsgálata és módosítása

(1) A Cégcsoport Adatvédelmi Tisztviselője köteles rendszeresen, de legalább évenként egyszer megvizsgálni a Binding Corporate Rules Privacy szabályzatot, hogy megállapítsa, azok megfelelnek-e a vonatkozó jogi környezetnek, és el kell végeznie a szükséges módosításokat.

(2) A jelen Binding Corporate Rules Privacy szabályzatban a jogi követelményekkel történő összhang megteremtése céljából végrehajtott bármilyen jelentősebb módosítást egyeztetni kell a felügyeleti hatósággal. Az ilyen módosítások a megfelelő átmeneti időszak eltelte után közvetlenül érvénybe lépnek mindazoknál a vállalatoknál, amelyek vállalták a kötelező erejű személyesadat-védelmi vállalati szabályok betartását.

(3) A Cégcsoport Adatvédelmi Tisztviselője a módosult tartalomról köteles tájékoztatni az összes vállalatot, amely bevezette a Binding Corporate Rules Privacy szabályzatot.

(4) A vállalatok Adatvédelmi Tisztviselői kötelesek megvizsgálni, hogy a Binding Corporate Rules Privacy szabályzat módosításai kihatással vannak-e a jogi megfelelőségre saját országukban, illetve ütköznek-e országuk törvényi, jogi rendelkezéseivel. Amennyiben a vállalat törvényi okok miatt nem tudja átültetni a módosításokat, haladéktalanul tájékoztatnia kell a Cégcsoport Adatvédelmi Tisztviselőjét és az illetékes felügyeleti hatóságot, és adott esetben átmenetileg fel kell függeszteni az adott vállalatra vonatkozóan a Binding Corporate Rules Privacy szabályzat alkalmazását.

(5) A személyes adatokat harmadik országokba továbbító vállalatok - adott esetben a címzettekkel együttműködve - folyamatosan figyelemmel kísérik az adott harmadik országban bekövetkező olyan fejleményeket, amelyek befolyásolhatják a meglévő adattovábbítási hatásvizsgálatokat és a Kötelező Erejű Vállalati Adatvédelmi Szabályok betartását.

46. §Kapcsolattartók és vállalatok listája

A Cégcsoport Adatvédelmi Tisztviselője listát vezet azokról a vállalatokról, amelyek bevezették a jelen Binding Corporate Rules Privacy szabályzatot, illetve ezeknek a vállalatoknak a kapcsolattartóiról. A listát naprakészen vezeti, kérésre az érintetteket tájékoztatja. Évente a hatáskörrel rendelkező felügyelő hatóság rendelkezésére kell bocsátani egy naprakész nyilvántartást azokról a vállalatokról, akik kötelező jelleggel bevezették a Binding Corporate Rules Privacy-t.

47. § Eljárásjog / elválaszthatatlansági záradék

A jelen Binding Corporate Rules Privacy szabályzatra jogvita esetén a Német Szövetségi Köztársaság eljárásjoga alkalmazandó.

Amennyiben a jelen Federal Republic of Germany szabályzat bármelyik különálló rendelkezése érvénytelenné válik, a jelen Binding Corporate Rules Privacy szabályzat és az érvénytelen rendelkezések eredeti szándékához legközelebb álló rendelkezések lépnek a helyébe. Amennyiben kétség merül fel, az ilyen esetekben vagy vonatkozó rendelkezések hiányában az Európai Unió vonatkozó adatvédelmi jogszabályait kell alkalmazni.

48. § Közzététel

A vállalatoknak az érintettek jogaira és a harmadik félként való kedvezményezettségére vonatkozó rendelkezésekkel kapcsolatos tájékoztatást megfelelő formában – például az interneten – elérhetővé kell tenniük a nyilvánosság számára. Ezt a tájékoztatást közzé kell tenni, amint a jelen Binding Corporate Rules Privacy szabályzat kötelezővé válik a vállalat számára.

Hetedik rész
Fogalom meghatározások és a használt kifejezések

Anonimizálás

az információk olyan jellegű módosítása, amelynek eredményeképpen a személlyel kapcsolatos adatok és egyéb tények nem vezethetők vissza az azonosított vagy azonosítható természetes személyre, illetve amelynek eredményeképpen aránytalanul sok idő, nagy költség és energia ráfordítása nélkül nem lehetséges visszavezetésük ilyen személyre.

Automatizált egyedi döntések

az érintettre jogi kihatással lévő vagy komoly hátrányt jelentő döntések, amelyek az érintett értékelését célzó bizonyos adatok – pl. munkahelyi teljesítményének, hitelképességének, megbízhatóságának, magatartásának stb. – kizárólagosan automatizált adatfeldolgozásán alapulnak.

Vállalat

bármely vállalat, amelyre vonatkozik a jelen Binding Corporate Rules Privacy szabályzat. Nyilvántartási célból külön lista készül ezekről a vállalatokról, a lista folyamatosan frissül. A listát bármikor, bárki megtekintheti.

Adatkezelő

azt a természetes vagy jogi személyt jelenti, aki/amely meghatározza a személyes adatok kezelésének célját és eszközeit.

Érintett

az azonosított vagy azonosítható természetes személy, akinek személyes adatait a Deutsche Telekom Cégcsoporton belül kezelik.

Deutsche Telekom Cégcsoport

A Deutsche Telekom AG és mindazon vállalatok, amelyekben a Deutsche Telekom AG közvetlen vagy közvetett tulajdona meghaladja az 50%-os részesedést, illetve amelyek teljes mértékben integráltak a Cégcsoportba.

Európai Gazdasági Térség

Az Európai Unió tagállamaiból és az Európai Szabadkereskedelmi Társulásból (Izland, Liechtenstein és Norvégia; Svájc kivételével) áll.

Cégcsoport Holding

A vállaltcsoport holdingcége jelenleg a Deutsche Telekom AG, amelynek központja Bonn (Németország), Friedrich-Ebert-Allee 140, 53113 címen található.

Személyes adat

Az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

Példák: név, születési idő, lakcím, bankszámla szám, e-mail cím, személyi szám, postai adatok, telefonszám, ügyfél adatok, (hálózati) forgalmi adatok, szolgáltatás használati adatok, hang és adattartalom, tartózkodási hely adatok, IP cím, bejelentkezési adatok.

Álnevesítés

a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

Adatkezelés

a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés

Adatfeldolgozó

az a vállalat amely az adatkezelő nevében személyes adatok kezelését (feldolgozását) végzi.

Fogadó fél

az a természetes vagy jogi személy, hatóság, intézmény vagy bármely más szerv, akinek vagy amelynek a részére az adatot továbbítják, függetlenül attól, hogy harmadik személy-e vagy sem. Azok az állami hatóságok, amelyek konkrét megkeresés alapján kapnak adatokat, nem tekinthetők Fogadó félnek.

Különleges adatok

jelentik a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatokat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatokat, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatokat.

Harmadik fél

jelent az érintetten, az adatkezelőn, az adatfeldolgozón és az adatkezelő vagy adatfeldolgozó közvetlen felügyelete alatt személyes adatok kezelésére jogosultakon kívüli természetes vagy jogi személyt, hatóságot, ügynökséget vagy egyéb szervezetet.