

# **Kódex ochrany práv jednotlivca pri práci s osobnými údajmi v skupine Deutsche Telekom Group**

## **Preambula a úvodná časť**

(1) V súvislosti s rozširovaním používania počítačových sietí pri spracovaní informácií a pri práci s komunikačnými systémami je ochrana osobných údajov zákazníkov, obchodných partnerov, zamestnancov a akcionárov dôležitá vo všetkých spoločnostiach v rámci Deutsche Telekom Group na celom svete.

(2) Najdôležitejším cieľom týchto Pravidiel je preto vytvorenie jednotnej a kvalitnej ochrany údajov v Deutsche Telekom Group na celom svete. Predovšetkým pri medzinárodnom toku údajov je potrebné zaručiť, aby príjemca spracúval osobné údaje podľa zásad zákona na ochranu údajov, ktoré platia pre odosielateľa takýchto údajov.

(3) Spoločnosti skupiny Deutsche Telekom Group si uvedomujú, že úspech firmy Deutsche Telekom ako celku závisí nielen od celosvetovej siete na tok informácií, ale tiež predovšetkým od dôveryhodnej a bezpečnej manipulácie s osobnými údajmi.

(4) V mnohých oblastiach vnímajú zákazníci formu Deutsche Telekom ako jeden celok. Preto spoločnostiam združeným v tejto skupine záleží na tom, aby dôležitým spôsobom prispievali k úspechu tejto firmy a aby podporovali jej zámer poskytovať vysoko kvalitné produkty a služby na základe implementácie týchto Pravidiel.

## **Prvá časť**

### **Rozsah a použitie**

#### **§ 1 Právna povaha týchto Pravidiel**

Tieto Pravidlá predstavujú smernicu, ktorá je záväzná pre celú skupinu Deutsche Telekom Group a ktorá vstupuje do platnosti, keď ju prijme a uverejní vedenie príslušnej spoločnosti. Týka sa manipulácie so všetkými osobnými údajmi fyzických osôb, najmä údajov zákazníkov, akcionárov, zamestnancov a iných tretích strán, zmluvných strán alebo obchodných partnerov.

#### **§ 2 Platné právne ustanovenia**

(1) Zámerom zásad uvedených ďalej je zaručiť v celej skupine Deutsche Telekom Group rovnako vysokú úroveň ochrany údajov. Tieto zásady však nenahrádzajú požadované – a podľa potreby zákonné – podmienky, ktoré musia existovať, aby sa manipulácia s osobnými údajmi stala zákonnou. Tieto Pravidlá nemajú vplyv na akékoľvek záväzky a predpisy týkajúce sa jednotlivých spoločností pokiaľ ide o spracovanie a používanie osobných údajov, ktoré presahujú nasledujúce zásady, alebo ktoré obsahujú ďalšie obmedzenia týkajúce sa spracovania a používania osobných údajov. Bez ohľadu na to, čo bolo uvedené vyššie spoločnosti súhlasia s tým, že zákony platné pre jednotlivé spoločnosti im nebudú brániť v plnení svojich povinností podľa týchto Pravidiel.

(2) Údaje zhromaždené v Európe sa musia spracúvať podľa zákonných ustanovení krajiny, kde boli zhromaždené, a to aj vtedy, keď ide o prenos do zahraničia.

(3) Zber osobných údajov a ich prenos na verejné orgány musí prebiehať v súlade s povinnými zákonnými ustanoveniami danej krajiny (ak takýto zber neprebieha v rámci normálnych zmluvných zákazníckych vzťahov).

(4) Tento Kódex podlieha zákonom Spolkovej republiky Nemecko.

### **§ 3 Ukončenie**

Ukončenie platnosti týchto Pravidiel (bez ohľadu na čas, okolnosti a príčiny) nezavaruje spoločnosti povinnosti a vyplývajúcich z ustanovení týchto Pravidiel týkajúcich sa spracovania už prenesených údajov.

## **Druhá časť**

### **Zásady**

#### **Článok 1**

### **Transparentnosť spracovania údajov**

#### **§ 4 Povinnosť informovať**

Subjekty ktoré poskytli údaje musia mať jednoduchý prístup k informáciám o primeranej manipulácii s ich osobnými údajmi, napríklad prostredníctvom uverejnenia zásad utajovania údajov a týchto Pravidiel na internete.

#### **§ 5 Obsah a forma informácií**

(1) Osoby ktoré poskytli údaje musia dostať primerané informácie

a) o spracovateľovi údaje, a o jeho kontaktných údajoch

b) o predpokladanom rozsahu a účele zberu, spracovania a/alebo použitia osobných údajov; v tejto informácii by malo byť uvedené, ktoré údaje sa nahrávajú a spracúvajú či používajú, a prečo, na aký účel a na aký dlhý čas sa to robí

c) o príjemcovi, rozsahu a účeloch prípadného poskytovania údajov tretím stranám

d) o spôsobe spracovania a používania údajov, najmä ak sa budú spracúvať a používať v zahraničí

e) o ich zákonných právach (pozri článok 7).

(2) Bez ohľadu na zvolené médium musia osoby, ktoré poskytli údaje, dostať tieto údaje jasným a ľahko zrozumiteľným spôsobom.

#### **§ 6 Dostupnosť informácií**

Pre osoby, ktoré poskytli údaje, musia byť informácie dostupné v čase, keď sa zber údajov začína, a potom vždy na požiadanie.

## **§ 7 Súhlas**

(1) S výnimkou prípadov, kedy zber, spracovanie alebo použitie údajov súvisí s uzatváraním alebo plnením zmluvy, alebo keď existuje iné zákonné oprávnenie, je potrebné získať súhlas osoby, ktorá poskytla údaje najneskôr v čase, keď sa začína zber, spracovanie alebo používanie údajov.

(2) Okrem povinnosti informovať (pozri vyššie) je potrebné v súvislosti so súhlasom dodržiavať nasledovné:

### **a) Obsah**

Súhlas musí byť výslovný, dobrovoľný a musí byť poskytnutý na základe informovanosti osoby, ktorá údaje poskytuje, a to predovšetkým o rozsahu tohto súhlasu a o dôsledkoch neposkytnutia súhlasu. Vyhlásenie o poskytnutí súhlasu musí mať dostatočne presné znenie a musí informovať osoby, ktoré poskytujú údaje o tom, že majú právo svoj súhlas hocikedy odvolať.

### **b) Forma**

Forma súhlasu musí zodpovedať okolnostiam (bežne býva písomná alebo elektronická). Vo výnimočných prípadoch sa môže súhlas poskytnúť ústne (ak táto forma súhlasu a osobitné okolnosti s ňou súvisiace sú primerané a sú dostatočným spôsobom zdokumentované).

## **Článok 2**

### **Použitie na osobitné účely**

## **§ 8 Princíp**

Osobné údaje je prípustné použiť len na tie účely, na ktoré sa pôvodne získali.

## **§ 9 Zákaz podmieňovania**

Nie je prípustné podmieňovať používanie služieb či obdržanie výrobkov alebo služieb poskytnutím súhlasu na použitie osobných údajov na iné účely ako uzatváranie alebo plnenie zmluvy, avšak iba vtedy, ak osoba, ktorá poskytla údaje, nemôže porovnateľné služby alebo výrobky používať.

## **Článok 3**

### **Osobitné prípady spracovania údajov**

## **§ 10 Priamy marketing**

(1) Osoby ktoré poskytli údaje musia byť informované o tom, že môžu hocikedy namietať voči používaniu svojich osobných údajov na účely priameho marketingu. Ďalej musia byť informované o povahe, obsahu a období, v rámci ktorých je možné ich osobné údaje na účely priameho marketingu použiť.

(2) Osoby ktoré poskytli údaje musia byť informované o tom, že majú právo na námietky, ak dostanú správu o priamom marketingu. Okrem toho musia osoby, ktoré poskytli údaje dostať primerané nástroje na uplatňovanie svojho práva na to, aby takéto správy nedostávali. Musia dostať najmä informácie o tom, komu treba takéto námietky adresovať.

(3) Osobitné zákonné ustanovenia podľa druhej vety paragrafu 2 (1) týchto Pravidiel, podľa ktorej používanie osobných údajov závisí od súhlasu osoby, ktorá ich poskytuje majú prednosť pred ostatnými ustanoveniami..

### **§ 11 Automatizované rozhodnutia**

(1) Rozhodnutia týkajúce sa individuálnych aspektov určitej osoby a ktoré môžu mať za následok právne dôsledky alebo závažný negatívny dopad pre túto osobu nesmú byť založené výlučne na automatickom spracovaní. Ide predovšetkým o rozhodnutia, pre ktoré sú dôležité údaje o dôveryhodnosti, profesionálnej vhodnosti alebo zdravotnom stave osoby, ktorá poskytla osobné údaje.

(2) Ak je v jednotlivých prípadoch objektívne potrebné použiť automatizované rozhodnutia, musí osoba, ktorá poskytla osobné údaje, dostať ihneď informáciu o výsledku automatizovaného rozhodnutia a musí dostať príležitosť na pripomienkovanie v primeranej lehote. Pripomienky osôb, ktoré poskytli osobné údaje sa musia pred konečným rozhodnutím vziať vhodným spôsobom do úvahy.

### **§ 12 Osobitné kategórie osobných údajov**

(1) Manipulácia s osobitnými kategóriami osobných údajov musí podliehať jednoznačnej právnej autorizácii alebo prechádzajúcemu súhlasu osoby, ktorá poskytla osobné údaje. Pripúšťa sa aj v prípadoch, kedy je potrebné údaje spracovať v rámci plnenia práv a povinností zodpovedného orgánu v oblasti pracovného práva, za predpokladu, že je to prípustné podľa zákonov danej krajiny, ktoré zabezpečujú primerané záruky.

(2) Pred začatím takéhoto zberu, spracovania alebo používania je potrebné písomne kontaktovať oddelenie na ochranu údajov príslušnej firmy a poradiť sa o všetkých prípadoch kedy je toto potrebné. Je potrebné riadnym spôsobom vziať do úvahy povahu, rozsah, účel, potrebu a právny základ použitia takýchto údajov.

## **Článok 4**

### **Kvalita údajov, hospodárnosť údajov a obmedzenie používania údajov**

#### **§ 13 Kvalita údajov**

(1) Osobné údaje musia byť vždy správne a v prípade potreby vždy aktuálne (kvalita údajov).

(2) Podľa účelu, na ktorý sa údaje získavajú, spracúvajú alebo používajú je potrebné urobiť primerané opatrenia na to, aby sa zabezpečilo vymazanie či oprava všetkých neúplných informácií.

#### **§ 14 Hospodárnosť údajov, obmedzenie používania údajov, anonymizácia a pseudonymizácia**

(1) Osobné údaje musia byť primerané, relevantné a nie nadmerné pokiaľ ide o používanie na osobitný účel (hospodárnosť údajov). Údaje sa musia spracúvať len v rámci určitej aplikácie, a to vtedy, keď je to potrebné (obmedzenie používania údajov).

(2) Ak je to možné a ekonomicky primerané, je potrebné používať postupy na vymazanie identifikačných prvkov osôb, ktoré poskytli údaje (anonymizácia), alebo na náhradu týchto prvkov inými charakteristikami (pseudonymizácia). Anonymizácia a pseudonymizácia sa musí robiť tak, aby nebolo možné zistiť pôvodnú totožnosť osôb, ktoré poskytli údaje, alebo aby na takéto zistenie bolo potrebné neprimerane veľké úsilie.

## **§ 15 Profilovanie, štatistické rozbory**

(1) Pomocou organizačných a technických opatrení v súlade s primeranými koncepciami súčasného stavu alebo techniky je potrebné zabezpečiť, aby profilovanie (napr. profily pohybu, používateľov, spotreby) nebolo možné inak ako na základe jednoznačného zákonného povolenia alebo predchádzajúceho súhlasu osoby, ktorá poskytla osobné údaje.

(2) Táto výhrada sa netýka čisto štatistických rozborov alebo štúdií s použitím anonymizovaných alebo pseudonymizovaných údajov.

## **§ 16 Archivovanie údajov**

Pri vypracúvaní pravidiel na archivovanie údajov je potrebné brať do úvahy zásady spracovania údajov, najmä zásadu hospodárnosti údajov a obmedzenia používania údajov. Osobné údaje sa nesmú archivovať bez jednoznačného súhlasu osoby, ktorá ich poskytla; výnimku tvoria prípady, kedy to vyžadujú prevádzkové dôvody alebo zákon.

# **Článok 5**

## **Obmedzenie ďalšieho poskytovania**

### **§ 17 Poskytovanie údajov tretím stranám**

(1) Poskytovanie osobných údajov tretím stranám musí mať právny základ. Toto môže nastať, lebo je potrebné splniť zmluvnú požiadavku voči osobe, ktorá poskytla osobné údaje, alebo vtedy, ak takáto osoba zabezpečila svoj súhlas.

(2) Odsek 1 neplatí, ak v danej krajine existujú obmedzenia, najmä z dôvodov bezpečnosti štátu, národnej obrany, verejnej bezpečnosti alebo prevencie, vyšetrovania alebo súdneho stíhania trestných činov, pri ktorých sa požaduje poskytnutie osobných údajov na uvedené účely.

### **§ 18 Zodpovednosť**

(1) Pri poskytovaní údajov tretím stranám, ktoré nie sú verejnými orgánmi musí firma, ktorá takéto údaje pôvodne získala, zabezpečiť ich spracovanie alebo používanie v súlade so zákonom. Pred poskytnutím (prenosom) takýchto údajov je potrebné s príjemcom prerokovať a odsúhlasiť primeranú ochranu a bezpečnosť týchto údajov. Pri uzatváraní dohôd s inštitúciami v krajinách, kde nemajú zavedenú primeranú ochranu údajov je potrebné zabezpečiť primerané záruky pokiaľ ide o ochranu práva jednotlivca na súkromie a o uplatňovanie práv s tým spojených.

(2) V súlade so všeobecne prijatými normami treba prijať primerané technicko-organizačné opatrenia na zabezpečenie úplnosti a bezpečnosti údajov počas prenosu tretej strane.

### **§ 19 Spracovanie údajov prostredníctvom subdodávky**

(1) Keď si firma objedná služby od subdodávateľa, musí zmluva s ním okrem dohody o službách a práce, ktorú má subdodávateľ vykonať obsahovať aj určenie povinností subdodávateľa ako zmluvnej strany, ktorá zabezpečuje spracovanie údajov. Tieto povinnosti budú obsahovať pokyny danej firmy (jednotky na riadenie údajov) týkajúce sa druhu a spôsobu spracovania osobných údajov, účelu spracovania a technicko-organizačných opatrení potrebných na ochranu údajov. Rovnakým spôsobom platí tretia veta paragrafu 18 (1) týchto Pravidiel.

(2) Bez predchádzajúceho súhlasu jednotky na riadenie údajov nesmie subdodávateľ takéto osobné údaje použiť na účely vlastného spracovania alebo spracovania treťou stranou. Ak takýto súhlas dostane, je potrebné dohodnúť vyššie uvedené pravidlá aj s takýmto subdodávateľom či subdodávateľmi.

(3) Výber subdodávateľov sa bude robiť na základe ich schopností splniť vyššie uvedené požiadavky.

## Článok 6

### Ochrana údajov, organizácia a bezpečnosť údajov

#### § 20 Zodpovedná osoba pre ochranu údajov

(1) Každá firma musí určiť Zodpovednú osobu pre ochranu údajov, ktorá bude mať za úlohu zabezpečiť, aby jednotlivé oddelenia dostávali správy o zákonných alebo interných požiadavkách a o stratégii ochrany údajov a súkromia.

(2) Zodpovedná osoba pre ochranu údajov sa musí zaoberať navrhovaním nových výrobkov a služieb od samého začiatku, aby boli v súlade so zásadami, ktoré sú stanovené v týchto Pravidlách.

#### § 21 Kontrola stupňa ochrany údajov

Za účelom sledovania účinnosti a úspešnosti používaných technicko-organizačných opatrení na ochranu údajov je potrebné pravidelne kontrolovať stupeň ochrany údajov (napríklad pomocou revízie ochrany údajov). Takúto revíziu môže robiť interne Zodpovedná osoba na ochranu údajov, iné organizačné zložky, ktoré boli poverené vykonaním takejto revízie, prípadne nezávislá externá organizácia, ktorú schválila jednotka na riadenie údajov. Základom pre určenie stupňa ochrany údajov budú požiadavky zákonnej a podnikovej stratégie platné pre danú organizačnú jednotku, ako aj požiadavky uvedené v týchto Pravidlách.

#### § 22 Technicko-organizačné opatrenia a opatrenia týkajúce sa zamestnancov

Na začiatku pracovného pomeru v danej firme je potrebné so zamestnancami dojednať primerané podmienky týkajúce sa zachovávaní dôvernosti. Ďalej je potrebné vypracovať primerané technicko-organizačné opatrenia týkajúce sa manipulácie s osobnými údajmi pre procesy v rámci firmy a pre systémy informačných technológií.

Takéto opatrenia musia zabezpečiť

- a) aby neoprávnené osoby nemali prístup k systémom na spracovanie údajov, na ktorých sa spracúvajú alebo používajú osobné údaje (kontrola prístupu osôb);
- b) aby neoprávnené osoby nemohli používať systémy na spracovanie údajov (kontrola odmietnutia používania);
- c) aby osoby, ktoré majú oprávnenie na používanie systému na spracovanie údajov mali prístup len k tým údajom, na ktoré majú oprávnenie, a aby počas spracovania alebo používania alebo po nahratí neoprávnené osoby nemali možnosť osobné údaje čítať, kopírovať, meniť alebo odstraňovať (kontrola prístupu k údajom);

- d) aby v priebehu elektronického prenosu, prepravy alebo nahrávania na nosič údajov neoprávnené osoby nemohli osobné údaje čítať, kopírovať, meniť alebo odstraňovať, a aby bolo možné skontrolovať a určiť, kam sa osobné údaje majú prostredníctvom zariadenia na prenos údajov prenášať (kontrola prenosu údajov);
- e) aby bolo možné spätne skontrolovať a určiť, či boli osobné údaje vložené do systému na spracovanie údajov, zmenené alebo odstránené, a kto tak urobil (kontrola zápisu údajov);
- f) aby sa osobné údaje ktoré spracúvajú subdodávatelia vždy spracúvali v súlade s pokynmi objednávateľa (kontrola subdodávateľov);
- g) aby osobné údaje boli chránené pred náhodným zničením alebo stratou (kontrola dostupnosti);
- h) aby sa údaje, ktoré boli získané na rôzne účely spracúvali osobitne (pravidlo osobitného spracovania).

## **Článok 7**

### **Práva osôb, ktoré poskytli osobné údaje**

#### **§ 23 Právo na dotazy a sťažnosti**

Každá osoba, ktorá poskytla osobné údaje, má právo hocikedy sa obrátiť na oddelenie ochrany údajov príslušnej firmy s otázkami a sťažnosťami týkajúcimi sa aplikácie týchto Pravidiel. Ak nebude neskôr stanovené inak, pre účely týchto ustanovení sa za príslušnú firmu považuje každá firma, ktorá má zmluvný vzťah s osobou, ktorá poskytla osobné údaje, alebo ktorá spracúva osobné údaje takejto osoby. Firma, na ktorú sa takáto osoba obrátila, musí preveriť, či ostatné príslušné firmy riadne dodržiavajú práva tejto osoby.

#### **§ 24 Právo na informácie**

(1) Každá osoba, ktorá poskytla osobné údaje môže od príslušnej firmy hocikedy požadovať informácie týkajúce sa

- a) zaznamenaných osobných údajov o nej, ako aj ich pôvodu a príjemcu či príjemcov;
- b) účelu spracovania alebo použitia takýchto údajov;
- c) osôb a jednotiek, ktorým sa takéto údaje pravidelne posielajú, najmä ak ide o posielanie takýchto údajov do zahraničia;
- d) ustanovení týchto Pravidiel.

(2) Príslušné informácie musí opytujúci sa dostať v zrozumiteľnej forme a v primeranej lehote, zvyčajne písomne alebo elektronicky.

(3) Ak to umožňujú zákony v danej krajine, môže firma požadovať za poskytnutie príslušných informácií určitý poplatok.

#### **§ 25 Právo na protest/Právo na vymazanie či zablokovanie údajov**

(1) Osoba, ktorá poskytla osobné údaje môže u príslušnej firmy protestovať proti použitiu jej údajov, ak má na to právo.

(2) Toto právo na protest bude platiť aj v prípade, keď osoba, ktorá poskytla osobné údaje predtým súhlasila s použitím jej údajov.

(3) Oprávnené požiadavky na vymazanie alebo zablokovanie údajov budú ihneď splnené. Takéto požiadavky sú oprávnené najmä v prípade, ak prestane platiť právny základ pre používanie príslušných údajov. Ak má osoba, ktorá poskytla osobné údaje právo na vymazanie svojich údajov, avšak údaje nie je možné vymazať alebo ich nie je možné vymazať s vynaložením primeraného úsilia, je potrebné takéto údaje pred nepovoleným používaním chrániť zablokovaním. Je potrebné dodržať zákonné lehoty zadržania.

## **§ 26 Právo na opravu**

Osoba, ktorá poskytla osobné údaje môže hocikedy požadovať, aby príslušná firma opravila u nej zaznamenané osobné údaje, pokiaľ sú takéto údaje neúplné alebo nesprávne.

## **§ 27 Právo na vysvetlenie a na pripomienky**

(1) Ak osoba, ktorá poskytla osobné údaje tvrdí, že jej údaje boli zneužitú pri nezákonom spracovaní údajov, najmä ak boli porušené tieto Pravidlá, sú príslušné firmy povinné bez trestuhodného omeškania tieto skutočnosti objasniť. V takomto prípade sú povinné navzájom úzko spolupracovať a zabezpečiť si navzájom prístup ku všetkým informáciám potrebným na objasnenie problémov spojených s daným prípadom.

(2) Všetku korešpondenciu s osobou, ktorá poskytla osobné údaje musí koordinovať oddelenie ochrany informácií tej firmy, ktorá je najviac zodpovedná za príslušné problémy.

## **§ 28 Uplatňovanie práv osôb, ktoré poskytli osobné údaje**

Nie je prípustné, aby osoby, ktoré poskytli osobné údaje boli v nevýhode v dôsledku toho, že využili tieto práva. Spôsob komunikácie s osobou, ktorá poskytla osobné údaje (telefonicky, elektronicky alebo písomne) by sa mal podľa možnosti zvoliť podľa požiadavky takejto osoby.

# **Článok 8**

## **Riadenie procesu ochrany údajov/Povinnosti a zodpovednosť**

### **§ 29 Zodpovednosť za spracovanie údajov**

(1) V rámci svojej funkcie spojenej s riadením údajov sú firmy povinné, najmä v priamom jednaní s osobami, ktoré poskytli osobné údaje, zabezpečiť dodržiavanie požiadaviek týkajúcich sa ochrany údajov, ako aj ustanovení týchto Pravidiel.

(2) Zodpovedná osoba pre ochranu údajov príslušnej firmy musí byť ihneď informovaná o akomkoľvek porušení (aj o podozrení z porušenia) ustanovení týkajúcich sa ochrany údajov a týchto Pravidiel. Ak ide o incidenty, ktoré sa týkajú viacerých firiem je potrebné o tom informovať aj hlavné oddelenie zachovávanie utajenia celej skupiny. Zodpovedná osoba pre ochranu údajov príslušnej firmy je povinný informovať oddelenie zachovávanie utajenia celej skupiny aj o akýchkoľvek zmenách zákonov, ktoré sa týkajú firmy, a ktoré sú výrazne nepriaznivé.

(3) Oddelenia ochrany údajov jednotlivých firiem sú povinné koordinovať svoju činnosť v rámci stratégie ochrany údajov v rámci celej skupiny, a taktiež sa navzájom podporovať a využívať existujúce prostriedky na súčinnosť.



### **§ 30 Koordinácia zo strany Zodpovednej osoby celej skupiny pre utajovanie**

(1) Zodpovedná osoba celej skupiny pre utajovanie je povinný koordinovať proces spolupráce a zhadu vo všetkých významných bodoch týkajúcich sa ochrany údajov. Koordinačný výbor skupiny Deutsche Telekom pre ochranu údajov bude slúžiť ako koordinačný orgán.

(2) Zodpovedná osoba celej skupiny pre utajovanie je povinný rozvíjať a vypracúvať stratégiu skupiny pre oblasť ochrany údajov. V tejto problematike sa do koordinácie musia zapojiť aj oddelenia ochrany údajov jednotlivých firiem.

### **§ 31 Povinnosti v oblasti dozoru a poradenstva**

(1) Zodpovedné osoby pre ochranu údajov v jednotlivých firmách budú mať za úlohu sledovať dodržiavanie domácich a medzinárodných predpisov týkajúcich sa ochrany údajov a týchto Pravidiel. V tejto súvislosti sú všetky oddelenia príslušných firiem povinné informovať príslušnú Zodpovednú osobu pre ochranu údajov o stave v danej oblasti a o plánoch do budúcnosti.

(2) Ak nebudú k dispozícii zákonné obmedzenia, budú príslušní Zodpovedné osoby pre ochranu údajov oprávnení kontrolovať priamo na mieste všetky metódy spracovania, v rámci ktorých sa používajú osobné údaje.

(3) Podľa potreby a v rámci svojich povinností týkajúcich sa kontroly sú úseky ochrany údajov jednotlivých firiem povinné používať mechanizmy, ktoré sú v celej skupine jednotné, t.j. spoločné previerky ochrany údajov.

### **§ 32 Školenie a povinnosti zamestnancov**

(1) Zamestnanci jednotlivých firiem musia byť dostatočne vyškolení pokiaľ ide o predpisy týkajúce sa ochrany údajov a o aplikáciu týchto Pravidiel.

(2) Jednotlivé firmy sú povinné v spolupráci s príslušnými oddeleniami ochrany údajov vypracovať vhodné materiály na školenie zamestnancov.

### **§ 33 Spolupráca s dozornými orgánmi**

(1) Jednotlivé firmy sú povinné súhlasiť s tým, že budú v primeranej lehote a rozsahu odpovedať na dotazy dozorného orgánu ktorému podliehajú, alebo ktorým podlieha firma, ktorá údaje vyváža, a že budú dodržiavať odporúčania takéhoto dozorného orgánu.

(2) Ak dôjde k zmene právnych predpisov týkajúcich sa niektorej firmy, ktorá by mohla podstatným spôsobom nepriaznivo ovplyvniť záruky poskytované týmito Pravidlami, bude príslušná firma o takejto zmene informovať príslušný dozorný orgán.

## Článok 9

### Odborné názvy a definície

#### Automatizované jednotlivé rozhodnutia

sú rozhodnutia, ktoré majú za následok právny vplyv na osobu, ktorá poskytla osobné údaje, alebo ktoré ju závažným spôsobom ovplyvňujú, a ktoré sú založené výlučne na automatizovanom spracovaní údajov so zámerom vyhodnotiť určité osobné aspekty s touto osobou súvisiace, napríklad jej výkonnosť v práci, dôveryhodnosť, spoľahlivosť, správanie sa a pod.

#### Osoba, ktorá poskytla osobné údaje

je fyzická osoba, s ktorej osobnými údajmi sa manipuluje v skupine Deutsche Telekom Group.

#### Zodpovedná osoba

je osoba, ktorá sama alebo spolu s inými určuje účely a spôsoby spracovania osobných údajov.

#### Deutsche Telekom Group

je spoločnosť Deutsche Telekom AG a všetky firmy, v ktorých má spoločnosť Deutsche Telekom AG priamo alebo nepriamo viac ako 50% akcií, alebo ktoré riadi.

#### Spracovateľ údajov

je každá fyzická alebo právnická osoba, verejný orgán, agentúra alebo iný orgán, ktorý spracúva osobné údaje v mene spracovateľa údajov (spracovanie údajov na základe subdodávky).

#### Firma

je každá firma či spoločnosť, ktorá súhlasí s tým, že bude dodržiavať tieto Pravidlá, a ktorá je uvedená v Prílohe A k týmto Pravidlám.

#### Osobné údaje

sú všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (osoby, ktorá poskytla osobné údaje); identifikovateľná osoba je taká, ktorú je možné priamo alebo nepriamo identifikovať, najmä podľa identifikačného čísla alebo podľa jedného alebo viacerých činiteľov špecifických pre jej fyzickú, fyziologickú, mentálnu, ekonomickú, kultúrnu alebo spoločenskú identitu.

#### Manipulácia s osobnými údajmi

je každá operácia alebo sled operácií s osobnými údajmi (zber, záznam, organizácia, uchovávanie, úpravy alebo zmeny, vyhľadávanie, nahliadnutie, používanie, oznamovanie prenosom, šírenie alebo dávanie k dispozícii iným spôsobom, zosúladovanie alebo kombinácia, blokovanie, vymazanie alebo zničenie). Patrí sem aj spracovanie osobných údajov v štruktúrovaných manuálnych súboroch.

## **Príjemca**

je každá fyzická alebo právnická osoba, verejný orgán, agentúra alebo iný orgán, ktorému sa údaje oznamujú, bez ohľadu na to, či ide o tretiu stranu alebo nie. Za príjemcov sa však nepovažujú verejné orgány, ktoré dostávajú údaje ako súčasť jediného dotazu.

## **Osobitné kategórie údajov**

sú údaje o rasovom alebo národnostnom pôvode, politických názoroch, náboženskej alebo filozofickej viere, členstve v odborových organizáciách, zdravotnom stave alebo sexuálnom živote.

## **Tretia osoba**

je každá osoba alebo orgán mimo manažéra údajov. Za tretiu osobu sa nepovažuje osoba, ktorá poskytla osobné údaje, alebo osoby či orgány, ktoré na príkaz zbierajú, spracúvajú alebo používajú osobné údaje v Nemecku, v inom členskom štáte Európskej únie alebo v inom združení štátov v rámci dohody v Európskom hospodárskom priestore.