Kodeks Postępowania w sprawie Ochrony Prawa Osób do Prywatności przy Przetwarzaniu Danych Osobowych w ramach Grupy Deutsche Telekom

English version – available below the Polish version

Niniejszy Kodeks Postępowania jest częścią Privacy Code of Conduct Grupy Deutsche Telekom, ponieważ Polska Telefonia Cyfrowa jest częścią Grupy Deutsche Telekom.

Preambuła

(1) Ze względu na wzmożone tworzenie systemów informatycznych oraz komunikacyjnych, spółki z całego świata należące do Grupy Deutsche Telekom przykładają wielka wagę do ochrony danych osobowych klientów, partnerów handlowych, pracowników oraz akcjonariuszy.

(2) W związku z powyższym, najważniejszym celem niniejszego Kodeksu Postępowania jest zapewnienie jednolitego i wysokiego poziomu ochrony danych osobowych w obrębie całej Grupy Deutsche Telekom. W szczególności, w przypadku międzynarodowych przepływów danych należy zapewnić, że odbiorca danych osobowych będzie je przetwarzał zgodnie z przepisami prawa ochrony danych osobowych, do których przekazujący dane musi się stosować.

(3) Spółki z Grupy Deutsche Telekom zdają sobie sprawę z tego, że sukces Deutsche Telekom zależy nie tylko od tworzenia globalnych sieci przepływu informacji, ale przede wszystkim od zapewnienia wiarygodnego i bezpiecznego sposobu przetwarzania danych osobowych.

(4) W wielu obszarach, klienci Grupy Deutsche Telekom postrzegają ją jako jeden podmiot. Z tego względu celem wszystkich spółek z Grupy Deutsche Telekom jest istotny udział we wspólnym sukcesie firmy oraz wspieranie Grupy Deutsche Telekom w dążeniu do utrzymania jej pozycji jako dostawcy wysokiej jakości produktów i usług poprzez wdrożenie niniejszego Kodeksu Postępowania.

Część I

Zakres i zastosowanie

§ 1 Charakter prawny Kodeksu Postępowania

Kodeks Postępowania jest Zarządzeniem, które obowiązuje wszystkie podmioty z Grupy Deutsche Telekom i które wchodzi w życie wraz z jego przyjęciem oraz opublikowaniem przez odpowiednie organy zarządzające spółki. Kodeks Postępowania dotyczy przetwarzania wszelkich danych osobowych osób fizycznych, w szczególności danych klientów, akcjonariuszy, pracowników i innych osób trzecich, kontrahentów oraz partnerów biznesowych.

§ 2 Obowiązujące przepisy prawa

(1) Zasady określone poniżej zostały opracowane w celu zapewnienia jednakowo wysokiego poziomu ochrony danych w obrębie całej Grupy Deutsche Telekom. Niemniej jednak nie zastępują one wymaganych oraz, stosownie do

zaistniałych okoliczności, ustawowych warunków, które należy spełnić, aby przetwarzanie danych osobowych było zgodne z prawem. Wszystkie zobowiązania oraz regulacje obowiązujące w stosunku do poszczególnych spółek, dotyczące przetwarzania i wykorzystywania danych osobowych, których zakres wykracza poza zasady przedstawione poniżej lub które określają dodatkowe ograniczenia dotyczące przetwarzania i wykorzystywania danych osobowych, będą miały charakter nadrzędny w stosunku do postanowień niniejszego Kodeksu Postępowania. Niezależnie od powyższych postanowień, spółki oświadczają, że przepisy prawa obowiązujące poszczególne spółki nie zwalniają spółek z wypełniania zobowiązań wynikających z niniejszego Kodeksu Postępowania.

(2) Dane zebrane na terenie Europy będą przetwarzane zgodnie z przepisami prawa państwa, w którym dane te zebrano, również w przypadku przekazania ich za granicę.

(3) Zbieranie danych osobowych oraz przekazywanie ich organom państwowym będzie odbywało się zgodnie z obowiązującymi przepisami prawa danego państwa, chyba że dane czynności będą podejmowane w ramach normalnego stosunku umownego z klientem.

(4) Niniejszy Kodeks Postępowania będzie podlegał przepisom prawa Rzeczypospolitej Polskiej.

§ 3 Rozwiązanie

Wygaśnięcie obowiązywania lub unieważnienie treści Kodeksu Postępowania – bez względu na termin, okoliczności i powody – nie zwolni spółek ze zobowiązań oraz obowiązku zastosowania się do postanowień niniejszego Kodeksu Postępowania w zakresie przetwarzania danych, które zostały przekazane.

Część II

Zasady

Artykuł 1

Przejrzystość procesu przetwarzania danych

§ 4 Obowiązek informacyjny

Osoby, których dane dotyczą, muszą mieć zapewniony łatwy dostęp do informacji na temat należytego przetwarzania ich danych osobowych, na przykład poprzez zamieszczenie polityki w sprawie ochrony prywatności oraz niniejszego Kodeksu Postępowania na stronie internetowej.

§ 5 Treść i forma informacji

(1) Osoby, których dane dotyczą, otrzymają stosowne informacje na temat:

a) tożsamości administratora (administratorów) danych oraz jego (ich) danych kontaktowych;

b) planowanego zakresu i celu zbierania, przetwarzania lub wykorzystywania danych osobowych. Powyższe informacje powinny określać, które dane będą utrwalane lub przetwarzane / wykorzystywane, z

jakich powodów, w jakim celu oraz przez jaki okres.

c) odbiorcy danych, zakresu oraz celu/celach przekazania danych - jeżeli dane osobowe będą przekazywane osobom trzecim;

d) sposobu przetwarzania lub wykorzystywania danych, szczególnie jeżeli będą one przetwarzane lub wykorzystywane w innym państwie.

e) przysługujących im praw ustawowych (zob. art. 7).

(2) Bez względu na wybrany środek przekazu, osoby, których dane dotyczą, powinny otrzymać jasne i łatwe do zrozumienia informacje.

§ 6 Dostępność informacji

Osoby, których dane dotyczą, będą miały zapewniony dostęp do powyższych informacji od momentu pierwszego zebrania danych, a następnie zawsze, gdy tylko o nie poproszą.

§ 7 Zgoda

(1) Zgodę osoby, której dane dotyczą, należy uzyskać najpóźniej w dniu rozpoczęcia zbierania, przetwarzania lub wykorzystywania danych osobowych, chyba że zbieranie, przetwarzanie lub wykorzystywanie danych będzie wymagane w celu zawarcia lub wykonania umowy, lub jeżeli czynności te będą ustawowo dozwolone.

(2) Oprócz obowiązku informacyjnego określonego powyżej, w związku z uzyskaniem zgody należy stosować się do następujących wytycznych:

a) Treść

Zgoda musi zostać wyraźnie i dobrowolnie udzielona na podstawie informacji skierowanych do osoby, której dane dotyczą, określających, w szczególności, zakres czynności, na które wyraża ona zgodę, oraz konsekwencje nie udzielenia zgody. Oświadczenie zgody powinno być sformułowane w sposób dostatecznie precyzyjny i powinno zawierać informacje na temat prawa osoby, której dane dotyczą, do wycofania zgody w dowolnym terminie.

b) Forma

Forma zgody będzie dostosowana do zaistniałych okoliczności (standardowo będzie to forma pisemna lub elektroniczna). W wyjątkowych sytuacjach, osoba, której dane dotyczą, może udzielić zgody ustnie, jeżeli fakt udzielenia zgody oraz wyjątkowe okoliczności, które potwierdzają zasadność takiej formy, zostaną dostatecznie udokumentowane.

Artykuł 2

Wykorzystanie danych w określonym celu

§ 8 Zasada

Danych osobowych nie należy wykorzystywać w celach innych niż te, dla których zostały pierwotnie zebrane.

§ 9 Zakaz uzależniania świadczenia usług od udzielenia zgody

Możliwość skorzystania z usług lub otrzymania produktów lub usług nie będzie uzależniona od udzielenia przez osoby, których dane dotyczą, zgody na wykorzystywanie ich danych dla celów innych niż zawarcie lub wykonanie umowy. Powyższe postanowienie będzie miało zastosowanie, wyłącznie jeżeli osoba, której dane dotyczą, nie będzie miała możliwości, w granicach rozsądku, skorzystania z podobnych usług lub produktów.

Artykuł 3

Szczególne przypadki przetwarzania danych

§ 10 Marketing bezpośredni

(1) Osoby, których dane dotyczą, zostaną poinformowane o możliwości wniesienia sprzeciwu, w dowolnym czasie, wobec wykorzystywania ich danych osobowych w marketingu bezpośrednim. Ponadto zostaną one poinformowane o charakterze, treści oraz okresie wykorzystywania ich danych w marketingu bezpośrednim.

(2) Osoby, których dane dotyczą, będą informowane o przysługującym im prawie do wniesienia sprzeciwu za każdym razem, gdy przekazywane im będą informacje o charakterze marketingu bezpośredniego. Ponadto osoby, których dane dotyczą, otrzymają odpowiednie narzędzia, dzięki którym będą miały możliwość zrezygnowania z otrzymywania tego typu materiałów. W szczególności zostaną im przekazane dane organu, do którego powinny zgłosić taki sprzeciw.

(3) Zgodnie ze zdaniem 2, par. 2 (1) niniejszego Kodeksu Postępowania, szczególne przepisy prawne, które uzależniają wykorzystywanie danych osobowych od zgody osoby, której dane dotyczą, będą nadrzędne wobec pozostałych postanowień.

§ 11 Zautomatyzowane decyzje indywidualne

(1) Decyzje, które będą dotyczyły oceny osobistych aspektów danej osoby i które mogą nieść za sobą konsekwencje prawne dla takiej osoby, lub które mogą mieć na nią znacząco niekorzystny wpływ, nie będą podejmowane wyłącznie na podstawie zautomatyzowanego przetwarzania danych. Powyższe postanowienia mają w szczególności zastosowanie do decyzji, dla których kluczowe znaczenie mają dane dotyczące zdolności kredytowej, kwalifikacji zawodowych lub stanu zdrowia osoby, której dane dotyczą.

(2) Jeżeli, w indywidualnych przypadkach, podjęcie decyzji opartej na zautomatyzowanym przetwarzaniu

danych będzie konieczne z obiektywnego punktu widzenia, osoba, której dane dotyczą, zostanie bezzwłocznie poinformowana o wyniku takiej decyzji i otrzyma możliwość zgłoszenia uwag w stosownym terminie. Uwagi zgłoszone przez osobę, której dane dotyczą, zostaną należycie rozpatrzone przez podjęciem ostatecznej decyzji.

§ 12 Szczególne kategorie danych osobowych

(1) Przetwarzanie szczególnych kategorii danych osobowych będzie wymagało wyraźnego umocowania prawnego lub uprzedniej zgody osoby, której dane dotyczą. Przetwarzanie takich danych będzie dopuszczalne, również jeżeli będzie to niezbędne do wykonania praw i obowiązków odpowiedzialnego organu wynikających z prawa pracy, pod warunkiem, że takie działania będą dopuszczalne na mocy prawa krajowego, zapewniającego odpowiednie gwarancje.

(2) Przed rozpoczęciem zbierania, przetwarzania bądź wykorzystywania tego rodzaju danych, dział ds. ochrony danych stosownej spółki zostanie poproszony o przedstawienie pisemnej opinii na temat wszystkich przypadków wymagających takiej konsultacji. Należy uwzględnić charakter, zakres, cel oraz konieczność, jak również podstawę prawną wykorzystywania tego rodzaju danych.

Artykuł 4

Jakość danych, oszczędne wykorzystywanie i ograniczanie danych

§ 13 Jakość danych

(1) Dane osobowe powinny być zawsze prawidłowe oraz, jeżeli zajdzie taka potrzeba, aktualizowane (jakość danych).

(2) Ze względu na cel (cele), dla którego (których) dane są zbierane, przetwarzane lub wykorzystywane, wprowadzone zostaną odpowiednie środki zapewniające, że wszelkie nieprawdziwe lub niekompletne informacje będą usuwane lub, jeżeli zajdzie taka potrzeba, odpowiednio poprawiane.

§ 14 Oszczędne wykorzystywanie i ograniczanie danych, anonimizacja oraz pseudonimizacja

(1) Dane osobowe będą odpowiednie i istotne, a ich ilość będzie dostosowana do konkretnego celu, dla którego są one wykorzystywane (oszczędne wykorzystywanie danych). Gdy zajdzie taka potrzeba, dane będą przetwarzane wyłącznie w ramach określonej aplikacji (ograniczanie danych).

(2) Jeżeli będzie taka możliwość oraz jeżeli będzie to ekonomicznie uzasadnione, wprowadzone zostaną procedury mające na celu usunięcie cech identyfikacyjnych osób, których dane dotyczą, (anonimizacja) lub zastąpienie takich cech innymi wartościami (pseudonimizacja). Anonimizacja oraz pseudonimizacja zostaną przeprowadzone w sposób zapewniający, że tożsamość osób, których dane dotyczą, nie zostanie ujawniona lub ujawnienie takich danych będzie wymagało nadzwyczajnych starań.

§ 15 Zbieranie informacji, analizy statystyczne

(1) Środki organizacyjne i techniczne, zgodne z najnowszymi koncepcjami lub technologiami, będą stosowne

w celu zapewnienia, że zbieranie informacji (np. profile ruchu, profile użytkowników, profile wykorzystania danych) nie będzie dozwolone bez uzyskania prawnego zezwolenia lub uprzedniej zgody osoby, której dane dotyczą.

(2) Powyższe postanowienia nie mają zastosowania do analiz statystycznych i badań przeprowadzanych na podstawie danych poddanych anonimizacji lub pseudonimizacji.

§ 16 Archiwizacja danych

Zasady dotyczące przetwarzania danych, w szczególności te odnoszące sie do oszczędnego wykorzystywania oraz ograniczania danych, zostaną uwzględnione przy opracowywaniu procedur archiwizacyjnych. Archiwizacja danych osobowych wymaga wyraźnej zgody osoby, której dane dotyczą, chyba że będzie to konieczne ze względu na prowadzoną działalność lub obowiązujące przepisy prawa.

Artykuł 5

Ograniczenia dotyczące dalszego przekazywania danych

§ 17 Przekazywanie danych osobom trzecim

(1) Przekazywanie danych osobowych osobom trzecim będzie dozwolone wyłącznie po wskazaniu odpowiedniej podstawy prawnej. Takie działania mogą okazać się konieczne w celu wykonania warunków umownych w stosunku do osoby, której dane dotyczą, lub z uwagi na zgodę udzieloną przez osobę, której dane dotyczą.

(2) Par. 1 nie będzie miał zastosowania, jeżeli w danym kraju będą obowiązywały jakiekolwiek ograniczenia, ustanowione w szczególności ze względu na bezpieczeństwo państwa, obronę narodową, bezpieczeństwo publiczne lub zapobieganie przestępstwom, prowadzenie dochodzeń w sprawie popełnionych przestępstw i ich wykrywanie lub toczące się postępowania karne, które to ograniczenia będą wymagały przekazania danych osobowych w powyższych celach.

§ 18 Zakres odpowiedzialności

(1) W przypadku przekazywania danych osobom trzecim niebędącym organami publicznymi, spółka, która w pierwszej kolejności zgromadziła te dane, zapewni, aby były one przetwarzane lub wykorzystywane zgodnie z prawem. W związku z powyższym przed przekazaniem danych, odpowiednie środki zapewniające ochronę i bezpieczeństwo danych zostaną omówione i uzgodnione z odbiorcą. Jeżeli umowy zawierane będą z organami w krajach niezapewniających właściwego poziomu ochrony danych, należy zapewnić odpowiednie gwarancje dotyczące ochrony prawa do prywatności danej osoby oraz wykonania odnośnych praw.

(2) Zgodnie z ogólnoprzyjętymi standardami, należy wprowadzić odpowiednie środki techniczne oraz organizacyjne, w celu zapewnienia spójności oraz bezpieczeństwa danych w trakcie ich przekazywania osobie trzeciej.

§ 19 Umowy o przetwarzanie danych zawierane z podwykonawcami

(1) Jeżeli spółka korzysta z usług podwykonawcy, umowa o świadczenie usług wchodzących w zakres zleconych prac będzie również odnosiła się do obowiązków podwykonawcy jako strony zaangażowanej w przetwarzanie danych. Obowiązki te będą określać instrukcje spółki (Administratora Danych) dotyczące rodzaju oraz sposobu przetwarzania danych osobowych, celu przetwarzania oraz środków technicznych i organizacyjnych niezbędnych do zapewnienia ochrony danych. Odpowiednio stosować się będzie postanowienia określone w zdaniu 3 par. 18(1) niniejszego Kodeksu Postępowania.

(2) Podwykonawca nie będzie wykorzystywał danych osobowych w celu przetwarzania ich we własnym zakresie lub przez osobę trzecią bez uprzedniej pisemnej zgody Administratora Danych. Jeżeli dane będą przetwarzane przez osobę trzecią, powyższe zasady zostaną uzgodnione również z takim podwykonawcą (podwykonawcami).

(3) Głównym kryterium wyboru podwykonawców będzie możliwość spełnienia powyższych wymogów.

Artykuł 6

Ochrona danych, organizacja i bezpieczeństwo danych

§ 20 Administrator Bezpieczeństwa Informacji

(1) Każda ze spółek wyznaczy Administratora Bezpieczeństwa Informacji, którego zadaniem będzie zapewnienie, aby poszczególne działy zostały poinformowane o ustawowych lub wewnątrzgrupowych wymogach oraz o polityce ochrony danych i prywatności.

(2) Administrator Bezpieczeństwa Informacji będzie zaangażowany w opracowywanie nowych produktów i usług już na początkowym etapie ich opracowywania w celu zapewnienia, że odpowiadają one zasadom określonym w niniejszym Kodeksie.

§ 21 Kontrola poziomu ochrony danych

Kontrole poziomu ochrony danych (np. audyty ochrony danych) będą przeprowadzane regularnie w celu sprawdzenia efektywności oraz skuteczności wprowadzonych środków technicznych i organizacyjnych służących zapewnieniu należytej ochrony danych. Powyższe audyty mogą być przeprowadzane wewnętrznie przez Administratora Bezpieczeństwa Informacji lub inne jednostki organizacyjne, którym polecono ich wykonanie, lub, alternatywnie, niezależną osobę trzecią z zewnątrz, która zostanie zatwierdzona przez Administratora Danych. Podstawą ustalenia odpowiedniego poziomu ochrony danych będą wymogi określone przepisami prawa oraz polityką firmy, które stosuje się w stosunku do danej jednostki organizacyjnej, jak również wymogi wskazane w niniejszym Kodeksie Postępowania.

§ 22 Środki techniczne, organizacyjne oraz dotyczące pracowników

Odpowiednie zobowiązania dotyczące poufności zostaną uzgodnione na piśmie z pracownikami, którzy będą rozpoczynać pracę w spółce. Ponadto odpowiednie środki techniczne i organizacyjne dotyczące przetwarzania

danych osobowych zostaną wprowadzone w odniesieniu do procesów stosowanych w spółce oraz systemów informatycznych.

Środki te obejmować będą:

a) niedopuszczenie, aby osoby nieupoważnione uzyskały dostęp do systemów przetwarzania danych, w ramach których przetwarzane oraz wykorzystywane będą dane osobowe (kontrola dostępu fizycznego);

b) zapewnienie, że systemy przetwarzania danych nie mogą być wykorzystywane przez nieupoważnione osoby (kontrola dostępu);

c) zapewnienie, że osoby upoważnione do korzystania z systemu przetwarzania danych będą miały dostęp wyłącznie do danych, które wchodzą w zakres uzyskanego przez nich zezwolenia, oraz że podczas przetwarzania, wykorzystywania lub po utrwaleniu danych osobowych osoby nieupoważnione nie będą miały możliwości przeczytania, skopiowania, zmodyfikowania lub usunięcia danych osobowych (kontrola dostępu do danych);

d) zapewnienie, że, w trakcie przekazywania danych drogą elektroniczną bądź podczas przenoszenia lub nagrywania danych na nośnik, osoby nieupoważnione nie będą miały możliwości przeczytania, skopiowania, zmodyfikowania lub usunięcia danych osobowych oraz że za pomocą sprzętu służącego do przekazywania danych nie będzie możliwe zapoznanie się z danymi danych lub ustalenie miejsca, do którego będą one przekazane (kontrola przekazywania danych);

e) zapewnienie możliwości sprawdzenia i ustalenia czy i przez kogo dane osobowe zostały wprowadzone do systemów przetwarzania danych, zmienione lub usunięte (kontrola wprowadzania danych);

f) zapewnienie, że podwykonawcy będą przetwarzać dane osobowe wyłącznie zgodnie z instrukcjami zleceniodawcy (kontrola podwykonawcy);

g) zapewnienie ochrony danych przed przypadkowym zniszczeniem lub utratą (kontrola dostępności);

h) zapewnienie możliwości oddzielnego przetwarzania danych zebranych dla różnych celów (zasada rozdzielności).

Artykuł 7

Prawa osób, których dane dotyczą

§ 23 Prawo do składania zapytań i skarg

Każda osoba, której dane dotyczą, ma prawo w dowolnym czasie złożyć zapytanie lub skargę dotyczące zastosowania niniejszego Kodeksu Postępowania do działu ochrony danych w spółce odpowiedzialnej. O ile nie zostaną przyjęte odmienne ustalenia, dla celów niniejszych postanowień, spółka odpowiedzialna będzie dowolną spółką, która pozostaje w stosunku umownym z osobą, której dane dotyczą, lub która przetwarza dane osobowe osoby, której dane dotyczą. Spółka, z którą skontaktowała się osoba, której dane

dotyczą, upewni się, że prawa osoby, której dane dotyczą, są należycie przestrzegane przez inne spółki odpowiedzialne.

§ 24 Prawo do uzyskania informacji

(1) Każda osoba, której dane dotyczą, ma prawo w dowolnym momencie zwrócić się do spółki odpowiedzialnej z prośbą o informacje na temat:

a) zarejestrowanych danych osobowych, które ich dotyczą, w tym również na temat źródła takich danych oraz ich odbiorcy (odbiorców);

b) celu przetwarzania lub wykorzystywania danych;

c) osób i jednostek, którym ich dane są regularnie przekazywane, w szczególności jeżeli dane te są przekazywane za granicę;

d) postanowień niniejszego Kodeksu Postępowania.

(2) Odpowiednie informacje zostaną przekazane osobie pytającej w łatwej do zrozumienia formie i w rozsądnym terminie. Powyższe informacje będą standardowo przekazywanie na piśmie lub drogą elektroniczną.

(3) O ile będzie to dozwolone stosownymi przepisami prawa krajowego, spółka może naliczać opłatę za dostarczenie odpowiednich informacji.

§ 25 Prawo do wnoszenia sprzeciwu/prawo do żądania usunięcia/zablokowania danych

(1) Osoba, której dane dotyczą, może wnieść sprzeciw do spółki odpowiedzialnej wobec wykorzystywania jej danych, jeżeli przysługuje jej takie prawo.

(2) Powyższe prawo do wnoszenia sprzeciwu będzie stosować się również w przypadku, gdy osoba, której dane dotyczą, udzieliła wcześniej zgody na wykorzystywanie jej danych.

(3) Zgodne z prawem wnioski o usunięcie lub zablokowanie danych będą bezzwłocznie realizowane. Powyższe wnioski uznaje się za zgodne z prawem, jeżeli brak będzie dalszej podstawy prawnej do wykorzystywania danych. Jeżeli osobie, której dane dotyczą, przysługuje prawo do żądania usunięcia danych, a nie można ich usunąć lub usunięcie danych jest niemożliwe po dołożeniu zasadnych starań, dane te zostaną zabezpieczone przed nieupoważnionym wykorzystaniem poprzez ich zablokowanie. Zachowane zostaną ustawowe okresy przechowania.

§ 26 Prawo do poprawiania danych

Osoba, której dane dotyczą, może w dowolnym czasie zwrócić się do spółki odpowiedzialnej z prośbą o poprawienie jej danych osobowych, jeżeli dane te będą niekompletne lub nieprawdziwe.

§ 27 Prawo do żądania wyjaśnień i zgłaszania uwag

(1) Jeżeli osoba, której dane dotyczą, twierdzi, że naruszono jej prawa, przetwarzając dane niezgodnie z

prawem, lub jeżeli naruszono postanowienia niniejszego Kodeksu Postępowania, spółki odpowiedzialne wyjaśnią zaistniałe okoliczności bez zbędnej zwłoki. W takim przypadku będą one ściśle współpracować i zapewnią sobie dostęp do wszelkich informacji niezbędnych do ustalenia faktów w niniejszej sprawie zgodnie z przepisami obowiązującego prawa.

(2) Dział ds. ochrony danych w spółce odpowiedzialnej, która będzie najbardziej związany z daną sprawą, będzie koordynowała wszelką korespondencję z osobą, której dane dotyczą.

§ 28 Wykonanie praw osób, których dane dotyczą

Osoby, których dane dotyczą i które skorzystają z powyższych praw, nie będą z tego powodu stawiane w niekorzystnej sytuacji. W stosownych przypadkach, forma komunikowania się z osobą, której dane dotyczą – np. telefonicznie, elektronicznie lub pisemnie – będzie odpowiadała życzeniom takiej osoby.

Artykuł 8

Zarządzanie procesem ochrony danych/zakres obowiązków

§ 29 Odpowiedzialność za przetwarzanie danych

(1) Spółki, jako Administratorzy Danych, są zobowiązane, w szczególności wobec osób, których dane dotyczą, zagwarantować zgodność z wymogami ochrony danych oraz postanowieniami niniejszego Kodeksu Postępowania.

(2) Administrator Bezpieczeństwa Informacji odpowiedniej spółki zostanie bezzwłocznie poinformowany o wszelkich naruszeniach (w tym podejrzeniu wystąpienia naruszenia) postanowień dotyczących ochrony danych oraz niniejszego Kodeksu Postępowania. W przypadku zdarzeń dotyczących więcej niż jednej spółki, należy poinformować również centralny Dział ds. Prywatności Grupy. Administrator Bezpieczeństwa Informacji spółki zawiadomi Dział ds. Prywatności Grupy, także jeżeli do przepisów prawa obowiązujących wobec spółki zostaną wprowadzone jakiekolwiek zmiany, które będą dla niej wyjątkowo niekorzystne.

(3) Działy ds. ochrony danych poszczególnych spółek będą koordynować swoje działania w ramach obowiązującej w Grupie polityki ochrony danych. W związku z powyższym, będą się nawzajem wspierać i stosować istniejące możliwości współdziałania (synergie).

§ 30 Koordynacja działań przez Dyrektora ds. Prywatności Grupy

(1) Dyrektor ds. Prywatności Grupy będzie koordynował współpracę oraz proces zawierania porozumień we wszelkich istotnych kwestiach związanych z ochroną danych. Komitet Koordynacyjny Grupy Deutsche Telekom powołany w związku z ochroną danych będzie organem koordynującym wszelkie działania.

(2) Obowiązkiem Dyrektora ds. Prywatności Grupy będzie opracowanie i udoskonalanie polityki ochrony danych Grupy. W powyższy projekt zaangażowane będą również działy ds. ochrony danych spółek.

§ 31 Obowiązek sprawowania nadzoru i przeprowadzania konsultacji

(1) Administratorzy Bezpieczeństwa Informacji poszczególnych spółek będą odpowiedzialni za monitorowanie zgodności z krajowymi i międzynarodowymi regulacjami w sprawie ochrony danych oraz postanowieniami niniejszego Kodeksu Postępowania. W powyższym zakresie, wszystkie działy poszczególnych spółek będą zobowiązane informować odpowiedniego Administratora Bezpieczeństwa Informacji o stosownych zmianach oraz planach na przyszłość.

(2) W przypadku braku jakichkolwiek ograniczeń prawnych, odpowiedni Administratorzy Bezpieczeństwa Informacji będą upoważnieni do sprawdzenia na miejscu wszystkich metod przetwarzania, które będą dotyczyć wykorzystywania danych osobowych.

(3) W stosownych przypadkach oraz w ramach obowiązków obejmujących powyższe badanie, jednostki ds. ochrony danych poszczególnych spółek będą stosować takie same mechanizmy w obrębie Grupy, np. wspólne audyty ochrony danych.

§ 32 Szkolenie i zaangażowanie pracowników

(1) Pracownicy spółek będą odpowiednio przeszkoleni w zakresie znajomości przepisów o ochronie danych oraz zastosowania postanowień niniejszego Kodeksu Postępowania.

(2) Spółki, we współpracy z odpowiednimi działami ds. ochrony danych, opracują stosowne materiały szkoleniowe.

§ 33 Współpraca z organami nadzoru

(1) Spółki zobowiążą się, że będą odpowiadać na zapytania organów sprawujących nad nimi kontrolę lub, jeżeli będzie to konieczne w przypadku spółek eksportujących dane, w rozsądnym terminie i zakresie, jak również będą stosować się do poleceń organów nadzoru.

(2) W przypadku zmiany przepisów mających zastosowanie wobec spółki, co może mieć znacząco niekorzystny wpływ na gwarancje przewidziane w niniejszym Kodeksie Postępowania, odpowiednia spółka poinformuje właściwy organ nadzoru o takim wpływie.

Artykuł 9

Terminy i definicje

Zautomatyzowane decyzje indywidualne

Termin ten oznacza decyzje niosące za sobą konsekwencje prawne w stosunku do osoby, której dane dotyczą, lub wywierające na nią znacząco negatywny wpływ, które to decyzje zostały podjęte wyłącznie na podstawie zautomatyzowanego procesu przetwarzania danych opracowanego w celu oceny określonych osobistych aspektów dotyczących danej osoby, jak na przykład wyników w pracy, zdolności kredytowej, niezawodności, postępowania itp.

Osoba, której dane dotyczą

Termin ten oznacza osobę fizyczną, której dane osobowe są przetwarzane przez spółkę lub spółki Grupy Deutsche Telekom.

Administrator danych

Termin ten oznacza spółkę, która samodzielnie bądź we współpracy z innymi podmiotami określa cele oraz środki służące do przetwarzania danych osobowych.

Grupa Deutsche Telekom

Termin ten oznacza Deutsche Telekom AG oraz wszystkie spółki, w których Deutsche Telekom AG posiada, bezpośrednio lub pośrednio, ponad 50 procent akcji / udziałów lub nad którymi sprawuje kontrolę.

Podmiot przetwarzający dane

Termin ten oznacza dowolną osobę fizyczną lub prawną, władzę państwową, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych (umowy o przetwarzanie danych zawierane z podwykonawcami).

Spółka

Termin ten oznacza dowolną spółkę, która zobowiązała się przyjąć Kodeks Postępowania i która została wymieniona w Aneksie A załączonym do niniejszego dokumentu.

Dane osobowe

Termin ten oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą); osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny bądź jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Przetwarzanie danych osobowych

Termin ten oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych, takie jak zbieranie, utrwalanie, porządkowanie, przechowywanie, dostosowywanie lub zmienianie, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnienie przez przekazywanie, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie. Termin ten odnosi się również do przetwarzania danych osobowych w ręcznie uporządkowanych katalogach.

Odbiorca

Termin ten oznacza dowolną osobę fizyczną lub prawną, władzę państwową, agencję lub inny organ, któremu ujawniane są dane bez względu na to, czy jest osobą trzecią czy też nie. Jednakże władze

państwowe, które maja prawo otrzymywać dane w ramach konkretnego dochodzenia, nie będą uważane za odbiorcę.

Szczególne kategorie danych

Termin ten oznacza dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych oraz dane dotyczące stanu zdrowia lub życia seksualnego.

Osoba trzecia

Termin ten oznacza dowolną osobę lub organ będące poza kontrola administratora danych. Osoba, której dane dotyczą, bądź osoby lub organy, które będą na polecenie zbierać, przetwarzać lub wykorzystywać dane osobowe na terenie Niemiec, w innym państwie członkowskim Unii Europejskiej lub innym państwie będącym stroną umowy o Europejskim Obszarze Gospodarczym, nie będą uważane za osoby trzecie.

Code of Conduct for the Protection of the Individual's Right to Privacy in the Handling of Personal Data within the Deutsche Telekom Group

Click to go to Polish version

Preamble and Recitals

(1) Due to increasing networking of information and communications systems, the protection of personal data of customers, sales partners, employees and shareholders is a significant concern of all companies in the Deutsche Telekom Group worldwide.

(2) The most important target of this Code of Conduct, therefore, is to create a uniform and high level of data protection in the Deutsche Telekom Group worldwide. In particular, in the case of transnational data flows it must be guaranteed that personal data is processed by the recipient according to the principles of data protection law that apply for the sender of such data.

(3) Deutsche Telekom Group companies are aware that the success of Deutsche Telekom as a whole is dependent not only on global networking of information flows, but also above all on trustworthy and safe handling of personal data.

(4) In many areas, the Deutsche Telekom Group is perceived by its customers as a single entity. Therefore it is the common concern of Deutsche Telekom Group companies to make an important contribution to the joint success of the company and to support the claim of the Deutsche Telekom Group of being a provider of high quality products and services by implementing this Code of Conduct.

Part One

Scope and Application

§ 1 Legal Nature of the Code of Conduct

This Code of Conduct is a Directive, which is binding for the entire Deutsche Telekom Group and comes into effect upon adoption and publication by the respective company management. It applies to the handling of all the personal data of natural persons, in particular the data of customers, shareholders, employees and other third parties, contracting parties or business partners.

§ 2 Legal Provisions to be Applied

(1) The principles set out below are intended to guarantee a uniformly high level of data protection throughout the entire Deutsche Telekom Group. However, they do not replace the required - and where necessary, statutory - conditions that must exist to legitimize the handling of personal data. Any obligations and regulations applying to individual companies on the processing and use of personal data which go beyond the following principles, or which contain additional limits on processing and use of personal data, shall remain unaffected by this Code of Conduct. Irrespective of the foregoing, the companies agree that laws applying for individual companies shall not prevent these companies from fulfilling their obligations under this Code of Conduct.

(2) Data collected in Europe must be processed according to the legal provisions of the country in which the data was collected, even in the event of transmission abroad.

(3) The collection of personal data and its transmission to public bodies shall - unless within the framework of a normal customer contractual relationship – be done in accordance with the obligatory legal provisions of the country.

(4) This Code of Conduct shall be governed by the law of the Republic of Poland.

§ 3 Termination

The expiry or termination of the Code of Conduct – irrespective of the time, circumstances and reasons – shall not release the companies from the obligations and/or provisions of this Code of Conduct regarding the processing of data already transmitted.

Part Two

Principles

Article 1

Transparency of Data Processing

§ 4 Duty to Inform

The data subjects must be given easy access to information about the appropriate handling of their personal data, for example by publishing privacy policy and this Code of Conduct on the Internet.

§ 5 Content and Form of Information

(1) The data subjects shall be adequately informed about the following:

a) The identity of the data controller(s) and their contact details.

b) The intended scope and purpose of the collection, processing and/or use of personal data. This information should include which data are being recorded and/or processed/used, why and for what purpose and for how long.

c) If personal data are transmitted to third parties, the recipient, extent and purpose(s) of such transmission.

d) The manner of data processing and/or use, especially if it is to be processed or used in another country.

e) Their legal rights (see Article 7).

(2) Irrespective of the chosen medium, data subjects should be given this information in a clear and easily understandable manner.

§ 6 Availability of Information

The information shall be available to data subjects when the data are first collected and, subsequently, whenever it is requested.

§ 7 Consent

(1) Unless the collection, processing or use of the data is required for purposes of initiating or fulfilling a contract or unless there is some other statutory authorization, the consent of the data subject shall be obtained at the latest when data starts to be collected, processed or used.

(2) In addition to the obligations to inform as set out above, the following shall be observed with regard to consent:

a) Content Consent must be given expressly, it must be voluntary and it must be on an informed basis that points out to the data subject, in particular, the scope of what he/she is consenting to and also the consequences of non-consent. The wording of declarations of consent shall be sufficiently precise and shall inform data subjects of their right to withdraw their consent at any time.

b) Form Consent shall be obtained in a form appropriate to the circumstances (normally in writing or electronically). In exceptional cases it can be obtained verbally, if the fact of the consent and the special circumstances that make verbal consent seem adequate are sufficiently documented.

Article 2

Use for Specific Purpose

§ 8 Principle

Personal data shall not be used for purposes other than those for which the data was originally collected.

§ 9 Prohibition of Tying-in

The use of services, or the receipt of products and/or services, shall not be made conditional on data subjects consenting to the use of their data for purposes other than the initiation or fulfillment of a contract. This shall only apply if it is not possible or not possible within reason for the data subject to use comparable services or comparable products.

Article 3

Special Data Processing Cases

§ 10 Direct Marketing

(1) Data subjects shall be informed that they may, at any time, object to their personal data being used for direct marketing purposes. Furthermore, they shall be made aware of the nature, content and period within which their data may be used for direct marketing purposes.

(2) Data subjects shall be informed about their right to object whenever they receive direct marketing communications. Furthermore, data subjects shall receive appropriate tools for exercising their right not to receive such communications. They shall receive, in particular, information about the body to whom the objection is to be made.

(3) Special legal provisions pursuant to sentence 2 of § 2 (1) of this Code of Conduct, which make the use of personal data dependent on the consent of the data subject, shall take precedence over other provisions.

§ 11 Automated Individual Decisions

(1) Decisions which evaluate individual aspects of a person and which may entail legal consequences for them, or which may have a considerable adverse effect on them, shall not be based exclusively on automated processing. This includes in particular decisions for which data about the creditworthiness, professional suitability or state of health of the data subject is significant.

(2) If, in individual cases, there is an objective need to make automated decisions, the data subject shall be informed without delay of the result of the automated decision, and shall be given an opportunity to comment within an appropriate period of time. The data subject's comments shall be suitably considered before a final decision is taken.

§ 12 Special Categories of Personal Data

(1) The handling of special categories of personal data shall be subject to express, legal authorization or to the data subject's prior consent. It shall also be permissible if it is necessary to process the data in order to

fulfill the rights and obligations of the responsible body in the area of labor law, provided that this is permissible due to national law that provides for adequate guarantees.

(2) Prior to the commencement of such collection, processing or use, the data protection department of the company in question shall be properly consulted, in writing, of all cases where this is necessary. Due consideration should be given to the nature, extent, purpose, necessity and legal basis of using the data.

Article 4

Data Quality, Data Economy and Data Avoidance

§ 13 Data Quality

(1) Personal data shall at all times be correct and, where necessary, kept up do date (data quality).

(2) In light of the purpose(s) for which the data are being collected, processed or used, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased or, if necessary, corrected.

§ 14 Data Economy, Data Avoidance, Anonymization and Pseudonymization

(1) Personal data shall be appropriate, relevant and not excessive with regard to the use of the data for a specific purpose (data economy). Data shall only be processed within a certain application when it is necessary (data avoidance)

(2) Where possible and economically reasonable, procedures shall be used to erase the identification features of data subjects (anonymization) or to replace the identification features with other characteristics (pseudonymization). Anonymization and pseudonymization shall be carried out in such a manner that the original identities of the data subjects cannot be revealed, or can only be revealed with disproportionately great effort.

§ 15 Profiling, Statistical Analyses

(1) Organizational and technical measures consistent with the appropriate state-of-the-art concepts or technology shall be used to ensure that profiling (e.g. movement profiles, user profiles, consumption profiles) is not allowed unless by express legal permission or the data subject's prior consent.

(2) Purely statistical analyses or studies on the basis of anonymized or pseudonymized data remains unaffected in this regard

§ 16 Data Archiving

The principles of data processing, particularly the principles of data economy and data avoidance, shall be taken into account when developing data archiving rules. Personal data must not be archived without the express consent of the data subject, unless where necessary for operational reasons or required by law.

Article 5

Restriction on Further Transmission

§ 17 Transmission of Data to Third Parties

(1) The transmission of personal data to a third party shall require a legal basis. This may arise because it is necessary to fulfill a contractual requirement towards the data subject or because the data subject has provided their consent.

(2) Paragraph 1 does not apply if national restrictions, in particular for reasons of security of the state, national defense, public safety or the prevention, investigation, detection and prosecution of criminal acts exist which require the transmission of personal data for these purposes.

§ 18 Responsibility

(1) When transmitting data to third parties that are not public bodies, the company that originally collected the data shall ensure that it is being processed or used lawfully. Accordingly, prior to the transmission of the data, appropriate data protection and data security measures shall be discussed and agreed with the recipient. Where agreements are concluded with bodies in countries without adequate data protection levels, sufficient guarantees must be ensured with respect to the protection of the right to privacy of the individual and the exercising of rights connected with this.

(2) In accordance with generally accepted standards, appropriate technical and organizational measures shall be taken to ensure the integrity and security of data during its transmission to a third party.

§ 19 Subcontracted Data Processing

(1) When a company engages the services of a subcontractor, then, in addition to a service agreement comprising the work to be performed, the contract shall also refer to the obligations of the subcontractor as the party engaged for processing the data. These obligations will set out the instructions of the company (the data controlling unit) concerning the type and manner of the processing of the personal data, the purpose of processing and the technical and organizational measures required for data protection. Sentence 3 of § 18 (1) of this Code of Conduct applies accordingly.

(2) The subcontractor shall not use the personal data for its own or third-party processing purposes without the prior consent of the data controlling unit. In the case of the latter, the above-stated rules shall also be agreed with such subcontractor(s).

(3) Subcontractors shall be selected according to their ability to fulfill the above-stated requirements.

Article 6

Data Protection, Organization and Data Security

§ 20 Data Protection Officers

(1) Each company shall appoint a data protection officer, whose task is to ensure that the individual departments are advised on the statutory and/or Group-internal requirements and on data protection and privacy policy.

(2) The data protection officer must be involved in the design of new products and services from the early stages to ensure that they are in harmony with the principles that are set out in this Code.

§ 21 Checks on the Level of Data Protection

Checks on the level of data protection (e.g. by data protection audits) should be carried out at regular intervals to review the effectiveness and success of the technical and organizational data protection measures implemented. Such audits may be carried out internally by the data protection officer or other organizational units which have been awarded an audit assignment or, alternatively, by an independent external third party approved by the data controlling unit. The basis for establishing the level of data protection shall be the legal and corporate policy requirements that apply for the respective organizational unit as well as the requirements of this Code of Conduct.

§ 22 Technical, Organizational and Employee-Related Measures

Appropriate confidentiality undertakings shall be agreed in writing with employees when commencing their work within the company. In addition, appropriate technical and organizational measures for handling personal data shall be established for the company processes and Information Technology systems.

Such measures shall include

a) preventing unauthorized persons from gaining access to data processing systems on which personal data are processed or used (physical access control);

b) ensuring that data processing systems cannot be used by unauthorized persons (denial-of-use control);

c) ensuring that those persons authorized to use a data processing system are able to access exclusively those data to which they have authorized access and that personal data cannot, during processing or use or after recording, be read, copied, altered or removed by unauthorized persons (data access control);

d) ensuring that, in the course of electronic transmission or during their transport or recording on data carrier, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to examine and establish where personal data are to be transmitted by data transmission equipment (data transmission control);

e) ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been entered into data processing systems, altered or removed (data entry control);

f) ensuring that personal data which are processed by subcontractors can only be processed in conformance with the instructions of the ordering party (subcontractor control);

g) ensuring that personal data are protected against accidental destruction or loss (availability control);

h) guaranteeing that data which have been collected for different purposes can be processed separately (separation rule).

Article 7

Rights of Data Subjects

§ 23 Right to Question and Complain

Every data subject has the right at any time to contact the data protection department of the responsible company with questions and complaints regarding the application of this Code of Conduct. If not subsequently specified otherwise, for the purpose of these provisions, the responsible company shall be any company that has a contract relationship with the data subject or that processes the data subject's personal data. The company that the data subject has contacted shall make sure that the data subject's rights are properly observed by the other responsible companies.

§ 24 Right to Information

(1) Every data subject may at any time, request information from the responsible company concerning:

a) the personal data recorded on them, including its origin and recipient(s);

b) the purpose of the processing or use;

c) the people and units to whom/which their data are regularly transmitted, particularly if the data are transmitted abroad;

d) the provisions of this Code of Conduct.

(2) The relevant information should be made available to the enquirer in an understandable form within a reasonable period of time. This should generally be done in writing or electronically.

(3) Where permissible under the relevant national law, a company may charge a fee for supplying the relevant information.

§ 25 Right of Protest/Right to Have Data Erased/Blocked

(1) The data subject concerned can protest to the responsible company against the use of his/her data, if he/she has the right to do so.

(2) This right to protest shall also apply in the event that the data subject had previously consented to the use of his/her data.

(3) Rightful requests to have data erased or blocked shall be promptly met. Such requests are rightful particularly when the legal basis for the use of the data ceases to apply. If a data subject has the right to

have data erased, but erasing the data is not possible or not possible with reasonable effort, the data shall be protected against non-permitted usage by blocking. Statutory retention periods shall be observed.

§ 26 Right to Correction

The data subject may at any time request that the responsible company corrects the personal data recorded on them insofar as such data are incomplete and/or incorrect.

§ 27 Right to Clarification and Comments

(1) If a data subject claims that his/her rights have been breached in the form of unlawful data processing, particularly in the event that this Code of Conduct has been breached, the responsible companies shall clarify the facts without culpable delay. In this case they shall work together closely and grant each other access, to all information necessary for establishing the facts of the case,

(2) The company's responsible data protection department most closely associated with the relevant issues must coordinate all the relevant correspondence with the data subject.

§ 28 Exercising of Rights of Data Subjects

Data subjects shall not be disadvantaged because they have availed themselves of these rights. The form of communication with the data subject - e.g. by telephone, electronically or in writing - should respect the request of the data subject, where appropriate.

Article 8

Data Protection Process Management/Responsibilities

§ 29 Responsibility for Data Processing

(1) The companies shall, in their capacity as Data Controllers, be obliged, particularly vis-a-vis data subjects, to guarantee compliance with the requirements of data protection and with the provisions of this Code of Conduct.

(2) The data protection officer of the respective company shall be informed without delay about any breaches (including suspicion of a breach) of data protection provisions and of this Code of Conduct. In the case of incidents that are of relevance to more than one company, the central Group Privacy Department should also be informed. The company's data protection officer shall also inform the Group Privacy Department if any changes are made to the laws applying for a company that are significantly unfavorable.

(3) The data protection departments of the individual companies shall coordinate their activities within the framework of the Group's data protection policy. Accordingly, they should mutually support each other and make use of existing synergies.

§ 30 Coordination by the Group Privacy Officer

(1) The Group Privacy Officer shall coordinate the processes of cooperation and agreement in all significant issues regarding data protection. The Deutsche Telekom Group Coordination Committee on data protection shall serve as the coordinating body.

(2) It shall be the duty of the Group Privacy Officer to develop and evolve the Group's policy on data protection. Also in this regard, the data protection departments of the companies shall engage in coordination.

§ 31 Supervisory and Consultation Duties

(1) The data protection officers of the respective companies shall be responsible for monitoring compliance with national and international data protection regulations and with this Code of Conduct. In this regard, all departments of the respective companies shall be obliged to inform the relevant data protection officer of appropriate developments and future plans.

(2) In the absence of legal restraints, the respective data protection officers shall be authorized to examine on-site all processing techniques that involve the use of personal data.

(3) Where appropriate, and within the framework of their examination duties, the data protection units of the companies shall use mechanisms which are identical throughout the Group, e.g. in the form of common data protection audits.

§ 32 Employee Training and Commitment

(1) The employees of the companies shall be sufficiently trained with regard to the data protection regulations and application of this Code of Conduct.

(2) The companies shall, with the participation of the competent data protection departments, devise suitable training materials.

§ 33 Cooperation with Supervisory Authorities

(1) The companies shall agree to respond to enquiries by the supervisory authority responsible for them or if applicable for the company exporting the data within a reasonable period of time and to a reasonable extent and to follow the supervisory authority's recommendations.

(2) In the event of a change in the legislation applicable to a company which might have substantial adverse effect on the guarantees provided by this Code of Conduct the relevant company will notify the change to the relevant supervisory authority.

Article 9

Terms and Definitions

Automated individual decisions

Shall mean decisions which produce legal effects for the data subject or which significantly affect him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Data subject

Shall mean any natural person whose personal data is handled in the Deutsche Telekom Group.

Data controller

Shall mean the company which alone or jointly with others determines the purposes and means of the processing of personal data.

Deutsche Telekom Group

Shall mean Deutsche Telekom AG and all companies in which Deutsche Telekom AG directly or indirectly holds more than a 50% share, or over which it has control.

Data processor

Shall mean any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller (subcontracting data processing)

Company

Shall mean any company that has agreed to be bound by this Code of Conduct and that is listed in Annex A hereto.

Personal data

Shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Handling of personal data

Shall mean any operation or set of operations which is performed upon personal data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This also includes the processing of personal data in structured manual files.

Recipient

Shall mean any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not. However, public authorities that may receive data as part of a single inquiry shall not be considered to be recipients.

Special categories of data

Shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life.

Third party

Shall mean any person or body outside the data controller. Third parties shall not mean the data subject or persons or bodies who by order collect, process or use personal data in Germany, in another member state of the European Union or in another state party of the agreement on the European Economic Area.