Wiążące Reguły Korporacyjne Dotyczące Prywatności (BCRP)

Wiążące Reguły Korporacyjne Dotyczące Ochrony Praw Osobistych Podczas Postępowania z Danymi Osobowymi w Grupie Deutsche Telekom

(English version is available below the polish version)

PREAMBUŁA

1. Ochrona danych osobowych klientów, pracowników i innych osób związanych z Grupą Deutsche Telekom stanowi najwyższy priorytet dla wszystkich spółek wchodzących w skład Grupy Deutsche Telekom.
2. Spółki Grupy Deutsche Telekom mają świadomość, że sukces Deutsche Telekom jako całości jest uzależniony nie tylko od globalnej sieci przepływu informacji, ale również przede wszystkim od odpowiedzialnego i bezpiecznego postępowania z danymi osobowymi.
3. W wielu obszarach Grupa Deutsche Telekom jest postrzegana przez jej klientów i społeczeństwo jako jeden podmiot. Z tego względu spółki z Grupy Deutsche Telekom dążą we wspólnym interesie do przyczynienia się w istotny sposób do wspólnego sukcesu firmy i wspierania deklaracji, że Grupa Deutsche Telekom jest dostawcą wysokiej jakości produktów i innowacyjnych usług poprzez wdrożenie niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
4. Przekazując niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności, Grupa Deutsche Telekom ustanawia jednolity i wysoki poziom prywatności danych w skali globalnej, mający zastosowanie do wykorzystania danych zarówno w jednej spółce, jak i pomiędzy spółkami, a także do przekazywania danych w Niemczech i w skali międzynarodowej. W Grupie Deutsche Telekom dane osobowe muszą być przetwarzane przez odbiorcę zgodnie z zasadami określonymi przez przepisy dotyczące ochrony danych, które mają zastosowanie do strony przekazującej.

CZĘŚĆ PIERWSZA. ZAKRES

§ 1 Charakter prawny Wiążących Reguł Korporacyjnych dotyczących Prywatności

Wiążące Reguły Korporacyjne dotyczące Prywatności będą obowiązywać w zakresie przetwarzania danych osobowych (według dokumentu roboczego 133, Grupy Roboczej Art. 29 Komisji Europejskiej) przez wszystkie spółki Grupy Deutsche Telekom, które przyjęły je do stosowania jako prawnie wiążące. Wiążące Reguły Korporacyjne dotyczące Prywatności będą również obowiązywać wszystkie spółki, w przypadku których ich przyjęcie wymagane jest przez Deutsche Telekom oraz wszystkie spółki, które przyjęły je dobrowolnie, niezależnie od miejsca zbierania danych.

§ 2 Zakres zastosowania

Wiążące Reguły Korporacyjne dotyczące Prywatności dotyczą wszystkich rodzajów danych osobowych wykorzystywanych w ramach Grupy Deutsche Telekom, niezależnie od miejsca zbierania danych. Dane osobowe wykorzystywane są w Grupie Deutsche Telekom w szczególności do następujących celów:

1. Do zarządzania danymi pracowników podczas inicjowania, wdrażania i przetwarzania umów o pracę oraz do przedstawiania pracownikom produktów i usług oferowanych im przez Grupę Deutsche Telekom lub osoby trzecie.
2. Do inicjowania, realizacji i przetwarzania umów z klientami biznesowymi i konsumentami oraz do wykonywania działań związanych z reklamą i badaniami rynku, mających na celu informowanie klientów i zainteresowane osoby

trzecie o produktach i usługach oferowanych odpowiednio przez Grupę Deutsche Telekom lub osoby trzecie.

3. Do inicjowania i realizacji umów z usługodawcami Grupy Deutsche Telekom w ramach świadczenia usług na rzecz Grupy Deutsche Telekom.
4. W celu umożliwienia utrzymywania odpowiednich relacji z innymi osobami trzecimi, w szczególności z udziałowcami, partnerami lub odwiedzającymi oraz w celu przestrzegania obowiązujących przepisów prawnych.

Dane wykorzystywane są zgodnie z obecnymi i przyszłymi celami biznesowymi spółek Grupy Deutsche Telekom, które obejmują świadczenie usług telekomunikacyjnych, usług cyfrowych dla konsumentów i klientów biznesowych, usług informatycznych (w tym usług centrum danych) i usług doradczych.

§ 3 Powiązania z innymi przepisami prawa

1. Postanowienia Wiążących Reguł Korporacyjnych dotyczących Prywatności mają na celu zapewnienie wysokiego i ujednoliconego poziomu prywatności danych w całej Grupie Deutsche Telekom. Niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności nie mają wpływu na istniejące obowiązki i regulacje, które powinny być przestrzegane przez poszczególne spółki w zakresie przetwarzania i wykorzystywania danych osobowych, wykraczające poza zasady zawarte w niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności lub zawierające dodatkowe ograniczenia w zakresie przetwarzania i wykorzystywania danych osobowych.
2. Dane zbierane w Europie są wykorzystywane zasadniczo zgodnie z przepisami prawa kraju, w którym dane zostały zebrane, niezależnie od miejsca wykorzystania danych, lecz co najmniej zgodnie z wymaganiami niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
3. Postanowienia niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności nie mają wpływu na stosowanie ustawodawstwa krajowego uchwalonego ze względów bezpieczeństwa państwa, obrony narodowej lub bezpieczeństwa publicznego lub w celu zapobiegania przestępstwom i prowadzenia dochodzenia w ich sprawie oraz ścigania przestępców, które wymaga przekazania danych osobom trzecim. Jeżeli spółka stwierdzi, że istotne fragmenty niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności są sprzeczne z krajowymi przepisami dotyczącymi prywatności danych, uniemożliwiając stronom podpisanie niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, Specjalista Grupy ds. Prywatności Danych w Grupie Deutsche Telekom zostanie o tym niezwłocznie poinformowany. Właściwy organ nadzorujący spółkę pełni funkcję rozjemczą.

§ 4 Wygaśnięcie i rozwiązanie

Niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności przestaną obowiązywać spółkę, jeżeli spółka wystąpi z Grupy Deutsche Telekom lub unieważni niniejsze zasady. Jednak wygaśnięcie lub unieważnienie Wiążących Reguł Korporacyjnych dotyczących Prywatności nie zwalnia spółki z obowiązków i/lub postanowień Wiążących Reguł Korporacyjnych dotyczących Prywatności, regulujących wykorzystanie danych, które zostały już przekazane. Dalsze przekazanie danych przez tę spółkę lub do tej spółki może nastąpić wyłącznie pod warunkiem zapewnienia innych odpowiednich gwarancji proceduralnych, zgodnie z wymaganiami prawa europejskiego.

CZĘŚĆ DRUGA. ZASADY

SEKCJA 1 PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH

§ 5 Obowiązek informacyjny

Osoby, których dane dotyczą są informowane o sposobie wykorzystania ich danych osobowych zgodnie z obowiązującymi przepisami i następującymi warunkami.

§ 6 Treść i forma informacji

1. Spółka informuje w odpowiedni sposób osoby, których dane dotyczą o następujących sprawach:
   a) tożsamość administratora danych i jego dane kontaktowe.
   b) przeznaczenie i cel wykorzystania danych. Powyższe informacje powinny określać, jakie dane są ewidencjonowane i/lub przetwarzane/wykorzystywane, dlaczego, w jakim celu i przez jaki okres.
   c) jeżeli dane osobowe są przekazywane lub transferowane osobom trzecim, powinny być znane takie szczegóły jak odbiorca, zakres i cel(e) przekazywania/transferu.
   d) prawa osób, których dane dotyczą w związku z wykorzystaniem ich danych.
2. Niezależnie od wybranego środka przekazu, osoby, których dane dotyczą otrzymają powyższe informacje w jasny i zrozumiały sposób.

§ 7 Dostępność informacji

Informacje są dostępne dla osób, których dane dotyczą, podczas zbierania danych, a następnie na żądanie.

SEKCJA 2. WARUNKI DOPUSZCZALNOŚCI WYKORZYSTANIA DANYCH OSOBOWYCH

§ 8 Zasada

Dane osobowe są wykorzystywane wyłącznie po spełnieniu następujących warunków i nie są wykorzystywane do innych celów niż cele, do których zostały pierwotnie zebrane.

Wykorzystanie zebranych danych do innych celów jest dozwolone wyłącznie, jeżeli spełnione zostały wymogi dopuszczalności, zgodne z następującymi warunkami.

§ 9 Dopuszczalność wykorzystania danych osobowych

Dane osobowe mogą zostać wykorzystane, jeżeli spełnione jest jedno lub więcej z poniższych kryteriów:

a) Wykorzystanie danych w planowany sposób jest wyraźnie dopuszczone przez prawo.

b) Osoba, której dotyczą dane udzieliła zgody na wykorzystanie jej/jego danych.

c) Niezbędne jest wykorzystanie danych w ten sposób w celu spełnienia przez spółkę jej obowiązków wynikających z umowy z osobą, której dane dotyczą, w tym jej obowiązków umownych dotyczących informowania i/lub drugorzędnych obowiązków lub w celu wdrożenia przez spółkę środków przed zawarciem umowy lub po zawarciu umowy w celu inicjowania lub przetwarzania umowy na żądanie osoby, której dane dotyczą.

d) Dane muszą zostać wykorzystane w celu spełnienia obowiązku prawnego spoczywającego na spółce.

e) Niezbędne jest wykorzystanie danych do ochrony żywotnych interesów osoby, której dane dotyczą.

f) Niezbędne jest wykorzystanie danych w celu wykonania zadania, które leży w interesie publicznym lub które wpisuje się w wykonywanie władzy publicznej i które zostało nałożone na spółkę lub osobę trzecią, której przekazywane są dane.

g) Niezbędne jest przetwarzanie danych w celu realizacji prawnie usprawiedliwionych interesów spółki lub osoby trzeciej/osób trzecich, której/którym dane są transferowane, pod warunkiem że powyższe interesy nie zostaną wyraźnie przeważone przez interesy osoby, której dane dotyczą, uzasadniające ochronę.

§ 10 Zgoda osoby, której dane dotyczą

Przyjmuje się, że osoba, której dane dotyczą udzieliła zgody na podstawie § 9 ust. 1, pkt b) niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, jeżeli:

a) Zgoda została udzielona wyraźnie, dobrowolnie i świadomie, co gwarantuje, że osoba, której dane dotyczą jest świadoma zakresu wyrażonej zgody. Brzmienie oświadczenia o wyrażeniu zgody jest wystarczająco precyzyjne i informuje osoby, których dane dotyczą o przysługujących im prawach do cofnięcia zgody w dowolnym czasie. W przypadku modeli biznesowych, w których cofnięcie zgody prowadzi do niewykonania obowiązków umownych, osoba, której dane dotyczą, jest o tym informowana.

b) Zgoda została uzyskana w formie adekwatnej do okoliczności (w formie pisemnej). W wyjątkowych przypadkach może zostać uzyskana ustnie, jeżeli fakt wyrażenia zgody i szczególne okoliczności uzasadniające ustną zgodę są odpowiednio udokumentowane.

§ 11 Automatyczne decyzje indywidualne

a) Decyzje oceniające indywidualne aspekty dotyczące danej osoby i które mogą się wiązać z konsekwencjami prawnymi dla tej osoby lub które mogą mieć znaczny niekorzystny wpływ na tę osobę nie będą oparte wyłącznie na automatycznym wykorzystaniu danych. Obejmuje to w szczególności decyzje, dla których istotne są dane dotyczące wiarygodności kredytowej, predyspozycji zawodowych lub stanu zdrowia osoby, której dane dotyczą.

b) Jeżeli w indywidualnych przypadkach wystąpi obiektywna potrzeba podjęcia automatycznej decyzji, osoba, które dane dotyczą, zostanie niezwłocznie poinformowana o wyniku automatycznej decyzji i będzie miała możliwość zgłoszenia uwag w odpowiednim terminie. Uwagi osoby, której dane dotyczą, zostaną odpowiednio uwzględnione przed podjęciem ostatecznej decyzji.

§ 12 Wykorzystanie danych osobowych do celów marketingu bezpośredniego

Jeżeli dane są wykorzystywane do celów marketingu bezpośredniego, osoby, których dane dotyczą:

a) są informowane o sposobie, w jaki ich dane zostaną wykorzystane do celów marketingu bezpośredniego;

b) są informowane o przysługującym im prawie do wyrażenia sprzeciwu wobec wykorzystania ich danych osobowych do celów bezpośredniej komunikacji marketingowej oraz

c) mają możliwość wykonania przysługującego im prawa do nieotrzymywania powyższej komunikacji. W szczególności otrzymają informacje dotyczące spółki, do której należy skierować sprzeciw.

§ 13 Szczególne kategorie danych osobowych

a) Wykorzystanie szczególnych kategorii danych jest dopuszczone wyłącznie, jeżeli jest regulowane przez przepisy lub jeżeli uzyskano uprzednio zgodę osoby, której dane dotyczą. Jest również dopuszczalne, jeżeli przetwarzanie danych jest niezbędne w celu wykonania praw i obowiązków spółki w obszarze prawa pracy, jeżeli podjęte zostaną stosowne środki ochrony i nie jest to zabronione przez prawo krajowe.

b) Przed rozpoczęciem zbierania, przetwarzania lub wykorzystywania danych spółka poinformuje swojego Specjalistę ds. Prywatności Danych i udokumentuje takie działania. Podczas oceny dopuszczalności należy zwrócić szczególną uwagę na charakter, zakres, cel, konieczność i podstawę prawną wykorzystania danych.

§ 14 Oszczędne wykorzystanie danych, ograniczenie wykorzystania danych, anonimizacja danych i stosowanie aliasów

1. Dane osobowe powinny być odpowiednie i istotne oraz nie nadmierne w stosunku do wykorzystania danych do konkretnego celu (oszczędne wykorzystanie danych). Dane powinny być przetwarzane w ramach określonej aplikacji wyłącznie jeżeli jest to niezbędne (ograniczenie wykorzystania danych).
2. Jeżeli jest to możliwe i zasadne z ekonomicznego punktu widzenia, należy stosować procedury usuwania cech identyfikujących osoby, których dane dotyczą (anonimizacja) lub zastępować cechy identyfikujące innymi charakterystykami (stosowanie aliasów).

§ 15 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.

SEKCJA 3. PRZEKAZYWANIE DANYCH OSOBOWYCH

§ 16 Charakter i cel przekazywania danych osobowych

1. Dane osobowe mogą być przekazywane wyłącznie, jeżeli strona otrzymująca przyjmuje odpowiedzialność za otrzymane dane (transferowanie danych) lub jeżeli odbiorca wykorzystuje dane wyłącznie zgodnie z instrukcjami i wymaganiami strony przekazującej (umowa powierzenia przetwarzania danych).
2. Dane osobowe mogą być przekazywane wyłącznie w dozwolonych celach, zgodnie z § 9 niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności w ramach działalności gospodarczej spółki lub obowiązków prawnych, lub po uzyskaniu zgody osób, których dane dotyczą.

§ 17 Transferowanie danych

1. Jeżeli spółka dokonuje transferu danych organom, których centrala znajduje się w kraju trzecim lub które przekazują dane poza granice kraju, należy podjąć kroki w celu zapewnienia, że powyższe dane są transferowane we właściwy sposób. Odpowiednie wymagania dotyczące prywatności danych i bezpieczeństwa danych powinny zostać uzgodnione z odbiorcą danych przed ich transferem. Ponadto dane osobowe, w szczególności dane zbierane w UE lub EOG, są transferowane administratorom spoza obszaru Unii Europejskiej wyłącznie, jeżeli zapewniony jest odpowiedni poziom prywatności danych za pomocą niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności lub innych odpowiednich środków, takich jak standardowe klauzule umowne EU lub indywidualne porozumienia umowne, które spełniają stosowne wymagania prawa europejskiego.
2. Na podstawie wymagań Grupy Deutsche Telekom i powszechnie uznanych standardów technicznych i organizacyjnych podejmowane są odpowiednie środki techniczne i organizacyjne w celu zagwarantowania

bezpieczeństwa danych osobowych, w tym podczas ich transferu.

§ 18 Powierzenie przetwarzania danych

1. Jeżeli spółka (klient) zleca osobie trzeciej (wykonawcy) świadczenie usług w jej (jego) imieniu, zgodnie z jej (jego) instrukcjami, wówczas, oprócz umowy o świadczenie usług obejmującej prace do wykonania, umowa powinna również określać obowiązki wykonawcy jako strony, której zlecono przetwarzanie danych. Powyższe obowiązki określają instrukcje klienta dotyczące rodzaju i sposobu przetwarzania danych osobowych, celu przetwarzania oraz środków technicznych i organizacyjnych wymaganych do ochrony danych.
2. Wykonawca nie będzie wykorzystywać danych osobowych (powierzonych mu w celu wykonania zlecenia) do jego własnych celów lub celów osoby trzeciej związanych z przetwarzaniem bez uprzedniej zgody klienta. Wykonawca poinformuje uprzednio klienta o planach zlecenia podwykonania prac innym osobom trzecim w celu wypełnienia jego obowiązków umownych. Klient ma prawo sprzeciwić się powyższemu wykorzystaniu podwykonawców. W przypadku wykorzystania podwykonawców w dozwolony sposób, wykonawca zobowiąże ich do spełniania wymagań wynikających z umów zawartych pomiędzy wykonawcą i klientem.
3. Wyboru podwykonawców dokonuje się na podstawie możliwości spełnienia przez nich powyższych wymagań.

SEKCJA 4. JAKOŚĆ DANYCH I BEZPIECZEŃSTWO DANYCH

§ 19 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.

§ 20 Bezpieczeństwo danych – środki techniczne i organizacyjne

Spółka podejmie odpowiednie środki techniczne i organizacyjne w odniesieniu do procesów spółki, systemów i platform informatycznych wykorzystywanych do zbierania, przetwarzania lub wykorzystania danych w celu ochrony tych danych.

Powyższe środki obejmują:

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 odczytania, 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 odczytania, skopiowania, zmodyfikowania lub usunięcia danych osobowych oraz że za pomocą sprzętu służącego do przekazywania danych będzie możliwe jednoznaczne ustalenie oraz zweryfikowanie odbiorców, którym dane mają zostać 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 przetwarzanie danych powierzonych odbywać się będzie 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).

CZĘŚĆ TRZECIA. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

§ 21 Prawo do informacji

1. Osoby, których dane dotyczą, mogą się w dowolnym czasie skontaktować ze spółką, która wykorzystuje ich dane i domagać się podania następujących informacji:
   a) dotyczących ich danych osobowych znajdujących się w posiadaniu spółki, łącznie z ich pochodzeniem i odbiorcą (odbiorcami);
   b) celu wykorzystania;
   c) dotyczących osób i administratorów, do których dane są regularnie przesyłane, w szczególności jeżeli dane są przesyłane za granicę;
   d) postanowień niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
2. Odpowiednie informacje powinny zostać udzielone osobie składającej zapytanie w zrozumiałej formie i w odpowiednim terminie. Następuje to zwykle w formie pisemnej lub elektronicznie. Przekazanie wydruku niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności jest wystarczające jako sposób przekazania informacji o ich wymaganiach.

Jeżeli dopuszczają to odpowiednie przepisy krajowe, spółka może naliczyć opłatę za przekazanie odpowiednich informacji.

§ 22 Prawo sprzeciwu, prawo do usunięcia lub zablokowania danych i prawo do poprawienia

1. Osoby, których dane dotyczą mogą sprzeciwić się wykorzystaniu ich danych w dowolnym czasie, jeżeli dane te są wykorzystywane do celów, które nie są prawnie obowiązujące.
2. Prawo sprzeciwu przysługuje również w przypadku, gdy osoby, których dane dotyczą wyraziły uprzednio zgodę na wykorzystanie ich danych.
3. Uzasadnione wnioski o usunięcie lub zablokowanie danych zostaną niezwłocznie zrealizowane. Powyższe wnioski są uzasadnione zwłaszcza w przypadku, gdy podstawa prawna wykorzystania danych przestanie obowiązywać. Jeżeli osoba, której dane dotyczą ma prawo do usunięcia danych, lecz usunięcie danych nie jest możliwe lub jest bezzasadne, dane będą chronione przed niedozwolonym wykorzystaniem poprzez ich zablokowanie. Przestrzegane są ustawowe terminy przechowywania.
4. Osoby, których dane dotyczą, mogą domagać się od spółki w dowolnym czasie poprawienia dotyczących ich danych osobowych przechowywanych przez spółkę, jeżeli dane są niekompletne i/lub nieprawidłowe.
5. W przypadku modeli biznesowych, w których cofnięcie lub usunięcie prowadzi do niewykonania obowiązków umownych, osoba, której dane dotyczą, jest o tym informowana.

§ 23 Prawo do wyjaśnienia, zgłoszenia uwag i podjęcia działań naprawczych

1. Jeżeli osoba, której dane dotyczą twierdzi, że jej/jego prawa zostały naruszone przez bezprawne wykorzystanie jej/jego danych, w szczególności przedstawiając dowody znajdującego potwierdzenie w faktach naruszenia niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, odpowiedzialne spółki wyjaśnią sytuację bez rozmyślnej zwłoki. W przypadku danych przekazywanych lub przesyłanych w szczególności do spółek poza terytorium Unii Europejskiej, spółka mająca siedzibę w Unii Europejskiej wyjaśni sytuację i przedstawi dowody, że strona otrzymująca nie naruszyła wymagań niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności danych ani nie jest odpowiedzialna za żadne powstałe szkody. Spółki będą ściśle współpracować w celu wyjaśnienia sytuacji i zapewnią sobie wzajemnie dostęp do wszelkich informacji niezbędnych im w tym celu.
2. Zainteresowana osoba, której dane dotyczą, może wnieść w dowolnym czasie zażalenie do Grupy Deutsche Telekom Holding, jeżeli podejrzewa, że spółka Grupy Deutsche Telekom nie przetwarza jej/jego danych osobowych zgodnie z wymaganiami przepisów prawa lub z postanowieniami niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Uzasadnione zażalenie zostanie rozpatrzone w odpowiednim czasie i osoba, której dane dotyczą, otrzyma odpowiednie informacje.
3. Jeżeli zażalenie dotyczy kilku spółek, Specjalista ds. Prywatności Danych spółki, która jest najlepiej zaznajomiona z przedmiotem, będzie koordynować całość odpowiedniej korespondencji z osobą, której dane dotyczą. Specjalista Grupy ds. Prywatności Danych będzie upoważniony w dowolnym czasie do skorzystania z przysługującego mu prawa subrogacji i przejęcia.
4. Udostępnione zostaną odpowiednie kanały do zgłaszania incydentów w zakresie prywatności danych (takie jak specjalne konta e-mail udostępniane przez Pion Ochrony Danych, Zagadnień Prawnych i Zgodności lub bezpośrednia osoba kontaktowa, z którą można się skontaktować elektronicznie).
5. Specjalista ds. Prywatności Danych zainteresowanej spółki poinformuje niezwłocznie Specjalistę Grupy ds. Prywatności Danych o incydencie w zakresie prywatności danych za pomocą odpowiednich procesów raportowania.
6. Osoby, których dane dotyczą, mogą wnieść roszczenie zgodnie z Częścią Piątą niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, jeżeli ich prawa zostały naruszone lub poniosły one jakiekolwiek straty.

§ 24 Prawo do zadawania pytań i zgłaszania skarg

Każda osoba, której dane dotyczą ma prawo do skontaktowania się w dowolnym czasie ze Specjalistą ds. Prywatności Danych spółki wykorzystującej jej/jego dane osobowe oraz zadawania pytań i zgłaszania skarg dotyczących stosowania niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Spółka najlepiej zaznajomiona z przedmiotem lub spółka, która zebrała dane osoby, której dane dotyczą zapewni, że prawa osoby, której dane dotyczą, będą respektowane przez inne odpowiedzialne spółki.

§ 25 Wykonywanie praw przysługujących osobom, których dane dotyczą

Osoby, których dane dotyczą, nie zostaną postawione w niekorzystnej sytuacji ze względu na skorzystanie przez nie z tych praw. Forma komunikacji z osobą, której dane dotyczą – np. telefonicznie, elektronicznie lub w formie pisemnej – powinna być w miarę możliwości zgodna z formą proponowaną przez osobę, której dane dotyczą.

§ 26 Wydruk Wiążących Reguł Korporacyjnych dotyczących Prywatności

Wydruk niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności zostanie dostarczony na żądanie.

CZĘŚĆ CZWARTA. ORGANIZACJA PRYWATNOŚCI DANYCH

§ 27 Odpowiedzialność za przetwarzanie danych

Spółki są zobowiązane do zapewnienia zgodności z przepisami prawa dotyczącymi ochrony danych oraz z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności.

§ 28 Specjalista ds. Prywatności Danych

1. Każda spółka mianuje niezależnego Specjalistę ds. Prywatności Danych, którego zadaniem jest zapewnienie, że poszczególne jednostki organizacyjne tej spółki są informowane o ustawowych i wewnętrznych wymaganiach spółki/Grupy w zakresie prywatności danych oraz w szczególności o niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności. Specjalista ds. Prywatności Danych stosuje odpowiednie środki, w szczególności wyrywkowe inspekcje, w celu monitorowania zgodności z przepisami dotyczącymi ochrony danych.
2. Spółka skonsultuje się ze Specjalistą Grupy ds. Prywatności Danych przed mianowaniem Specjalisty ds. Prywatności Danych.
3. Spółka zapewni, że Specjalista ds. Prywatności Danych posiada odpowiednie kompetencje do oceny aspektów prawnych, technicznych i organizacyjnych środków ochrony prywatności danych.
4. Spółka udostępni Specjaliście ds. Prywatności Danych zasoby finansowe i osobowe niezbędne do wykonywania jego/jej obowiązków.
5. Specjalista ds. Prywatności Danych otrzyma prawo do raportowania bezpośrednio do kierownictwa spółki i będzie powiązany organizacyjnie z kierownictwem spółki.
6. Specjalista ds. Prywatności Danych każdej spółki jest odpowiedzialny za wdrożenie wymagań Specjalisty Grupy ds. Prywatności Danych i strategii prywatności danych Grupy Deutsche Telekom.
7. Wszystkie departamenty każdej spółki są zobowiązane do informowania Specjalisty ds. Prywatności Danych w ich spółce o sytuacji w zakresie infrastruktury informatycznej, infrastruktury sieciowej, modeli biznesowych, produktów, przetwarzania danych pracowników i odpowiednich planach strategicznych. Specjalista ds. Prywatności Danych jest powiadamiany o zaistniałej sytuacji we wczesnej fazie w celu zapewnienia, że wszelkie sprawy dotyczące prywatności danych zostaną rozpatrzone i poddane ocenie.

§ 29 Specjalista Grupy ds. Prywatności Danych

1. Specjalista Grupy ds. Prywatności Danych koordynuje procesy współpracy i uzgadniania wszelkich istotnych spraw dotyczących prywatności danych w ramach Grupy Deutsche Telekom. Informuje prezesa Holdingu Grupy Deutsche Telekom o aktualnej sytuacji i w razie potrzeby opracowuje rekomendacje.
2. Obowiązkiem Specjalisty Grupy ds. Prywatności Danych jest opracowanie i rozwijanie polityki prywatności danych Grupy Deutsche Telekom oraz przeprowadzanie w razie potrzeby konsultacji ze Specjalistami ds. Prywatności Danych spółek Grupy. Specjaliści ds. Prywatności Danych opracowują politykę prywatności danych dla ich spółek zgodnie z polityką Grupy dotyczącą prywatności danych. Specjalista Grupy ds. Prywatności Danych i Specjaliści ds. Prywatności Danych ze spółek krajowych spotykają się co roku w celu wymiany informacji na Międzynarodowych Spotkaniach Specjalistów ds. Prywatności (bezpośrednie spotkania).

§ 30 Obowiązek informowania w przypadku naruszeń

Zainteresowana spółka niezwłocznie informuje jej Specjalistę ds. Prywatności Danych o wszelkich naruszeniach lub sytuacjach wskazujących wyraźnie na naruszenie przepisów dotyczących ochrony danych, w szczególności niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Specjalista ds. Prywatności Danych z kolei informuje niezwłocznie Specjalistę Grupy ds. Prywatności Danych, jeżeli incydent ma potencjalny wpływ na publiczny wizerunek spółki, dotyczy więcej niż jednej spółki lub wiąże się z potencjalną stratą w wysokości ponad 500 000 euro. Specjalista ds. Prywatności Danych spółki informuje również Specjalistę Grupy ds. Prywatności Danych w przypadku wprowadzenia zmian do przepisów mających zastosowanie do spółki, które są w znacznym stopniu niekorzystne w aspekcie zgodności z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności.

§ 31 Przegląd poziomu prywatności danych

1. Przeglądy mające na celu sprawdzenie zgodności z wymaganiami niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności i wynikającego z nich poziomu prywatności danych są przeprowadzane przez Specjalistę Grupy ds. Prywatności Danych w ramach rocznego planu inspekcji oraz za pomocą innych środków, takich jak inspekcje przeprowadzane przez Specjalistów ds. Prywatności Danych spółek i sprawozdawczość.
2. Wewnętrzni i zewnętrzni audytorzy przeprowadzają inspekcje zlecone przez Specjalistę Grupy ds. Prywatności Danych. W ramach Grupy Deutsche Telekom przeprowadzane są również regularne procesy samooceny koordynowane przez Specjalistę Grupy ds. Prywatności Danych. Prezes Holdingu Grupy Deutsche Telekom jest informowany o wynikach najważniejszych inspekcji i środkach uzgodnionych po ich przeprowadzaniu. Właściwy organ nadzoru ds. ochrony danych otrzymuje kopię wyników inspekcji na żądanie. Organ nadzoru odpowiedzialny za spółkę może również zainicjować inspekcję. Spółka zapewni wszelkie możliwe wsparcie podczas powyższych inspekcji i wdroży wynikające z nich środki.
3. Spółka podejmie również odpowiednie środki w celu usunięcia słabych punktów zidentyfikowanych w trakcie inspekcji, a Specjalista Grupy ds. Prywatności Danych będzie monitorować wdrożenie tych środków. W przypadku niewdrożenia przez spółkę takich środków bez odpowiedniego uzasadnienia, Specjalista Grupy ds. Prywatności Danych oceni wpływ na prywatność danych i podejmie niezbędne działania, eskalując sprawę w razie potrzeby.
4. Specjaliści ds. Prywatności Danych spółek lub innych jednostek organizacyjnych, którym zlecono przeprowadzenie inspekcji przeprowadzą również kontrole na podstawie dedykowanych planów audytów udokumentowanych w formie pisemnej w celu stwierdzenia, czy spółki spełniają wymagania w zakresie ochrony danych.
5. Jeżeli nie istnieją ograniczenia prawne w tym zakresie, Specjalista Grupy ds. Prywatności Danych i Specjaliści ds. Prywatności Danych są upoważnieni do sprawdzenia, odpowiednio we wszystkich spółkach i w ich spółce, czy dane osobowe są wykorzystywane prawidłowo. Odpowiednie spółki zapewnią Specjaliście Grupy ds. Prywatności Danych i Specjalistom ds. Prywatności Danych nieograniczony dostęp do informacji, które są im niezbędne w celu wyjaśnienia i oceny sytuacji. Specjalista Grupy ds. Prywatności Danych i Specjaliści ds. Prywatności Danych są upoważnieni do wydania instrukcji w tym zakresie.
6. W ramach przeprowadzanych przez nich inspekcji, Specjaliści ds. Prywatności Danych spółek korzystają ze standardowych procedur obowiązujących w całej Grupie, np. wspólne audyty ochrony danych, jeżeli jest to możliwe. Powyższe procedury mogą zostać udostępnione przez Specjalistę Grupy ds. Prywatności Danych.

§ 32 Zaangażowanie i szkolenia pracowników

1. Spółki zobowiązują swoich pracowników do zachowania tajemnicy danych i tajemnicy telekomunikacyjnej nie później niż od rozpoczęcia ich zatrudnienia. Pracownicy zostaną odpowiednio przeszkoleni w zakresie prywatności danych w ramach tego zobowiązania. Spółka zainicjuje odpowiednie procesy i zapewni w tym celu środki.
2. Pracownicy będą uczestniczyć w szkoleniach dotyczących podstaw prywatności danych regularnie lub co najmniej

raz na dwa lata. Spółki są upoważnione do opracowania i prowadzenia dedykowanych szkoleń dla ich własnych pracowników. Specjalista ds. Prywatności Danych każdej spółki dokumentuje przeprowadzenie powyższych szkoleń i informuje co roku Specjalistę Grupy ds. Prywatności Danych.

3. Specjalista Grupy ds. Prywatności Danych może udostępnić centralnie zasoby i procesy w celu zobowiązania i przeszkolenia pracowników Grupy Deutsche Telekom.

§ 33 Współpraca z organami nadzoru

1. Spółki zobowiązują się do współpracy na zasadzie zaufania z organem nadzoru odpowiedzialnym za nie lub za spółkę przesyłającą dane, w szczególności do udzielania odpowiedzi na pytania i wdrażanie rekomendacji.
2. W przypadku zmiany przepisów dotyczących spółki, które mają istotny niekorzystny wpływ na gwarancje zapewniane w niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności, odpowiednia spółka powiadomi o zmianie właściwy organ nadzoru.

§ 34 Odpowiedzialna osoba kontaktowa ds. zapytań

Specjaliści ds. Prywatności Danych spółek lub Specjalista Grupy ds. Prywatności Danych są osobami kontaktowymi odpowiedzialnymi za udzielanie odpowiedzi na pytania dotyczące niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Specjalista Grupy ds. Prywatności Danych przekaże dane kontaktowe Specjalistów ds. Prywatności Danych spółek na żądanie.

CZĘŚĆ PIĄTA. ODPOWIEDZIALNOŚĆ

§ 35 Obszar zastosowania zasad dotyczących odpowiedzialności

1. Niniejsza Część Piąta Wiążących Reguł Korporacyjnych dotyczy wyłącznie przetwarzania danych osobowych zbieranych na terytorium UE/EOG, które mieści się w zakresie unijnej Dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.
2. Na terytorium UE/EOG obowiązują postanowienia dotyczące odpowiedzialności prawnej kraju, w którym ma siedzibę spółka. W przypadku danych, które nie podlegają § 35, Sekcja 1 BCRP, obowiązują postanowienia dotyczące odpowiedzialności prawnej kraju, w którym ma siedzibę odpowiednia spółka, która zebrała dane lub jeżeli nie istnieją przepisy prawa w tym zakresie, warunki spółki, która zebrała dane.
3. Zapłata odszkodowania z nawiązką, w przypadku której spółka musi zapłacić osobie, której dane dotyczą kwotę przewyższającą wartość szkody, zostanie wyraźnie wykluczona.

§ 36 Zwolnienia z odpowiedzialności

1. Osoba, która poniosła stratę w wyniku naruszenia jednego lub więcej obowiązków określonych w Wiążących Regułach Korporacyjnych dotyczących Prywatności przez spółkę Grupy Deutsche Telekom lub przez odbiorców danych, którym spółka Grupy Deutsche Telekom przekazała lub przesłała dane, jest uprawniona do dochodzenia odszkodowania od odpowiednich spółek Grupy Deutsche Telekom.
2. Osoba, której dane dotyczą jest również uprawniona do dochodzenia odszkodowania od spółki holdingowej Grupy

Deutsche Telekom. Jeżeli spółka holding wypłaci odszkodowanie, będzie ona uprawniona do domagania się zwrotu kwoty odszkodowania od spółek, które są odpowiedzialne za stratę lub które zleciły wykonanie prac osobie trzeciej, która spowodowała szkodę.

3. Osoba, której dane dotyczą dochodzi początkowo odszkodowania od spółki, która przekazała lub przesłała dane. Jeżeli spółka przekazująca nie jest odpowiedzialna de iure lub de facto, osoba, której dane dotyczą jest uprawniona do dochodzenia odszkodowania od spółki będącej odbiorcą. Spółka otrzymująca nie jest uprawniona do odstąpienia od odpowiedzialności przez odwołanie się do odpowiedzialności wykonawcy w przypadku naruszenia.
4. Osoba, której dane dotyczą jest również uprawniona do wniesienia w dowolnym czasie skargi do właściwego organu nadzoru lub organu nadzoru odpowiedzialnego za spółkę holdingową Grupy Deutsche Telekom.

§ 37 Ciężar dowodu

Ciężar dowodu prawidłowego wykorzystania danych osoby, której dane dotyczą, spoczywa na odpowiedzialnych spółkach.

§ 38 Korzyści osoby trzeciej dla osób, których dane dotyczą

Jeżeli osobie, której dane dotyczą nie przysługują żadne bezpośrednie prawa, osoba ta jest uprawniona, jako beneficjent będący osobą trzecią, do dochodzenia roszczeń w stosunku do spółek, które naruszyły ich obowiązki umowne, na podstawie postanowień niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.

§ 39 Miejsce jurysdykcji

Według uznania zainteresowanej osoby, miejscem jurysdykcji do dochodzenia roszczeń odszkodowawczych może być

a) miejsce mające zastosowanie do zainteresowanej osoby lub
b) miejsce w jurysdykcji członka grupy w momencie inicjowania przekazania lub
c) siedziba na terytorium UE europejskiego członka grupy, na którym spoczywają obowiązki związane z ochroną danych.

§ 40 Rozstrzygnięcie pozasądowe

1. Osoby trzecie, które uważają, że ich indywidualne prawo do prywatności zostało naruszone w wyniku rzeczywistego lub podejrzewanego wykorzystania ich danych osobowych mają prawo domagać się od Specjalisty ds. Prywatności Danych odpowiedniej spółki rozstrzygnięcia tej sprawy. Specjalista ds. Prywatności Danych jest uprawniony do zbadania skargi i poinformowania osoby, której dane dotyczą, o przysługujących jej/jemu prawach. Podczas wykonywania tych czynności Specjalista ds. Prywatności Danych jest zobowiązany do zachowania poufności innych danych osobowych skarżącego, chyba że skarżący zwolni Specjalistę ds. Prywatności Danych z tego obowiązku. Na wniosek zainteresowanej osoby podjęta zostanie próba osiągnięcia porozumienia w sprawie skargi, z udziałem osoby, której dane dotyczą i Specjalisty ds. Prywatności Danych. Powyższe porozumienie może również obejmować rekomendację w sprawie rekompensaty za stratę poniesioną przez osobę, której dane dotyczą wskutek naruszenia jej/jego prawa do prywatności. Rekomendacja jest wiążąca dla odpowiednich spółek, jeżeli została zatwierdzona w drodze wzajemnego porozumienia.
2. Prawo do złożenia skargi do właściwego organu nadzoru lub do wszczęcia czynności prawnych pozostaje nienaruszone.

CZĘŚĆ SZÓSTA. POSTANOWIENIA KOŃCOWE

§ 41 Przegląd i zmiany do niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności

1. Specjalista Grupy ds. Prywatności Danych bada Wiążące Reguły Korporacyjne dotyczące Prywatności w regularnych odstępach czasu, lecz co najmniej raz w roku, w celu weryfikacji ich zgodności z obowiązującymi przepisami i może wprowadzić niezbędne zmiany.
2. Wszelkie istotne zmiany do niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, które staną się niezbędne np. wskutek modyfikacji dokonanych w celu dostosowania ich do wymagań prawnych, zostaną uzgodnione z organem nadzoru. Powyższe zmiany mają zastosowanie bezpośrednio do wszystkich spółek, które podpisały Wiążące Reguły Korporacyjne dotyczące Prywatności po upływie odpowiedniego okresu przejściowego.
3. Specjalista Grupy ds. Prywatności Danych poinformuje wszystkie spółki, które wprowadziły Wiążące Reguły Korporacyjne dotyczące Prywatności o zmienionej treści.
4. Specjaliści ds. Prywatności Danych spółek mają obowiązek zbadania, czy zmiany wprowadzone do niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności mają implikacje dla zgodności z przepisami w ich własnym kraju lub czy są sprzeczne z przepisami prawa w ich odpowiednim kraju. Jeżeli spółka nie ma możliwości wprowadzenia zmian ze względu na obowiązujące uwarunkowania prawne, spółka poinformuje niezwłocznie Specjalistę Grupy ds. Prywatności Danych i właściwy organ nadzoru, a w razie potrzeby odpowiednie postanowienia Wiążących Reguł Korporacyjnych dotyczących Prywatności zostaną czasowo zawieszone w odniesieniu do tej spółki.

§ 42 Wykaz danych kontaktowych i spółek

Specjalista Grupy ds. Prywatności Danych prowadzi wykaz spółek, które wprowadziły niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności i danych kontaktowych tych spółek. Aktualizuje on powyższy wykaz i informuje osoby, których dane dotyczą oraz organ ds. ochrony danych na żądanie.

§ 43 Prawo procesowe/klauzula salwatoryjna

W przypadku sporów niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności regulowane są przez prawo procesowe Federalnej Republiki Niemiec.

Jeżeli poszczególne postanowienia niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności są lub staną się nieważne, zostaną one uznane za zastąpione przez postanowienia, które odpowiadają jak najdokładniej pierwotnym intencjom niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności i nieważnym postanowieniom. W razie wątpliwości, w takich przypadkach lub w przypadku braku odpowiednich przepisów prawa mają zastosowanie odpowiednie przepisy Unii Europejskiej dotyczące ochrony danych.

§ 44 Publikacja

Spółki udostępniają publicznie informacje dotyczące praw osób, których dane dotyczą i klauzuli korzyści dla osoby trzeciej w odpowiedniej formie, np. w informatorach na temat ochrony danych w Internecie. Powyższe informacje są publikowane niezwłocznie, gdy niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności staną się wiążące dla spółki.

CZĘŚĆ SIÓDMA. DEFINICJE I TERMINY

Stosowanie aliasów

Oznacza zastąpienie nazwiska osoby i innych cech identyfikacyjnych przez inne charakterystyki w celu uniemożliwienia identyfikacji osoby, której dane dotyczą lub znacznego utrudnienia identyfikacji osoby, której dane dotyczą.

Anonimizacja

Anonimizacja oznacza proces zmiany informacji w taki sposób, że dane osobowe i inne fakty nie pozwalają na ustalenie zidentyfikowanej lub możliwej do identyfikacji osoby fizycznej lub nie pozwalają na doprowadzenie do takiej osoby bez nieproporcjonalnie dużych nakładów czasu, kosztów i energii.

Automatyczne decyzje indywidualne

Oznaczają decyzje, które mają implikacje prawne dla osoby, której dane dotyczą lub które mają istotny niekorzystny wpływ na tę osobę i które są oparte wyłącznie na automatycznym przetwarzaniu danych mających na celu ocenę określonych aspektów prywatnych osoby, której dane dotyczą, takich jak jej/jego wyniki osiągane w pracy, zdolność kredytowa, rzetelność, zachowanie itp.

Spółka

Oznacza spółkę objętą niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności. Odrębny wykaz tych spółek jest prowadzony do celów informacyjnych i na bieżąco aktualizowany. Wykaz jest dostępny dla wszystkich osób w dowolnym czasie.

Administrator

Oznacza organ, który przetwarza dane osobowe, lecz niekoniecznie jest osobą prawną.

Osoba, której dane dotyczą

Oznacza osobę fizyczną, której dane osobowe są przetwarzane w ramach Grupy Deutsche Telekom.

Grupa Deutsche Telekom AG

Oznacza Deutsche Telekom AG i wszystkie spółki, w których Deutsche Telekom AG posiada bezpośrednio lub pośrednio udział powyżej 50% lub które są w pełni skonsolidowane.

Spółka Holdingowa Grupy

Spółką Holdingową Grupy jest obecnie Deutsche Telekom AG, z siedzibą przy Friedrich-Ebert-Allee 140, 53113 Bonn, Niemcy.

Dane osobowe

Oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą); osoba możliwa do zidentyfikowania jest to osoba, którą można zidentyfikować, bezpośrednio lub pośrednio, w szczególności poprzez odniesienie do numeru identyfikacyjnego lub jednego lub więcej czynników charakterystycznych dla jej/jego tożsamości fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturalnej lub społecznej.

Odbiorca

Oznacza osobę fizyczną lub prawną, organ władzy publicznej, agencję lub inny organ, któremu ujawniane są dane osobowe, będącą lub niebędącą osobą trzecią. Jednak władze publiczne, które mogą otrzymywać dane w ramach jednego zapytania, nie są uważane za odbiorców.

Szczególne kategorie danych osobowych

Oznaczają dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, religijne lub poglądy filozoficzne, przynależność do związków zawodowych lub informacje dotyczące stanu zdrowia lub życia seksualnego.

Osoba trzecia

Oznacza dowolną osobę lub administratora poza podmiotem odpowiedzialnym. Osoby trzecie nie oznaczają osoby, której dane dotyczą lub osób lub administratorów, którym zlecono zbieranie, przetwarzanie lub wykorzystanie danych osobowych w Niemczech, w innym państwie członkowskim Unii Europejskiej lub w innym państwie będącym stroną umowy o Europejskim Obszarze Gospodarczym.

Wykorzystanie

Oznacza postępowanie z danymi osobowymi, w szczególności zbieranie, przetwarzanie i wykorzystanie takich danych, łącznie z ich przekazywaniem.

Binding Corporate Rules Privacy (BCRP)

Binding corporate rules for the protection of personal rights in the handling of personal data within the Deutsche Telekom Group

Preamble

1. Protecting the personal data of customers, employees and other individuals connected with the Deutsche Telekom Group is a top priority for all companies within the Deutsche Telekom Group.
2. 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.
3. In many areas, the Deutsche Telekom Group is perceived by its customers and the general public 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 innovative services by implementing these Binding Corporate Rules Privacy.
4. In providing these Binding Corporate Rules Privacy, the Deutsche Telekom Group is creating a standardized and high level of data privacy worldwide, applicable to the use of data both within one company and across companies, and to the transfer of data within Germany and internationally. Within the Deutsche Telekom Group, personal data must be processed by the recipient according to the principles of data protection law that apply to the transferring party.

Part One. Scope

§ 1 Legal nature of the Binding Corporate Rules Privacy

The Binding Corporate Rules Privacy shall be binding with regard to the processing of personal data (according to working paper 133, Article 29 of the working group of the European Commission) by all Deutsche Telekom Group companies which have adopted them on a legally binding basis. The Binding Corporate Rules Privacy shall also be binding on all companies that can be required by Deutsche Telekom to adopt them and on all companies that have adopted them on a voluntary basis, regardless of where data is collected.

§ 2 Scope of application

The Binding Corporate Rules Privacy shall apply to all types of personal data use within the Deutsche Telekom Group, regardless of where the data is collected. Personal data shall be used within the Deutsche Telekom Group for the following purposes in particular:

1. To manage employee data when initiating, implementing and processing employment contracts and to address employees with products and services offered to them by the Deutsche Telekom Group or third parties.
2. To initiate, implement and process business-customer and consumer agreements, and to carry out advertising and market-research activities aimed at informing customers and interested third parties about products and services offered by the Deutsche Telekom Group or third parties as appropriate.
3. To initiate and implement agreements with Deutsche Telekom Group service providers as part of the provision of services for the Deutsche Telekom Group.
4. To enable appropriate dealings with other third parties, in particular shareholders, partners or visitors, and to comply with binding legal regulations.

Data shall be used in line with the current and future business purposes of the Deutsche Telekom Group companies, which include the provision of telecommunications services, digital services for consumers and business customers, IT services (including data center services) and advisory services.

§ 3 Relationship to other legal provisions

1. The provisions of the Binding Corporate Rules Privacy are designed to ensure a high and standardized level of data privacy throughout the Deutsche Telekom Group. Existing obligations and regulations which individual companies have to comply with for the processing and use of personal data that go beyond the principles laid out in these Binding Corporate Rules Privacy, or that contains additional restrictions on the processing and use of personal data, shall remain unaffected by these Binding Corporate Rules Privacy.
2. Data collected in Europe shall be used generally in accordance with the legal provisions of the country in which the data was collected, regardless of where the data is used, but at the very least in accordance with the requirements of these Binding Corporate Rules Privacy.
3. The applicability of national legislation decreed for reasons of state security, national defense or public safety, or to prevent and investigate crimes and prosecute criminals, that requires data to be passed on to third parties shall remain unaffected by the provisions of these Binding Corporate Rules Privacy. If a company finds that significant sections of these Binding Corporate Rules Privacy contravene national data privacy provisions, preventing the parties from signing these Binding Corporate Rules Privacy, then the Group Data Privacy Officer of the Deutsche Telekom Group shall be informed without delay. The responsible supervisory authority of the company shall be involved in a mediatory capacity.

§ 4 Expiry and termination

These Binding Corporate Rules Privacy shall cease to be binding on a company if it leaves the Deutsche Telekom Group or invalidates these rules. However, the expiry or invalidation of the Binding Corporate Rules Privacy shall not release the company from the obligations and/or provisions of the Binding Corporate Rules Privacy governing the use of data already transmitted. Further data transfer from or to this company can only take place if other appropriate procedural guarantees are provided in line with the requirements of European law.

Part Two. Principles

Section 1 Transparency of Data Processing

§ 5 Duty to inform

The data subjects shall be informed about how their personal data is used in line with applicable legislation and the following conditions.

§ 6 Content and form of information

1. The company shall inform the data subjects adequately about the following items:
   a) the identity of the data processor(s) and their contact details.
   b) the intended use and purpose of use of the data. This information is to include which data is being recorded and/or processed/used, why, for what purpose and for how long.
   c) If personal data is transferred or transmitted to third parties, the recipient, scope and purpose(s) of such transfer/transmission shall be known.
   d) the rights of the data subjects in connection with the use of their data.
2. Irrespective of the chosen medium, data subjects shall be given this information in a clear and easily understandable manner.

§ 7 Availability of information

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

Section 2. Conditions of admissibility for the use of personal data

§ 8 Principle

Personal data shall only be used under the following conditions and shall not be used for purposes other than those for which it was originally collected.

The use of collected data for other purposes shall only be permitted if the conditions of admissibility have been satisfied in accordance with the following conditions.

§ 9 Admissibility of personal data use

Personal data can be used if one or more of the following criteria have been satisfied:

a) It is clearly legally permissible to use the data in the way intended.

b) The data subject has consented to his/her data being used.

c) It is necessary to use the data in this way in order for the company to fulfill its obligations under an agreement with the data subject, including its contractual duties to inform and/or secondary duties, or in order for the company to implement pre- or post-contractual measures for initiating or processing an agreement that have been requested by the data subject.

d) The data must be used to fulfill a legal obligation of the company.

e) It is necessary to use the data to safeguard the data subject's vital interests.

f) It is necessary to use the data to complete a task that is in the interest of the general public or that forms part of the exercise of public authority and with which the company or third party to whom the data is transferred was charged.

g) It is necessary to process the data in order to realize the legitimate interests of the company or the third party/parties to whom data is being transmitted, provided these interests are not clearly outweighed by interests of the data subject warranting protection.

§ 10 Consent by the data subject

It shall be deemed that the data subject has given his/her consent pursuant to § 9 (1), item b) of these Binding Corporate Rules Privacy if:

a) Consent has been given expressly, voluntarily and on an informed basis that makes the data subject aware of the scope of what he/she is consenting to. 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. For business models in which the withdrawal leads to a non-fulfillment of contractual obligations the data subject shall be informed.

b) Consent has been obtained in a form appropriate to the circumstances (written form). 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.

§ 11 Automated individual decisions

a) 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 data use. This includes in particular decisions for which data about the creditworthiness, professional suitability or state of health of the data subject is significant.

b) 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 The use of personal data for direct marketing purposes

Where data is used for direct marketing purposes, data subjects shall be:

a) informed about the way in which their data will be used for direct marketing purposes;
b) informed about their right to object at any time to the use of their personal data for direct marketing communications, and
c) equipped to exercise their right not to receive such communications. They shall receive, in particular, information about the company to whom the objection should be made.

§ 13 Special categories of personal data

a) The use of special categories of data shall only be permitted where it is governed by legal regulations or where the data subject's consent has been obtained in advance. It shall also be permissible if it is necessary to process the data in order to fulfill the rights and obligations of the company in the area of labor law, provided that suitable protection measures are taken and that this is not prohibited under national law.
b) Prior to the commencement of such collection, processing or use, the company shall inform its Data Privacy Officer accordingly and document this action. When assessing admissibility, particular consideration should be given to the nature, scope, purpose, necessity and legal basis of using the data.

§14 Data minimization, data avoidance, anonymization and aliasing

1. Personal data shall be appropriate, relevant and not excessive with regard to the use of the data for a specific purpose (data minimization). 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 (aliasing).

§15 Prohibition of tying-in

The use of services, or the receipt of products and/or services, shall not be made conditional upon data subjects consenting to the use of their data for purposes other than the initiation or fulfillment of an agreement. 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.

Section 3. Transfer of personal data

§ 16 Nature and purpose of transfer of personal data

1. Personal data can only be transferred where the receiving party assumes responsibility for the data received (transmission) or where the recipient only uses the data in accordance with the instructions and requirements of the transferring party (commissioned data processing agreement).
2. Personal data shall only be transferred for the permitted purposes pursuant to § 9 of these Binding Corporate Rules Privacy as part of the company's business activities or legal obligations, or following consent from the data subjects.

§ 17 Transmission of data

1. If a company transmits data to bodies that are headquartered in a third country or that transfer data across national borders, steps shall be taken to ensure that this data is transmitted properly Appropriate data privacy and data security requirements shall be agreed with the recipient before data is transmitted. In addition, personal data, particularly data collected in the EU or the EEA, shall only be transmitted to controllers outside of the European Union if the appropriate level of data privacy has been ensured using these Binding Corporate Rules Privacy or other appropriate measures, such as the EU standard contractual clauses or individual contractual agreements that meet the relevant requirements of European law.
2. Based on the requirements of the Deutsche Telekom Group and generally recognized technical and organizational standards, appropriate technical and organizational measures shall be taken to guarantee the security of personal data, including during its transmission to another party.

§ 18 Commissioned data processing1

(1 This § is not a provision in the sense of working paper 195 of Art. 29 working group of the European Commisssion)

1. When a company (customer) commissions a third party (contractor) to provide services on its behalf in accordance with its instructions, then, in addition to a service agreement comprising the work to be performed, the agreement shall also refer to the obligations of the contractor as the party commissioned to process the data. These obligations shall set out the instructions of the customer concerning the type and manner of processing of the personal data, the purpose of processing and the technical and organizational measures required for data protection.
2. The contractor shall not use the personal data (entrusted to it for performing the order) for its own or third-party processing purposes without the prior consent of the customer. The contractor shall inform the customer in advance of any plans to sub-contract work out to other third parties in order to fulfill its contractual obligations. The customer shall have the right to object to such use of subcontractors. Where subcontractors are used in the permissible way, the contractor shall obligate them to comply with the requirements of the agreements concluded between the contractor and the customer.
3. Subcontractors shall be selected according to their ability to fulfill the above-stated requirements.

Section 4. Data quality and data security

§ 19 Data quality

1. Personal data shall be correct and, where necessary, kept up to date (data quality).
2. In light of the purpose for which the data is being used, appropriate measures shall be taken to ensure that any incorrect or incomplete information is erased, blocked or, if necessary, corrected.

§ 20 Data security – technical and organizational measures

The company shall take appropriate technical and organizational measures for company processes, IT systems and platforms used to collect, process or employ data in order to protect this data.

Such measures shall include:

a) preventing unauthorized persons from gaining access to data processing systems on which personal data is processed or used (admittance 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 the 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 its transport or recording on data media, personal data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to check and identify the controllers to which personal data is 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 has been entered into data processing systems, altered or removed (data entry control);
f) ensuring that outsourced personal data can only be processed in accordance with the instructions of the customer (contractor control);
g) ensuring that personal data is protected against accidental destruction or loss (availability control);
h) ensuring that data which has been collected for different purposes can be processed separately (separation rule).

Part Three. Rights of Data Subjects

§ 21 Right to information

1. Data subjects shall be entitled at any time to contact any company using their data and request the following information:
   a) the personal data held on them, including its origin and recipient(s);
   b) the purpose of use;
   c) the persons and controllers to whom/which their data is regularly transmitted, particularly if the data is transmitted abroad;
   d) the provisions of these Binding Corporate Rules Privacy.
2. The relevant information is to be made available to the enquirer in an understandable form within a reasonable period of time. This is generally done in writing or electronically. Providing a hard copy of these Binding Corporate Rules Privacy shall suffice as a means of communicating information about their requirements.

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

§ 22 Right of protest, right to have data erased or blocked, and right to correction

1. Data subjects can object to the use of their data at any time if this data is being used for purposes that are not legally binding.
2. This right of protest shall also apply in the event that data subjects had previously consented to the use of their data.
3. Legitimate requests to have data erased or blocked shall be promptly met. Such requests are legitimate 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 unreasonable, the data shall be protected against non-permitted usage by blocking. Statutory retention periods shall be observed.
4. Data subjects can request from the company to correct the personal data it holds on them at any time if this data is incomplete and/or incorrect.
5. For business models in which the withdrawal or the erasure leads to a non-fulfillment of contractual obligations the data subject shall be informed.

§ 23 Right to clarification, comments and remediation

1. If a data subject claims that his/her rights have been violated by unlawful use of his/her data, particularly by providing evidence of a verifiable violation of these Binding Corporate Rules Privacy, the responsible companies shall clarify the facts without deliberate delay. For data transferred or transmitted to companies outside of the European Union in particular, the company based in the European Union shall clarify the facts and provide evidence that the receiving party has not violated the requirements of these Binding Corporate Rules on Data Privacy or is responsible for any damage caused. The companies shall work together closely to clarify the facts and shall grant each other access to all information they require to do so.
2. The data subject concerned can file a complaint against the Deutsche Telekom Group Holding at any time if he/she suspects that a Deutsche Telekom Group company is not processing his/her personal data in accordance with legal requirements or with the provisions of these Binding Corporate Rules Privacy. The substantiated complaint shall be dealt with within an appropriate period of time and the data subject informed accordingly.
3. If a complaint concerns several companies, the Data Privacy Officer of the company most familiar with the subject matter shall coordinate all relevant correspondence with the data subject. The Group Data Privacy Officer shall be entitled to exercise his/her right of subrogation and takeover at any time.
4. There shall be suitable channels in place for reporting data privacy incidents (such as a special purpose e-mail account provided by Data Privacy, Legal Affairs and Compliance or a direct contact who can be contacted online).
5. The Data Privacy Officer of the company concerned shall inform the Group Data Privacy Officer of a data privacy incident without delay using the relevant reporting processes.
6. Data subjects can make a claim pursuant to Part Five of these Binding Corporate Rules Privacy if their rights have been infringed or if they have suffered any loss.

§ 24 Right to question and complain

Every data subject has the right at any time to contact the Data Privacy Officer of the company using his/her personal data with questions and complaints regarding the application of these Binding Corporate Rules Privacy. The company most familiar with the subject matter or the company that collected the data subject's data shall make sure that the data subject's rights are properly observed by the other responsible companies.

§ 25 Exercising of rights of data subjects

Data subjects shall not be disadvantaged because they have made use 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.

§ 26 Hard copy of the Binding Corporate Rules Privacy

A hard copy of these Binding Corporate Rules Privacy shall be provided to anyone upon request.

Part Four. Data Privacy Organization

§ 27 Responsibility for data processing

The companies shall be obligated to ensure compliance with the legal provisions on data protection and with these Binding Corporate Rules Privacy.

§ 28 Data Privacy Officer

1. Each company shall appoint an independent Data Privacy Officer , whose task is to ensure that the individual organizational units of that company are advised on the statutory and internal company/Group requirements for data privacy and, in particular, on these Binding Corporate Rules Privacy. The Data Privacy Officer shall use suitable measures, in particular random inspections, to monitor compliance with data protection regulations.
2. The company shall consult with the Group Data Privacy Officer before appointing a Data Privacy Officer.
3. The company shall ensure that the Data Privacy Officer possesses the relevant expertise for evaluating the legal, technical and organizational aspects of data privacy measures.
4. The company shall provide the Data Privacy Officer with the financial and personnel resources necessary for carrying out his/her duties
5. The Data Privacy Officer shall be granted the right to report directly to company management, and shall be connected organizationally to company management.
6. The Data Privacy Officer of each company shall be responsible for implementing the requirements of the Group Data Privacy Officer and of the Deutsche Telekom Group's data privacy strategy.
7. All departments of each company shall be obligated to inform their company's Data Privacy Officer of any developments in IT infrastructure, network infrastructure, business models, products, staff data processing and corresponding strategic plans. The Data Privacy Officer shall be brought in on new developments at an early stage in order to ensure that any data privacy matters can be considered and evaluated.

§ 29 Group Data Privacy Officer

1. The Group Data Privacy Officer shall coordinate the processes of cooperation and agreement on all significant issues regarding data privacy within the Deutsche Telekom Group. He shall inform the CEO of the Deutsche Telekom Group Holding about current developments and draft recommendations where necessary.
2. It shall be the duty of the Group Data Privacy Officer to develop and evolve the Deutsche Telekom Group's policy on data privacy, consulting with the Data Privacy Officers of the Group companies where appropriate. These Data Privacy Officers shall develop the data privacy policy for their company in line with the Group data privacy policy. The Group Data Privacy Officer and the Data Privacy Officers from the national companies shall meet annually to share information at the International Privacy Leader Meetings (face-to-face events).

§ 30 Duty to inform in case of infringements

The company concerned shall inform its Data Privacy Officer immediately of any infringement or clear indication of infringement of data protection regulations in particular of these Binding Corporate Rules Privacy. The Data Privacy Officer shall in turn inform the Group Data Privacy Officer immediately if the incident has a potential impact on the public,

affects more than one company, or entails a potential loss of over EUR 500,000. The company's Data Privacy Officer shall also inform the Group Data Privacy Officer if any changes are made to the laws applying to a company that are significantly unfavorable to compliance with these Binding Corporate Rules Privacy.

§ 31 Review of the level of data privacy

1. Reviews to find out about the compliance with the requirements of these Binding Corporate Rules Privacy and the level of data privacy derived there from shall be carried out by the Group Data Privacy Officer as part of an annual inspection plan as well as by other measures such as inspections carried out by the Data Privacy Officers of the companies and reporting.
2. Internal and external auditors shall carry out the inspections of the Group Data Privacy Officer. Regular self-assessments shall also be carried out within the Deutsche Telekom Group, coordinated by the Group Data Privacy Officer. The CEO of the Deutsche Telekom Group Holding shall be informed of the results of key inspections and the subsequently agreed measures. The responsible data supervisory authority shall be sent a copy of the inspection results upon request. The supervisory authority responsible for the company can also initiate an inspection. The company shall provide as much support as possible for these inspections and shall implement the measures derived there from.
3. The company shall take relevant measures to remedy any weaknesses identified during an inspection, and the Group Data Privacy Officer shall monitor the implementation of these measures. If the company fails to implement the measures without sufficient reasons, the Group Data Privacy Officer shall assess the impact on data privacy and take the necessary action, escalating the matter where necessary.
4. The Data Privacy Officers of the companies or other organizational units commissioned to conduct inspections shall also carry out checks based on dedicated audit plans documented in writing to determine whether the companies are complying with data protection requirements.
5. In the absence of legal restraints, the Group Data Privacy Officer and the Data Privacy Officers shall be authorized to check, at all companies and at their own company respectively, whether personal data is being used properly. The companies concerned shall grant the Group Data Privacy Officer and the Data Privacy Officers full access to the information they require to clarify and evaluate a situation. The Group Data Privacy Officer and the Data Privacy Officers shall be entitled to issue instructions in this regard.
6. As part of their inspections, the Data Privacy Officers of the companies shall use standardized procedures valid for the entire Group, e.g. common data protection audits, wherever possible. Such procedures can be made available by the Group Data Privacy Officer.

§ 32 Employee commitment and training

1. The companies shall obligate their employees to maintain the data and telecommunications secrecy upon commencing their employment at the latest. Employees shall receive sufficient training in data privacy matters as part of this commitment. The company shall initiate suitable processes and provide resources to this end.
2. Employees shall receive training in the basics of data privacy regularly, or at least every two years. The companies shall be entitled to develop and run dedicated training courses for their own employees. The Data Privacy Officer of each company shall document the delivery of these training courses and inform the Group Data Privacy Officer on an annual basis.
3. The Group Data Privacy Officer can make resources and processes available centrally for obligating and training Deutsche Telekom Group employees.

§ 33 Cooperation with supervisory authorities

1. The companies shall agree to work together on the basis of trust with the supervisory authority responsible for them or for the company transmitting data, in particular, to respond to queries and follow recommendations.
2. In the event of a change in the legislation applicable to a company which might have substantial adverse effects on the guarantees provided by these Binding Corporate Rules Privacy, the company concerned shall notify the responsible supervisory authority of the change.

§ 34 Responsible contacts for queries

The Data Privacy Officers of the companies or the Group Data Privacy Officer are the contacts responsible for dealing with queries about these Binding Corporate Rules Privacy. The Group Data Privacy Officer shall provide the contact details for the Data Privacy Officers of the companies upon request.

Part Five. Liability

§ 35 Area of application of the rules on liability

1. This Part Five of The Binding Corporate Rules shall apply exclusively for the processing of personal data collected in the EU / the EEA, which falls within the scope of the EU Directive on Data Protection 95/46/EC.
2. Within the EU/EEA, the legal liability provisions of the country in which a company is headquartered shall apply. For data that is not subject to § 35, Section 1 of the BCRP the legal liability provisions of the country in which the respective company that collected the data has its registered office, or if there are no legal provisions existing, the terms and conditions of the company that collected the data shall apply.
3. Payment of exemplary damages, where a company must make payments to a data subject that exceed the damage itself, shall be explicitly ruled out.

§ 36 Indemnitor

1. Any individual who has suffered loss as a result of one or more of the duties specified in the Binding Corporate Rules Privacy being violated by a Deutsche Telekom Group company or by data recipients to which a Deutsche Telekom Group company has transferred or transmitted data, shall be entitled to claim corresponding damages against the Deutsche Telekom Group companies concerned.
2. The data subject shall also be entitled to claim damages against the Deutsche Telekom Group holding company. If the holding company pays damages, it shall be entitled to claim reimbursement from the companies that are responsible for the loss or that commissioned a third party which caused it.

The data subject shall claim damages initially against the company that transferred or transmitted the data. If the transferring company is not liable de jure or de facto, the data subject shall be entitled to claim damages from the

recipient company. The recipient company shall not be entitled to withdraw from liability by appealing to the responsibility of a contractor in case of violation.

(4) The data subject shall be entitled to submit a complaint to the responsible supervisory authority or to the supervisory authority responsible for the Deutsche Telekom Group holding company at any time.

§ 37 Burden of proof

The burden of proof for the proper use of the data subject's data shall rest with the liable companies.

§ 38 Third-party benefits for data subjects

If the data subject has no direct rights, he/she shall be entitled, as a third-party beneficiary, to assert claims against companies which have violated their contractual duties, based on the provisions of these Binding Corporate Rules Privacy.

§ 39 Place of jurisdiction

At the individual's discretion, the place of jurisdiction to assert liability claims may be:

a) applicable to the individual concerned or

b) within the jurisdiction of the member of the group at the origin of the transfer or

c) the EU headquarters or the European member of the group with delegated data protection responsibilities.

§ 40 Out-of-court arbitration

1. Third parties who consider their individual right to privacy to have been violated as a result of actual or suspected use of their personal data shall be entitled to request that the Data Privacy Officer of the company concerned arbitrate in the matter. The Data Privacy Officer shall be entitled to examine the complaint and advise the data subject on his/her rights. In doing so, the Data Privacy Officer shall be obligated to maintain the confidentiality of other personal data of the complainant unless the complainant releases the Data Privacy Officer from such obligation. At the request of the individual concerned, an attempt shall be made to reach an agreement regarding the complaint, with the involvement of the data subject and the Data Privacy Officer. Such an agreement may also include a recommendation regarding compensation for any loss suffered as a result of the data subject's right to privacy being violated. This recommendation shall be binding on the companies concerned if it is approved by mutual consent.
2. The right to submit a complaint to the responsible supervisory authority or to take legal action shall remain unaffected.

Part Six. Final Provisions

§ 41 Reviewing and amending these Binding Corporate Rules Privacy

1. The Group Data Privacy Officer shall examine the Binding Corporate Rules Privacy at regular intervals, but at least once a year, to find out about their compliance with applicable legislation, and shall make any necessary adjustments.

2. Any significant amendments to these Binding Corporate Rules Privacy that become e.g. necessary as a result of adjustments made to bring them in line with legal requirements shall be agreed with the supervisory authority. These amendments shall apply directly to all companies that have signed the Binding Corporate Rules Privacy following an appropriate transition period.
3. The Group Data Privacy Officer shall inform all companies that have introduced the Binding Corporate Rules Privacy of the amended content.
4. The Data Privacy Officers of the companies shall be obligated to examine whether amendments to these Binding Corporate Rules Privacy have any implications for legal compliance in their own country or whether they conflict with the legal provisions in their respective country. If the company is unable to implement the amendments for binding legal reasons, it shall inform the Group Data Privacy Officer and the responsible supervisory authority immediately and, if relevant, these Binding Corporate Rules Privacy shall be suspended temporarily for this company.

§ 42 List of contacts and companies

The Group Data Privacy Officer shall keep a list of companies that have introduced these Binding Corporate Rules Privacy and the contacts for these companies. He shall keep this list up to date and inform data subjects and data protection authority upon request.

§ 43 Procedural law / severability clause

These Binding Corporate Rules Privacy shall be subject to the procedural law of the Federal Republic of Germany in the case of disputes.

If individual provisions of these Binding Corporate Rules Privacy are or become void, they shall be deemed to have been replaced by the provisions that most closely approximate the original intentions of these Binding Corporate Rules Privacy and the void provisions. In case of doubt, the applicable data protection regulations of the European Union shall apply in these cases or in the absence of relevant provisions.

§ 44 Publication

The companies shall make information about the rights of data subjects and the third-party benefit clause available to the public in a suitable format, such as in the notes on data protection on the Internet. This information shall be published as soon as these Binding Corporate Rules Privacy have become binding on a company.

Part Seven. Definitions and Terms

Aliasing

Shall mean the replacement of a person's name and other identification features with another characteristic in order to prevent the data subject being identified or make it considerably harder to identify the data subject.

Anonymization

Anonymization shall mean the process of changing information in such a manner that personal details and other facts can no longer be traced back to an identified or identifiable natural person or can no longer be traced back to such a person without a disproportionately large amount of effort in terms of time, cost and energy.

Automated individual decisions

Shall mean decisions which have legal implications for the data subject or which have a significant adverse effect on him/her and which are based solely on automated processing of data intended to evaluate certain personal aspects of the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc.

Company

Shall mean any company that is subject to these Binding Corporate Rules Privacy. A separate list of these companies is kept for reference purposes and updated on an ongoing basis. The list can be viewed by anyone at any time.

Controller

Shall mean any body that processes personal data, but is not necessarily a legal person.

Data subject

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

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 which are fully consolidated.

Group Holding

The Group Holding is currently Deutsche Telekom AG, headquartered on Friedrich-Ebert-Allee 140, 53113 Bonn, Germany.

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/her physical, physiological, mental, economic, cultural or social identity.

Recipient

Shall mean any natural or legal person, public authority, agency or any other body to whom personal data is 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 personal 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 controller outside the body in charge. Third parties shall not mean the data subject or persons or controllers who are commissioned to collect, process or use personal data in Germany, in another member state of the European Union or in another state party to the agreement on the European Economic Area.

Use

Shall mean any handling of personal data, particularly collection, processing and use, including transfer, of such data.