

**Reguli Corporatiste Obligatorii cu privire la Datele cu Caracter
Personal (BCRP)**

**Reguli corporatiste obligatorii pentru protectia drepturilor personale
în privinta prelucrării datelor cu caracter personal în cadrul
Grupului Deutsche Telekom**

Varianta revizuita de catre Deutsche
Telekom AG, Group Privacy, versiunea 2.8,
la data de 19 Februarie 2019

Cuprins

Obiect.....	6
Natura legala a Regulilor Corporatiste Obligatorii cu privire la datele cu caracter personal	6
Domeniul de aplicare.....	6
Relatia cu alte dispozitii legale.....	7
Expirarea si incetarea.....	8
PARTEA A DOUA – PRINCIPII.....	9
SECTIUNEA 1 - TRANSPARENȚA PRELUCRĂRII DATELOR.....	9
Obligatia de a informa.....	9
Continutul si forma informarilor.....	9
Disponibilitatea informatiilor.....	9
Inregistrarea tuturor categoriilor de date personale prelucrate.....	9
SECTIUNEA 2 - CONDITII DE ADMISIBILITATE PENTRU UTILIZAREA DATELOR CU CARACTER PERSONAL.....	11
Principiu.....	11
Admisibilitatea utilizarii datelor cu caracter personal.....	11
Consimtamantul persoanei vizate.....	12
Decizii individuale automatizate incluzand profilarea.....	12
Utilizarea datelor cu caracter personal in scopuri de marketing direct.....	12
Categorii speciale de date cu caracter personal.....	13
Minimizarea datelor, evitarea prelucrării datelor, limitarea retentiei datelor, anonimizarea si pseudonimizarea.....	13
Interzicerea de a conditiona.....	13
SECTIUNEA 3 - TRANSFERUL DATELOR CU CARACTER PERSONAL.....	15
Natura si scopul transferului datelor cu caracter personal.....	15
Transmiterea datelor.....	15
Prelucrarea datelor.....	16



SECȚIUNEA 4 - CALITATEA DATELOR SI SECURITATEA DATELOR.....	17
Calitatea datelor.....	17
Securitatea Datelor - masuri tehnice si organizatorice – protectia datelor conform principiilor “privacy by design” si “privacy by default”	17
PARTEA A TREIA - DREPTURILE PERSOANELOR VIZATE.....	19
Dreptul de acces.....	19
Dreptul de a se opune, Dreptul de a solicita stergerea sau blocarea datelor si Dreptul de a solicita rectificarea datelor	19
Dreptul la clarificare, Dreptul de a formula comentarii precum si Dreptul de a fi despagubit.....	20
Dreptul de a formula intrebari si plangeri.....	21
Exercitarea drepturilor de catre persoanele vizate.....	21
Copie tiparita a Regulilor Corporatiste Obligatorii privind datele cu caracter personal.....	21
PARTEA A PATRA - ORGANIZAREA STRUCTURII DE PROTECTIE A DATELOR CU CARACTER PERSONAL.....	22
Responsabilitatea pentru procesarea datelor.....	22
Ofiterul de Protectie a Datelor cu Caracter Personal.....	22
Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului.....	24
Obligatia de a informa in caz de incalcare a prevederilor in materie	24
Verificarea nivelului de protectie a datelor cu caracter personal.....	24
Angajamentul angajatilor si instruirea acestora.....	26
Cooperarea cu Autoritatile de Supraveghere.....	26
Persoanele responsabile pentru solutionarea solicitarilor.....	26
PARTEA A CINCEA – RASPUNDERE.....	28
Domeniul de aplicare a regulilor de raspundere.....	28
Persoana indreptatita la despagubiri.....	28
Responsabilitatea de a face dovada.....	29
Substituirea tertului in drepturile persoanei vizate.....	29
Competenta autoritatilor din punct de vedere teritorial.....	29
Arbitrajul.....	29



PARTEA A SASEA - PREVEDERI FINALE.....	31
Revizuirea si modificarea acestor Reguli Corporatiste Obligatorii.....	31
Lista de contacte si companii.....	31
Norme de procedura/ Clauza de nulitate.....	32
Publicarea.....	32
PARTEA A SAPTEA - Definitii si Termeni.....	33

PREAMBUL

(1) Protejarea datelor cu caracter personal ale clientilor, angajatilor si ale altor persoane conectate cu Grupul Deutsche Telekom reprezinta o prioritate pentru toate companiile din cadrul Grupului Deutsche Telekom.

(2) Companiile din cadrul Grupului Deutsche Telekom sunt constiente de faptul ca succesul Deutsche Telekom ca intreg este dependent nu numai de raspandirea globala a fluxurilor de informatii, cat si, mai presus de toate, de administrarea corecta si in siguranta a datelor cu caracter personal.

(3) In multe domenii, Grupul Deutsche Telekom este perceput de catre clientii sai si de catre publicul general ca o singura entitate. De aceea este o preocupare comuna a companiilor Grupului Deutsche Telekom de a aduce o contributie importanta la succesul comun al companiei si de a sprijini cerinta Grupului Deutsche Telekom de a fi un furnizor de produse de inalta calitate si servicii inovatoare prin implementarea acestor Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal.

(4) Prin furnizarea acestor Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal, Grupul Deutsche Telekom creaza un nivel standardizat si ridicat de protectie a datelor la nivel mondial, aplicabil pentru utilizarea datelor atat in cadrul unei companii cat si intre companii, precum si la transferul de date in Germania si la nivel international. In cadrul Grupului Deutsche Telekom, datele personale trebuie procesate de catre persoana imputernicita in conformitate cu principiile legislatiei privind protectia datelor aplicabile partii care transfera datele (operatorul).

PARTEA INTAI

SCOP

1. Natura legala a Regulilor Corporatiste Obligatorii cu privire la datele cu caracter personal

Regulile Corporatiste Obligatorii cu privire la date cu caracter personal sunt obligatorii in ceea ce priveste prelucrarea datelor cu caracter personal (in conformitate cu documentul de lucru 256, Articolul 29 al grupului de lucru al Comisiei Europene¹) pentru toate companiile din Grupul Deutsche Telekom care le-au adoptat avand la baza un temei legal. Regulile Corporatiste Obligatorii cu privire la datele cu caracter personal vor fi obligatorii pentru toate companiile care vor fi solicitate de catre Deutsche Telekom sa le adopte si pentru toate companiile care le-au adoptat in mod voluntar, indiferent de locul in care sunt colectate datele.

2. Domeniul de aplicare

Regulile Corporatiste Obligatorii cu privire la datele cu caracter personal se aplica tuturor tipurilor de date cu caracter personal procesate in cadrul Grupului Deutsche Telekom, indiferent de locul in care se colecteaza datele. Datele cu caracter personal vor fi utilizate in cadrul Grupului Deutsche Telekom in special in urmatoarele scopuri:

- a) Pentru a gestiona datele angajatilor la initierea, implementarea si procesarea contractelor de munca si pentru a se adresa angajatilor cu produse si servicii oferite de catre Grupul Deutsche Telekom sau terti.

- b) Pentru a initia, implementa si procesa contractele de afaceri cu clientii si consumatorii, si pentru a desfasura activitati de publicitate si cercetare de piata care vizeaza informarea clientilor si tertilor interesati despre produsele si serviciile oferite de catre Grupul Deutsche Telekom sau partenerii sai dupa caz.

¹ Aprobarea Comitetul european pentru protecția datelor, a orientarilor WP29 1/2018;



NEXTGEN
communications

c) Pentru a initia si implementa acorduri cu furnizorii de servicii ai Grupului Deutsche Telekom ca parte a furnizarii de servicii pentru Grupul Deutsche Telekom.

d) Pentru a desfasura relatii cu alte parti terte, in special actionari, parteneri sau vizitatori, si pentru a respecta reglementarile legale obligatorii.

Datele vor fi utilizate in conformitate cu scopurile de business actuale si viitoare ale companiilor din Grupul Deutsche Telekom, care includ furnizarea de servicii de telecomunicatii, servicii digitale pentru clienti rezidentiali si de afaceri, servicii IT (inclusiv servicii de centre de date) si servicii de consultanta.

3. Relatia cu alte dispozitii legale

(1) Dispozitiile Regulilor Corporatiste Obligatorii cu privire la datele cu caracter personal sunt concepute pentru a asigura un nivel ridicat si standardizat de confidentialitate a datelor in tot Grupul Deutsche Telekom. Obligatiile existente si reglementarile cu care companiile individuale trebuie sa se conformeze pentru prelucrarea si utilizarea datelor cu caracter personal care trebuie aplicate dincolo de principiile prevazute in aceste Reguli Corporatiste Obligatorii, sau care contin restrictii suplimentare privind prelucrarea si utilizarea datelor cu caracter personal vor ramane neafectate de aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal.

(2) Datele cu caracter personal colectate in Europa vor fi folosite, in general, in concordanta cu dispozitiile legale ale tarii in care datele au fost colectate, indiferent de locul in care se utilizeaza datele, dar cel putin in conformitate cu cerintele acestor Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal.

(3) Aplicabilitatea legislatiei nationale cu privire la securitatea statului, apararea nationala sau securitatea publica, sau pentru prevenirea si investigarea infractiunilor si condamnarea infractorilor, care necesita ca datele sa fie transmise catre terti nu va fi afectata de dispozitiile acestor Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal. Daca o companie considera ca sectiuni importante din aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal contravin dispozitiilor nationale privind confidentialitatea datelor, impiedicand-o de la a semna aceste Reguli Corporatiste Obligatorii, atunci va informa de indata Ofiterul de Conformitate din cadrul Grupului Deutsche Telekom. Autoritatea de supraveghere



NEXTGEN

communications

responsabila a companiei trebuie implicata in calitate de mediator.

4. Expirarea si incetarea

Aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal inceteaza sa mai fie obligatorii pentru o companie in cazul in care compania paraseste Grupul Deutsche Telekom sau invalideaza aceste norme. Cu toate acestea, expirarea sau invalidarea Regulilor Corporatiste Obligatorii cu privire la datele cu caracter personal nu va elibera compania de obligatiile si/sau dispozitiile Regulilor Corporatiste Obligatorii cu privire la datele cu caracter personal care reglementeaza datele deja transmise. Transferul ulterior al datelor de la sau catre aceasta companie poate avea loc numai in cazul in care sunt prevazute alte garantii procedurale adecvate in conformitate cu cerintele legislatiei europene.

PARTEA A DOUA

PRINCIPII

SECTIUNEA 1 TRANSPARENȚA PRELUCRĂRII DATELOR

5. Obligația de a informa

Persoanele vizate trebuie să fie informate cu privire la modul de utilizare a datelor lor cu caracter personal în conformitate cu legislația aplicabilă și cu următoarele condiții.

6. Conținutul și forma informațiilor

(1) Compania trebuie să informeze persoanele vizate în mod corespunzător asupra următoarelor aspecte:

- a) Identitatea operatorului/rilor de date și datele lor de contact.
- b) Datele de contact ale ofițerilor de protecția datelor;
- c) Scopul prelucrării datelor personale; de asemenea temeiul juridic pentru prelucrarea datelor și perioada de retenție a datelor;
- d) În cazul în care datele cu caracter personal sunt transferate sau transmise către terți, destinatarul, întinderea și scopul/rile unui astfel de transfer/transmitere vor trebui să fie cunoscute.
- e) Drepturile persoanelor vizate în legătură cu utilizarea datelor lor.

(2) Indiferent de modalitatea de informare aleasă, se vor furniza aceste informații persoanelor vizate, într-un mod clar și ușor de înțeles.

7. Disponibilitatea informațiilor

Informațiile trebuie să fie disponibile pentru persoanele vizate atunci când se colectează datele și, ulterior, ori de câte ori se solicită acest lucru.

8. Înregistrarea tuturor categoriilor de date cu caracter personal prelucrate

Comaniile vor păstra o evidență a categoriilor de date cu caracter personal prelucrate. Înregistrările trebuie să conțină următoarele informații:



NEXTGEN
communications

- a) Numele si datele de contact ale Companiei, ale reprezentantilor acesteia si ale Ofiterului de Protectie a Datelor;
- b) Descrierea categoriilor de date cu caracter personal prelucrate si scopul prelucrarii;
- c) Categoriile de destinatari si tertele parti carora le vor fi divulgate sau transferate datele personale;
- d) Numele tarilor tertе si documentatia privind garantiile adecvate, acolo unde Regulile Corporatiste Obligatorii cu privire la datele cu caracter personal nu sunt aplicabile;
- e) Daca este posibil, termenele limita pentru stergerea datelor si,
- f) Daca este posibil, o descriere generala a masurilor de securitate tehnice si organizationale.

SECTIUNEA 2

CONDITII DE ADMISIBILITATE PENTRU UTILIZAREA DATELOR CU CARACTER PERSONAL

9. Principiu

- (1) Datele cu caracter personal vor fi utilizate numai in urmatoarele conditii si nu vor fi folosite in alte scopuri decat pentru cele pentru care au fost colectate initial.
- (2) Utilizarea datelor colectate in alte scopuri este permisa numai in cazul in care conditiile de admisibilitate au fost indeplinite in conformitate cu urmatoarele conditii.

10. Admisibilitatea utilizarii datelor cu caracter personal

Datele cu caracter personal pot fi folosite in cazul in care au fost indeplinite unul sau mai multe din urmatoarele criterii:

- a) Este permis in mod clar din punct de vedere legal sa se foloseasca datele in scopul avut in vedere.
- b) Persoana vizata si-a dat acordul cu privire la utilizarea datelor sale.
- c) Este necesar sa se utilizeze datele in acest mod pentru ca societatea comerciala sa-si indeplineasca obligatiile care ii revin in temeiul unui acord cu persoana vizata, incluzand obligatiile sale contractuale de a informa si/sau obligatii secundare, sau pentru ca societatea sa implementeze masuri pre- sau post-contractuale pentru initierea sau procesarea unui acord care a fost solicitat de persoana vizata.
- d) Datele trebuie sa fie utilizate pentru a indeplini o obligatie legala a companiei.
- e) Este necesar sa se utilizeze datele pentru a proteja interesele vitale ale persoanei vizate.
- f) Este necesar sa se utilizeze datele pentru a finaliza o sarcina care este in interesul publicului larg sau care face parte din exercitarea autoritatii publice si cu care compania sau o terta parte catre care data este transferata a fost incarcată.
- g) Este necesar sa se proceseze datele in scopul de a realiza interesele legitime ale companiei



sau terței parti către care datele sunt transmise, cu condiția ca aceste interese să nu fie disproporționate față de interesul privind garantarea protecției persoanei vizate.

11. Consimțământul persoanei vizate

Se consideră că persoana vizată și-a dat consimțământul în conformitate cu punctul 10 alineatul (1), articolul b) din aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal dacă:

- a) Consimțământul a fost dat în mod expres, în mod voluntar și în cunoștința de cauză, lucru care face persoana vizată conștientă de scopul pentru care își dă consimțământul. Modul de redactare a declarațiilor de consimțământ va fi suficient de precis și va informa persoana vizată despre dreptul ei de a-și retrage consimțământul în orice moment. Persoana vizată este informată pentru modelele de afaceri în care retragerea consimțământului duce la neîndeplinirea obligațiilor contractuale.
- b) Consimțământul a fost obținut într-o formă adecvată circumstanțelor (formă scrisă). În cazuri excepționale consimțământul poate fi obținut verbal, dacă modul de acordare și circumstanțele speciale care fac ca acest consimțământ verbal să fie adecvat și suficient documentat.

12. Decizii individuale automatizate incluzând profilarea

(1) Deciziile care evaluează aspecte individuale ale unei persoane și care ar putea atrage după sine consecințe juridice pentru aceasta, sau care ar putea avea un efect advers considerabil asupra acesteia, nu se bazează exclusiv pe utilizarea automatizată a datelor. Aceasta include în special decizii pentru care datele cu privire la bonitate, adecvare profesională sau starea de sănătate a persoanei vizate sunt semnificative.

(2) În cazuri individuale, în care este necesar în mod obiectiv de a lua o decizie automată, persoana vizată este informată fără întârziere cu privire la rezultatul deciziei automatizate și i se va acorda posibilitatea de a prezenta observații într-o perioadă de timp corespunzătoare. Comentariile persoanei vizate vor fi considerate în mod corespunzător înainte de luarea unei decizii finale.

13. Utilizarea datelor cu caracter personal în scopuri de marketing direct

În cazul în care datele personale sunt utilizate în scopuri de marketing direct, persoanele vizate vor fi:

- a) Informate cu privire la modul în care datele lor vor fi folosite în scopuri de marketing direct;



- b) Informate cu privire la dreptul lor de a se opune in orice moment cu privire la utilizarea datelor lor cu caracter personal pentru comunicari de marketing direct, si
- c) Echipate pentru a-si exercita dreptul de a nu primi astfel de comunicari. Acestea vor primi, in special, informatii despre compania careia ar trebui sa-i fie adresata obiectiunea.

14. Categoriile speciale de date cu caracter personal

(1) Utilizarea categoriilor speciale de date cu caracter personal este permisa numai in cazul in care este guvernata de prevederi legale sau in cazul in care a fost obtinut in avans consimtamantul persoanei vizate. Aceasta este de asemenea permisa in cazul in care este necesara prelucrarea datelor cu caracter personal pentru a indeplini drepturile si obligatiile companiei in domeniul dreptului muncii, cu conditia sa se ia masuri de protectie adecvate, iar acest lucru sa nu fie interzis in temeiul legislatiei nationale.

(2) Inainte de inceperea acestui tip de colectare, procesare sau utilizare, compania va informa Ofiterul de Protectia Datelor si va documenta aceasta actiune. La evaluarea admisibilitatii procesarii datelor, o atentie deosebita trebuie acordata naturii, scopului, necesitatii si bazei juridice de utilizare a datelor.

15. Minimizarea datelor, evitarea prelucrării datelor, limitarea retentiei datelor, anonimizarea si pseudonimizarea

(1) Datele cu caracter personal trebuie sa fie adecvate, relevante si neexcesive in ceea ce priveste utilizarea acestora pentru un anumit scop (minimizarea datelor). Datele trebuie prelucrate intr-o anumita aplicatie doar atunci cand este necesar (data avoidance - evitarea datelor). Datele trebuie pastrate, intr-o forma care sa permita identificarea persoanelor vizate, însă nu mai mult decat este necesar pentru scopul procesarii datelor.(storage limitation- limitarea pastrării datelor)

(2) In cazul in care este posibil si rezonabil din punct de vedere economic, se utilizeaza proceduri pentru a sterge caracteristicile de identificare ale persoanelor vizate (anonimizare) sau pentru a inlocui functiile de identificare cu alte caracteristici (atribuirea unui alias/pseudonimizarea).

16. Interzicerea de a conditiona

Utilizarea serviciilor sau primirea de produse si/sau servicii, nu se conditioneaza de consimtamantul persoanei vizate cu privire la utilizarea datelor sale in alte scopuri decat pentru



NEXTGEN

.communications

inițierea sau îndeplinirea unui contract. Acest lucru se aplică numai în cazul în care nu este posibil sau nu este posibil cu un motiv pentru persoana vizată în cauză să utilizeze servicii sau produse comparabile.

SECȚIUNEA 3

TRANSFERUL DATELOR CU CARACTER PERSONAL

17. Natura și scopul transferului datelor cu caracter personal

- (1) Datele cu caracter personal pot fi transferate numai în cazul în care partea care primește datele își asumă responsabilitatea datelor primite (transmisia) sau în cazul în care beneficiarul utilizează datele conform instrucțiunilor și cerințelor părții care transferă (acord de prelucrare a datelor încredințate).
- (2) Datele cu caracter personal sunt transferate numai în scopuri autorizate în conformitate cu punctul 10 din aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal ca parte a activității comerciale a companiei sau a obligațiilor legale, sau în urma obținerii consimțământului persoanelor vizate.

18. Transmiterea datelor

- (1) În cazul în care o companie transmite date către organisme care au sediul într-o altă țară sau care transferă date dincolo de granițele naționale, se vor lua măsuri pentru a se asigura că aceste date sunt transmise în mod corespunzător. Înainte de transmiterea datelor se stabilesc de comun acord cu destinatarul cerințe de confidențialitate și securitate a datelor. În plus, datele cu caracter personal, în special datele colectate în UE sau Zona Economică Europeană vor fi transmise operatorilor din afara Uniunii Europene numai dacă a fost asigurat un nivel adecvat de confidențialitate a datelor folosind aceste Reguli Corporatiste Obligatorii cu privire la datele cu caracter personal sau alte măsuri corespunzătoare cum ar fi clauzele standard contractuale ale UE sau acorduri contractuale individuale care îndeplinesc cerințele relevante ale legislației europene.
- (2) Pentru a se asigura securitatea datelor cu caracter personal, inclusiv pe durata transmiterii lor către o terță parte, se vor lua măsuri tehnice și organizatorice adecvate pe baza cerințelor Grupului Deutsche Telekom și standardelor tehnice și organizatorice general recunoscute.



NEXTGEN
communications

19. Prelucrarea datelor²

- (1) Atunci cand o companie (client) angajeaza o terta parte (contractor) pentru a furniza servicii in numele sau in conformitate cu instructiunile sale, atunci, acordul de prestari servicii incheiat intre parti va include suplimentar fata de serviciile care trebuie sa fie efectuate, si obligatiile contractorului ca parte contractata sa proceseze datele personale. Aceste obligatii stabilesc instructiunile clientului referitoare la tipul si modul de procesare a datelor cu caracter personal, scopul procesarii si masurile tehnice si organizatorice necesare pentru protectia datelor.
- (2) Contractorul nu poate utiliza datele cu caracter personal (care ii sunt incredintate pentru indeplinirea comenzii) pentru scopurile de procesare proprii sau ale unei terte parti, fara acordul prealabil al clientului. Contractorul trebuie sa informeze clientul in prealabil cu privire la orice planuri de a subcontracta munca catre alte terte parti, in scopul de a-si indeplini obligatiile contractuale. Clientul are dreptul de a se opune la folosirea unor astfel de subcontractori. Acolo unde folosirea subcontractorilor este permisa, contractorul ii va obliga sa se conformeze cu cerintele acordurilor incheiate intre contractor si client.
- (3) Subcontractorii vor fi selectati in functie de abilitatea lor de a indeplini cerintele mentionate mai sus.

² Aceasta sectiune nu reprezintă o prevedere in sensul WP 195 al art. 29, a grupului de lucru al Comisiei Europene;
NextGen Communications S.R.L. București, Șos. București-Ploiești, nr. 42-44, BBTP, Clădirea A, Aripa A2, Sector1, 013696
Tel: 021/316.78.84, Fax: 021/316.78.85, J40/11898/2008, CUI RO24166583, Cap. Soc. 50.564.200 RON

SECȚIUNEA 4

CALITATEA DATELOR SI SECURITATEA DATELOR

20. Calitatea datelor

- (1) Datele cu caracter personal trebuie sa fie corecte si, acolo unde este necesar, actualizate (calitatea datelor).
- (2) Avand in vedere scopul pentru care datele sunt procesate trebuie adoptate masuri adecvate care sa asigure stergerea, blocarea sau, daca este necesar, corectarea oricarei informatii incorecte sau incomplete.

21. Securitatea Datelor - masuri tehnice si organizatorice – protectia datelor conform principiilor privacy by design si privacy by default

Compania trebuie sa adopte masuri tehnice si organizatorice adecvate pentru procesele, sistemele si platformele IT utilizate pentru colectarea, prelucrarea sau intrebuintarea datelor in asa fel incat aceste date sa fie protejate.

Astfel de masuri trebuie sa includa:

- a) Prevenirea accesului persoanelor neautorizate la sistemele in cadrul carora datele sunt procesate sau intrebuintate (controlul privind accesul);
- b) Asigurarea faptului ca sistemele de procesare a datelor nu pot fi folosite de persoane neautorizate (controlul privind refuzul la utilizare);
- c) Asigurarea faptului ca persoanele autorizate pentru folosirea sistemelor de procesare a datelor au posibilitatea de a accesa in mod exclusiv datele la care acestea au acces autorizat si a faptului ca datele cu caracter personal nu pot, cu ocazia procesarii, intrebuintarii sau ulterior inregistrarii, sa fie citite, copiate, modificate sau sterse de persoane neautorizate (controlul accesului la date);
- d) Asigurarea faptului ca, in cursul transmiterii electronice sau cu ocazia transportului sau inregistrarii pe suporturi de date, datele cu caracter personal nu pot fi citite, copiate, modificate sau sterse de catre persoane neautorizate si a faptului ca este posibila verificarea si identificarea operatorilor spre care sunt transmise datele cu caracter personal prin



NEXTGEN
communications

intermediul echipamentului de transmitere a datelor (controlul asupra transmiterii datelor);

- e) Asigurarea posibilitatii de a examina si stabili ulterior daca si de catre cine au fost introduse, modificate sau sterse datele cu caracter personal din sistemele de procesare a datelor (controlul asupra introducerii datelor);
- f) Asigurarea faptului ca prelucrarea datelor cu caracter personal incredintate poate fi realizata (procesata) in conformitate cu instructiunile clientului (controlul asupra contractorului);
- g) Asigurarea faptului ca datele cu caracter personal sunt protejate impotriva distrugerii accidentale sau pierderii (controlul privind disponibilitatea);
- h) Asigurarea faptului ca datele cu caracter personal care au fost colectate pentru diferite scopuri pot fi procesate separat (regula separarii).

PARTEA A TREIA

DREPTURILE PERSOANELOR VIZATE

22. Dreptul de acces

(1) Persoanele vizate sunt îndreptăţite în orice moment să contacteze orice companie care le prelucraza datele și să solicite următoarele informații:

- a) Datele cu caracter personal reținute și care se referă la acestea, inclusiv proveniența și destinația acestora;
- b) Scopul prelucrării;
- c) Persoanele și operatorii cărora li se transmit datele în mod regulat, în special, dacă datele sunt transmise în străinătate;
- d) Prevederile prezentelor Reguli Corporatiste Obligatorii privind datele cu caracter personal.

(2) Informația relevantă trebuie să fie făcută accesibilă solicitantului, într-o formă inteligibilă și într-o perioadă rezonabilă de timp. Acest lucru se realizează, în general, într-o formă scrisă sau electronică. Furnizarea unei copii a prezentelor Reguli Corporatiste Obligatorii privind datele cu caracter personal ar trebui să reprezinte o modalitate suficientă pentru informarea solicitantului cu privire la cerințele sale.

(3) Acolo unde este permis de către legislația națională, o companie poate solicita o taxă pentru oferirea informațiilor.

23. Dreptul de a se opune, Dreptul de a solicita stergerea sau blocarea datelor și Dreptul de a solicita rectificarea datelor

(1) Persoanele vizate se pot opune, în orice moment, față de prelucrarea datelor ce îi vizează, dacă aceste date sunt utilizate în alte scopuri decât cele obligatorii din punct de vedere legal.

(2) Dreptul de a se opune trebuie să fie acordat și în cazul în care persoana vizată și-a exprimat anterior consimțământul față de prelucrarea datelor cu caracter personal ce o vizează.

(3) Solicitățile legitime privitoare la stergerea sau restricționarea datelor trebuie să fie aduse la îndeplinire de îndată. De asemenea, se vor respecta perioadele legale de retenție a datelor.

(4) Persoanele vizate pot solicita oricând companiei să corecteze datele cu caracter



definite de aceasta, daca aceste date sunt incomplete si/sau incorecte.

(5) In situatia in care retragerea sau stergerea datelor conduce la neindeplinirea obligatiilor contractuale, persoana vizata trebuie informata.

24. Dreptul la clarificare, Dreptul de a formula comentarii precum si Dreptul de a fi despagubit

(1) Daca persoana vizata sustine ca drepturile sale au fost incalcate prin prelucrarea ilegala a datelor sale cu caracter personal, in special prin obtinerea unor probe verificabile privitoare la violarea acestor Reguli Corporatiste Obligatorii, compania in cauza trebuie sa clarifice aceste fapte fara nici o intarziere. Pentru datele transferate sau transmise unor terte companii, in special din afara Uniunii Europene, compania aflata in Uniunea Europeana trebuie sa clarifice aceste fapte si sa obtina probe din care sa rezulte neviolarea de catre compania care a primit datele a cerintelor Regulilor Corporatiste Obligatorii, in caz contrar fiind responsabila de orice prejudiciu produs. Companiile vor lucra impreuna pentru a clarifica faptele si isi vor acorda acces reciproc la toate informatiile de care au nevoie pentru a face acest lucru.

(2) Persoana vizata poate inainta oricand o plangere impotriva Grupului Deutsche Telekom daca suspecteaza faptul ca o companie din cadrul Grupului Deutsche Telekom nu proceseaza datele sale cu caracter personal in conformitate cu cerintele legale sau cu prevederile prezentelor Reguli Corporatiste Obligatorii. Plangerea motivata va fi solutionata intr-o perioada de timp adecvata, iar persoana vizata va fi informata in consecinta in decurs de o luna de la data procesarii solicitarii . Aceasta perioada poate fi prelungita cu inca doua luni, daca este necesar, luand in considerare complexitatea si numarul de solicitari, persoana vizata fiind informata despre aceasta situatie.

(3) In cazul unei plangeri ce vizeaza mai multe companii, Ofiterul pentru Protectia Datelor cu caracter Personal al companiei cea mai familiarizata cu subiectul trebuie sa coordoneze toata corespondenta fata de persoana vizata. Ofiterul pentru Protectia Datelor cu caracter Personal al Grupului trebuie sa fie imputernicit sa isi exercite dreptul de subrogare si preluare a cazului in orice moment.

(4) Trebuie sa fie implementate canale adecvate pentru raportarea neregulilor privitoare la incidentele de protectia datelor cu caracter personal (cum ar fi un cont de mail organizat de Departamentul de Protectie a datelor, Departamentul Juridic si de Conformitate sau o persoana care poate fi contactata in mod direct pe internet).

(5) Ofiterul pentru Protectia Datelor cu Caracter Personal al companiei in cauza trebuie sa il informeze pe Ofiterul pentru Protectia Datelor cu caracter Personal al Grupului despre



NEXTGEN
communications

orice incident referitor la protectia datelor fara intarziere si prin utilizarea unor proceduri de raportare adecvate, care poate fi pusa la dispozitia autoritatilor, la cerere.

(6) Persoanele vizate pot inainta o plangere in baza Partii a V-a din prezentele Reguli Corporatiste Obligatorii privitoare la datele cu caracter personal daca drepturile lor au fost incalcate sau daca au suferit un prejudiciu.

25. Dreptul de a formula intrebari si plangeri

Orice persoana vizata are dreptul sa se adreseze in orice moment Ofiterului pentru protectia Datelor din cadrul companiei care ii proceseaza datele cu caracter personal prin intermediul formularii unor intrebari sau al unei plangeri referitoare la aplicarea prezentelor Reguli Corporatiste Obligatorii privitoare la datele cu caracter personal. Compania cea mai familiarizata cu acea situatie sau compania care a colectat datele persoanei vizate trebuie sa se asigure ca drepturile persoanei vizate sunt respectate in mod corespunzator si de catre celalalte companii raspunzatoare.

26. Exercitarea drepturilor de catre persoanele vizate

Persoanele vizate nu trebuie sa fie dezavantajate intrucat au facut uz de aceste drepturi. Forma prin care se comunica cu persoana vizata - ex., prin telefon, prin mijloace electronice sau in scris - trebuie sa respecte solicitarea persoanei vizate.

27. Copie tiparita a Regulilor Corporatiste Obligatorii privind datele cu caracter personal

O copie tiparita a acestor Reguli Corporatiste Obligatorii privind Datele cu Caracter Personal trebuie sa fie furnizata oricarei persoane care o solicita.



PARTEA A PATRA

ORGANIZAREA STRUCTURII DE PROTECTIE A DATELOR CU CARACTER PERSONAL

28. Responsabilitatea pentru procesarea datelor

Comaniile sunt obligate sa asigure conformitatea cu prevederile legale referitoare la protectia datelor si cu Regurile Corporatiste Obligatorii privitoare la datele cu caracter personal.

29. Ofiterul de Protectie a Datelor cu Caracter Personal

(1) Fiecare companie trebuie sa numeasca un Ofiter pentru Protectia Datelor cu Caracter Personal independent, a carui raspundere consta in asigurarea faptului ca fiecare departament individual al companiei este sfatuit asupra cerintelor interne si statutare ale companiei/Grupului cu privire la Confidentialitate si, in special, asupra acestor Reguli Corporatiste Obligatorii privind datele cu caracter personal. Ofiterul pentru protectia datelor cu caracter personal trebuie sa foloseasca masuri adecvate, in special inspectii aleatorii, pentru a monitoriza conformitatea cu prevederile referitoare la protectia datelor cu caracter personal.

(2) Compania trebuie sa se consulte cu Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului inainte de a numi un Ofiter pentru Protectia Datelor cu Caracter Personal propriu.

(3) Compania trebuie sa se asigure ca Ofiterul pentru Protectia Datelor cu Caracter Personal detine expertiza necesara pentru evaluarea aspectelor legale, tehnice si organizationale ale masurilor privind protectia datelor cu caracter personal.

(4) Compania trebuie sa ii ofere Ofiterului pentru Protectia Datelor cu Caracter Personal resursele financiare si de personal necesare pentru indeplinirea sarcinilor sale.

(5) Ofiterului pentru Protectia Datelor cu Caracter Personal trebuie sa ii fie garantat dreptul de a raporta direct catre managementul companiei si trebuie sa se afle, din punct de vedere organizational, in permanenta legatura cu managementul companiei.

(6) Ofiterul pentru Protectia Datelor cu Caracter Personal al fiecarei companii trebuie sa fie responsabil pentru implementarea cerintelor Ofiterului pentru Protectia Datelor cu Caracter Personal al Grupului si strategiei privitoare la protectia datelor cu caracter personal a Grupului Deutsche Telekom.



Toate departamentele companiei trebuie sa informeze Ofiterul pentru Protectia Datelor cu Caracter Personal in privinta oricarei evolutii a infrastructurii IT, a infrastructurii retelelor, modelelor de business, produselor, a datelor personalului si a planurilor de strategie corespunzatoare. Ofiterul pentru Protectia Datelor cu Caracter Personal trebuie sa fie implicat in orice moment in noile evolutii astfel incat sa se asigure faptul ca problemele legate de protectia datelor cu caracter personal vor fi avute in vedere si evaluate.



30. Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului

(1) Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului va coordona procesul de cooperare si solutionare a tuturor problemelor semnificative in privinta datelor cu Caracter personal din cadrul Grupului Deutsche Telekom. Acesta trebuie sa informeze CEO-ul Grupului Deutsche Telekom despre noile implementari si trebuie sa intocmeasca recomandari acolo unde este necesar.

(2) Este responsabilitatea Ofiterului pentru Protectia Datelor cu Caracter Personal al Grupului sa implementeze si sa dezvolte Politica Grupului Deutsche Telekom cu privire la confidentialitatea datelor si de a se consulta cu Ofiterii pentru Protectia Datelor cu Caracter Personal ai companiilor din cadrul Grupului atunci cand este necesar. Ofiterii pentru Protectia Datelor cu Caracter Personal trebuie sa implementeze politici privitoare la protectia datelor in cadrul companiei din care fac parte prin alinierea acestora la politicile Grupului. Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului si Ofiterii pentru Protectia Datelor cu Caracter Personal din cadrul companiilor nationale se vor intalni anual cu ocazia "Reuniunii Internationale a Liderilor cu atributii in domeniul Datelor cu Caracter Personal" in vederea impartasirii de informatii (intalniri in persoana).

31. Obligatia de a informa in caz de incalcare a prevederilor in materie

Compania in cauza trebuie sa isi informeze imediat Ofiterul pentru Protectia Datelor cu Caracter Personal despre orice incalcare sau indiciu despre orice incalcare a prevederilor referitoare la protectia datelor, in special a prezentelor Reguli Corporatiste Obligatorii. Ofiterul pentru Protectia Datelor cu Caracter Personal trebuie sa informeze imediat, la randul sau, Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului daca incidentul are un impact potential asupra publicului, afecteaza mai mult de o companie sau daca presupune o pierdere potentiala de peste 500.000 EUR. Ofiterul pentru Protectia Datelor cu Caracter Personal al companiei trebuie, de asemenea, sa informeze Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului daca au loc orice fel de modificari ale legilor aplicabile unei companii si care sunt nefavorabile semnificativ din punct de vedere al conformitatii cu aceste Reguli Corporatiste Obligatorii.

32. Verificarea nivelului de protectie a datelor cu caracter personal

(1) Verificarile pentru a evalua conformitatea cu cerintele prezentelor Reguli Corporatiste Obligatorii precum si a nivelului de protectie a datelor cu caracter personal trebuie sa fie realizate de Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului ca parte integranta a



NEXTGEN
communications

planului de inspecție anuală și a altor măsuri precum inspecțiile și raportările efectuate de către Ofiterii pentru Protecție a Datelor cu Caracter personal din cadrul companiilor.

(2) Auditorii interni și externi vor conduce inspecțiile Ofiterului pentru Protecția Datelor cu Caracter Personal al Grupului. De asemenea, se efectuează autoevaluări periodice în cadrul Grupului Deutsche Telekom care sunt conduse de către Ofiterul pentru Protecția Datelor cu Caracter Personal al Grupului. CEO-ul Grupului Deutsche Telekom trebuie să fie informat cu privire la rezultatele inspecțiilor relevante precum și cu privire la măsurile agreate ca atare. Autoritatea de supraveghere responsabilă trebuie să primească o copie a rezultatelor inspecțiilor în urma solicitării acesteia. Autoritatea de supraveghere responsabilă pentru companie poate și ea să inițieze o inspecție. Compania trebuie să ofere tot suportul necesar posibil pentru aceste inspecții și trebuie să implementeze măsurile rezultate din acestea.

(3) Compania trebuie să ia toate măsurile necesare pentru a remedia toate problemele identificate cu ocazia inspecției, iar Ofiterul pentru Protecția Datelor cu Caracter Personal al Grupului trebuie să monitorizeze implementarea acestor măsuri. Dacă compania nu reușește să implementeze aceste măsuri fără a da suficiente motive, Ofiterul pentru Protecția Datelor cu Caracter Personal al Grupului trebuie să verifice impactul asupra protecției datelor cu Caracter personal și să ia măsurile necesare, escaladând problema acolo unde este necesar.

(4) Ofiterii pentru Protecția Datelor cu Caracter Personal ai companiilor sau ai altor unități organizatorice împuternicite să conducă inspecțiile trebuie, de asemenea, să conducă verificări bazate pe planuri de audit dedicate documentate în scris, astfel încât să determine dacă companiile se conformează cu cerințele de protecție a datelor cu caracter personal.

(5) În absența unor restricții legale, Ofiterul pentru Protecția Datelor cu Caracter Personal al Grupului precum și Ofiterii pentru Protecția Datelor cu Caracter Personal ai companiilor trebuie să fie autorizați să verifice, pentru toate companiile, respectiv pentru propria companie, dacă datele cu caracter personal sunt procesate corespunzător. Companiile vizate trebuie să asigure Ofiterului pentru Protecția Datelor cu Caracter Personal al Grupului precum și Ofiterilor pentru Protecția Datelor cu Caracter Personal accesul complet la informațiile pe care aceștia le solicită în vederea evaluării și clarificării situației. Ofiterul pentru Protecția Datelor cu Caracter Personal al Grupului precum și Ofiterii pentru Protecția Datelor cu Caracter Personal ai companiilor trebuie să fie îndreptați să emită instrucțiuni în această privință.

(6) Ca parte integrantă a inspecțiilor, Ofiterii pentru Protecția Datelor cu Caracter Personal ai companiilor trebuie să folosească proceduri standardizate valabile pentru întregul Grup, ex. audit comun pentru protecția datelor, oriunde este posibil. Aceste proceduri pot fi puse la



33. Angajamentul angajatilor si instruirea acestora

(1) Companiile trebuie sa isi oblige angajatii, cel mai tarziu la momentul angajarii acestora, sa pastreze secretul datelor si telecomunicatiilor. Angajatii vor fi instruiti corespunzator in privinta protectiei datelor cu caracter personal ca parte a angajamentului acestora. Compania trebuie sa initieze procesele si sa procure resursele necesare pentru a indeplini aceste obligatii.

(2) Angajatii vor beneficia de formare in domeniul protectiei datelor cu caracter personal in mod regulat sau cel putin o data la 2 ani. Companiile trebuie sa fie imputernicite sa organizeze si sa sustina cursuri de formare dedicate pentru proprii angajati. Ofiterul pentru Protectia Datelor cu Caracter Personal al fiecarei companii trebuie sa pastreze dovada efectuarii acestor cursuri de formare si sa il informeze anual pe Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului in ceea ce priveste aceste aspecte.

(3) Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului poate pune la dispozitie la nivel central resurse si procese pentru obtinerea cursurilor de formare pentru angajatii Grupului Deutsche Telekom.

34. Cooperarea cu Autoritatile de Supraveghere

(1) Fiecare companie trebuie sa colaboreze cu incredere cu Autoritatea de supraveghere din tara in care activeaza sau care este reponsabila pentru transmiterea datelor cu caracter personal, in special, pentru a raspunde solicitarilor si a respecta recomandarile autoritatii.

(2) In eventualitatea unei schimbari a legislatiei aplicabile companiei care poate avea efecte adverse substantiale asupra garantiilor acordate de aceste Reguli Corporatiste Obligatorii, compania vizata trebuie sa notifice autoritatea de supraveghere responsabila despre aceasta schimbare.

35. Persoanele responsabile pentru solutionarea solicitarilor

Ofiterii pentru Protectia Datelor cu Caracter Personal ai companiilor sau Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului sunt persoanele responsabile cu solutionarea solicitarilor legate de aceste Reguli Corporatiste Obligatorii. Ofiterul pentru Protectia Datelor cu caracter Personal al Grupului trebuie sa furnizeze datele de contact ale Ofiterilor pentru Protectia Datelor cu Caracter Personal ai companiilor in urma unei astfel de solicitari.



NEXTGEN

communications

Ofițerul pentru Protecția Datelor cu caracter Personal al Grupului poate fi contactat la:

datenschutz@telekom.d privacy@telekom.de

+49-228-181-82001

În timpul orelor normale de lucru (Central European Time)

PARTEA A CINCEA

RASPUNDERE

36. Domeniul de aplicare a regulilor de raspundere

(1) Aceasta Parte a V-a din cadrul Regulilor Corporatiste Obligatorii se aplica exclusiv procesarii datelor cu caracter personal care se incadreaza in domeniul de aplicare a Regulamentului General privind Protectia Datelor 2016/679.

(2) In cadrul UE/SEE, se vor aplica, de asemenea, prevederile legale referitoare la raspundere din tara in care compania isi are sediul. Pentru datele care nu fac obiectul articolului 36, Sectiunea 1, al Regulilor Corporatiste Obligatorii, se vor aplica prevederile legale referitoare la raspundere din tara in care compania care a colectat datele isi are sediul inregistrat, sau daca nu exista astfel de prevederi legale, se vor aplica termenii si conditiile companiei care a colectat datele.

(3) Plata unor daune interese exemplare, atunci cand compania trebuie sa faca astfel de plati catre o persoana vizata care depasesc prejudiciul efectiv, este exclusa.

37. Persoana indreptatita la despagubiri

(1) Orice persoana care a suferit un prejudiciu in urma incalcarii obligatiilor prevazute in Regulile Corporatiste Obligatorii de catre o companie din Grupul Deutsche Telekom sau de catre persoana imputernicita catre care au fost transferate sau transmise datele cu caracter personal, are dreptul de a solicita despagubiri de la compania vizata din grupul Deutsche Telekom.

(2) Persoana vizata are dreptul de a solicita despagubiri si Grupului Deutsche Telekom. Daca compania mama plateste despagubiri, aceasta are dreptul de a se indrepta impotriva companiei responsabile pentru prejudiciul creat sau care a imputernicit tertul vinovat de producerea prejudiciului.

(3) Persoana vizata trebuie sa solicite despagubiri initial companiei care a transferat sau transmis datele cu caracter personal. Daca compania care a transmis datele nu este responsabila de jure sau de facto, persoana vizata este indreptatita sa solicite despagubiri companiei care a primit datele cu caracter personal (companiei imputernicite). Compania imputernicita nu are dreptul de a se sustrage de raspundere prin apelul la responsabilitatea unui contractor in cazul unei incalcari in aceasta privinta.



NEXTGEN
communications

(4) Persoana vizata are dreptul de a inainta, in orice moment, o plangere in fata Autoritatii de supraveghere responsabila din statul de resedinta sau Autoritatii de supraveghere a companiei mama a Grupului Deutsche Telekom.

38. Responsabilitatea de a face dovada

Responsabilitatea de a dovedi corecta procesare a datelor cu caracter personal ale persoanelor vizate, revine companiei responsabile.

39. Substituirea tertului in drepturile persoanei vizate

Daca persoana vizata nu are drepturi directe, ea trebuie sa fie indreptatita, in calitate de tert beneficiar, sa introduca plangere impotriva companiei care a incalcat obligatiile contractuale, in baza prezentelor Reguli Corporatiste Obligatorii privind datele cu caracter personal.

40. Competenta autoritatilor din punct de vedere teritorial

Ramanand la latitudinea persoanei vizate, autoritatile competente sa solutioneze plangerile referitoare la raspundere poate fi:

- a) cele de la resedinta persoanei vizate;
- b) cele din statul unde se afla compania membra a Grupului, sau
- c) cea de la sediului central din U.E. sau din statul European unde se afla compania membra a Grupului delegata cu responsabilitati in materia protectiei datelor cu caracter personal.

41. Arbitrajul

(1) Persoanele terte care considera ca drepturile lor referitoare la viata privata au fost incalcate ca urmare a unei posibile sau intrebuintari reale a datelor cu caracter personal au dreptul de a solicita ca Ofiterul pentru Protectia Datelor cu Caracter Personal al companiei vizate sa arbitreze aceasta situatie. Ofiterul pentru Protectia Datelor cu Caracter Personal este indreptatit sa examineze plangerea si sa sfatuiasca persoana vizata cu privire la drepturile ei. Cu aceasta ocazie, Ofiterul pentru Protectia Datelor cu Caracter Personal este obligat sa mentina confidentialitatea celorlalte date cu caracter personal ale reclamantului cu exceptia cazului in care reclamantul il elibereaza de aceasta obligatie. La cererea persoanei in cauza trebuie sa se incerce ajungerea la intelegere cu privire la plangerea formulata, cu participarea persoanei vizate si a Ofiterului



NEXTGEN
communications

pentru Protecția Datelor cu Caracter Personal. O astfel de înțelegere poate include și o recomandare cu privire la compensația pentru orice fel de daună suferită ca urmare a încălcării dreptului la intimitate al persoanei vizate. Această recomandare trebuie să fie obligatorie pentru companiile vizate dacă este aprobată prin exprimarea consimțământului.

(2) Dreptul de a înainta o plângere către autoritatea de supraveghere competentă de la domiciliul, locul de muncă sau de la locul săvârșirii încălcării, sau dreptul de a înainta o acțiune în fața instanței nu vor putea fi restricționate.

PARTEA A SASEA

PREVEDERI FINALE

42. Revizuirea si modificarea acestor Reguli Corporatiste Obligatorii

(1) Ofiterul pentru Protectia datelor cu Caracter Personal al Grupului trebuie sa examineze la intervale regulate de timp, dar cel putin o data pe an, aceste Reguli Corporatiste Obligatorii in scopul de a verifica conformitatea acestora cu prevederile legale aplicabile in materie si va face toate modificarile necesare in acest sens.

(2) Orice modificare semnificativa adusa prezentelor Reguli Coporatiste Obligatorii care devine, spre exemplu, necesara ca urmare a modificarii cerintelor legale, trebuie agreata impreuna cu autoritatea de supraveghere. Aceste amendamente se vor aplica direct pentru toate companiile care au semnat prezentele Reguli Corporatiste Obligatorii, ulterior trecerii unei perioade de timp adecvate pentru tranzitie.

(3) Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului trebuie sa informeze toate companiile care aplica aceste Reguli Corporatiste Obligatorii despre continutul modificarilor aduse.

(4) Ofiterii pentru protectia datelor cu caracter personal ai companiilor sunt obligati sa examineze daca amendamentele aduse acestor Reguli Corporatiste Obligatorii au vreo implicatie fata de conformitatea cu legea din propria tara sau daca intra in conflict cu prevederile legale din tara in cauza. Daca respectiva companie nu poate implementa modificarile din motive legale aceasta trebuie sa informeze de indata Ofiterul pentru Protectia Datelor cu Caracter Personal al Grupului si autoritatea de supraveghere responsabila si, daca este cazul, aplicarea acestor Reguli Corporatiste Obligatorii privind datele cu caracter personal va fi suspendata pentru compania in cauza.

43. Lista de contacte si companii

Ofiterul pentru Protectia Datelor cu Caracter personal al Grupului va tine o lista cu companiile care au implementat aceste Reguli Corporatiste Obligatorii si datele de contact ale acestor companii. Acesta trebuie sa pastreze lista actualizata si sa informeze, in urma unei solicitari,



NEXTGEN

communications

persoanele vizate, conform solicitarilor. O data pe an, autoritatea de supraveghere competenta va primi o lista actualizata a companiilor care au implementat prezentele Reguli Corporatiste Obligatorii privind prelucrarea datelor personale, intr-o modalitate obligatorie.

44. Norme de procedura/ Clauza de nulitate

Aceste Reguli Corporatiste Obligatorii privind datelor cu caracter personal vor fi guvernate in caz de conflict de legea procedurala a Republicii Federale Germane.

Daca anumite prevederi privite in mod independent din cadrul acestor Reguli Corporatiste Obligatorii sunt sau vor fi declarate nule, ele vor fi inlocuite cu alte prevederi care se apropie cel mai mult de intentia originala a acestor Reguli Corporatiste Obligatorii privind datele cu caracter personal. In caz de dubiu, se vor aplica prevederile Uniunii Europene privind datele cu caracter personal precum si in acele cazuri in care nu exista alte prevederi relevante.

45. Publicarea

Comaniile vor face publice intr-un mod adecvat drepturile persoanei vizate si clauza privind beneficiile tertilor, de exemplu sub forma unei anexe a sectiunii privind Protectia datelor cu caracter personal disponibile pe internet. Aceste informatii vor fi publicate imediat ce prezentele Reguli Corporatiste Obligatorii privind datele cu caracter personal au fost adoptate de catre companie.

PARTEA A SAPTEA

Definitii si Termeni

Anonimizarea

Reprezinta procesul prin care se schimba informatia de o asa maniera incat datele cu caracter personal si alte fapte nu mai pot conduce la o persoana fizica identificata sau identificabila sau nu mai pot conduce la o asemenea persoana fara un efort disproportionat de mare in timp, cost si energie.

Decizii individuale automate

Reprezinta acele decizii care au o implicare legala fata de persoana vizata sau care au un efect advers semnificativ asupra acesteia si care sunt bazate numai pe prelucrarea automata a datelor menite sa evalueze anumite aspecte personale ale persoanei vizate cum ar fi, performanta de la locul de munca al lui/ei, bonitatea, increderea, conduita etc.

Compania

Reprezintă orice companiei care obiectul prezentelor Reguli Corporatiste Obligatorii privind prelucrarea datelor personale. O lista distincta a acestor companii, va fi tinuta pentru scopuri de referinta si actualizata in mod regulat. Lista va putea fi vizualizata de orice persoana in orice moment.

Operator

Orice persoana fizica sau juridica care determina scopul procesarii datelor cu caracter personal.

Persoana vizata

Reprezinta orice persoana fizica ale carei date cu caracter personal sunt procesate in interiorul Grupului Deutsche Telekom.

Reprezinta orice persoana fizica sau juridica, autoritate publica, agentie sau orice alta forma legala careia ii sunt dezvaluite date cu caracter personal, indiferent daca este o persoana terta sau nu. In orice caz, autoritatile publice care pot primi date cu caracter personal ca urmare a unei cereri individuale nu trebuie considerate destinatari.

Grupul Deutsche Telekom

Reprezinta societatea pe actiuni Deutsche Telekom AG precum si toate celalalte companii la care Deutsche Telekom A.G. detine mai mult de 50% din actiuni, sau care sunt consolidate de catre acesta.

Compania Mama

Compania Mama este in prezent reprezentata de Deutsche Telekom A.G. cu sediul principal in Bonn, Aleea Friedrich -Ebert nr. 140, cod postal 53113, Germania.

Date cu caracter personal

Reprezinta orice informatie referitoare la o persoana fizica identificata sau identificabila (persoana vizata); o persoana identificabila este o persoana care poate fi identificata , direct sau indirect, in special printr-o referinta la un numar de identificare sau la unul sau mai multi factori specifici fizicului, psihicului, mentalului, economicului, culturalului sau identitatii sale sociale.

Pseudonimizarea

Inseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

Prelucrarea

Inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la



NEXTGEN
communications

dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

Categorii speciale de date cu caracter personal

Inseamnă orice date care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice

Parte Terta

Inseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal

