

Wiążące Reguły Korporacyjne dotyczące Prywatności (BCRP)

Wiążące Reguły Korporacyjne dotyczące ochrony praw przysługujących osobom fizycznym podczas przetwarzania danych osobowych w Grupie Deutsche Telekom

Wersja 3.0 – wersja ostateczna
29.12.2023

Publiczne



Informacje o publikacji

Opublikowane przez

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

Nazwa pliku	Numer dokumentu	Nazwa dokumentu
[Binding Corporate Rules Privacy DTAG.docx]	[2,9]	[Wiążące Reguły Korporacyjne dotyczące Prywatności]

Wersja	Data ostatniej zmiany	Stan
3.0 ostateczna	29.12.2023	

Autor	Weryfikacja treści	Zatwierdził
Dr Jörg Friedrichs Bonn, 27.10.2023	Jan Lichtenberg, Strategy and Steering [Bonn, 30.10.2023]	Dr Claus-Dieter Ulmer, Group Privacy Officer [Bonn, 31.10.2023]

Krótkie streszczenie

Regulacja dotycząca postępowania z danymi osobowymi w Grupie Deutsche Telekom AG

Historia zmian

Wersja	Data ostatniej zmiany	Opracował/-a	Zmiany/uwagi
2.2	20.01.2013	Sonja Klauck	Zmieniona wersja Privacy Code of Conduct, Niemcy, wersja 2.1
2.3	08.02.2013	Dr Claus-Dieter Ulmer	Ujednolicenie całego dokumentu
2.4	14.02.2013	Dr Claus-Dieter Ulmer	Transfer danych i odpowiedzialność
2.5	21.03.2013	Marcus Schmitz Dr Claus-Dieter Ulmer	Zmiany uwzględniające uwagi niemieckiego Federalnego Komisarza ds. Ochrony Danych i Swobody Informacji
2.6	09.04.2013	Daniel Hoff	Zmiany uwzględniające uwagi niemieckiego Federalnego Komisarza ds. Ochrony Danych i Swobody Informacji
2.7	05.12.2013	Daniel Hoff Marcus Schmitz	Zmiany uwzględniające uwagi austriackiego Urzędu Ochrony Danych
2.8	19.02.2019	Dr. Jörg Friedrichs Christina Kreft-Spallek	Dostosowanie do Ogólnego Rozporządzenia o Ochronie Danych (RODO) na podstawie WP 256, wer. 01
3.0	29.12.2023	Dr Jörg Friedrichs	Dostosowanie do Zaleceń nr 1/2022 w sprawie wniosku o zatwierdzenie oraz elementów i zasad zawartych w Wiążących Regułach Korporacyjnych administratora danych (art. 47 RODO)



Connecting
your world.

Spis treści

Preambuła	6
Część pierwsza: Zakres	7
§ 1 Charakter prawny Wiążących Reguł dot. Prywatności.....	7
§ 2 Zakres zastosowania	7
§ 3 Powiązania z innymi przepisami prawa	7
§ 4 Wygaśnięcie i rozwiązanie	8
Część druga: Zasady	9
Sekcja 1 Przejrzystość przetwarzania danych	9
§ 4 Obowiązek informowania.....	9
§ 5 Treść i forma informacji	9
§ 6 Dostępność informacji	9
§ 8 Rejestr wszystkich kategorii czynności przetwarzania	9
Sekcja 2 Warunki dopuszczalności przetwarzania danych osobowych	10
§ 9 Zasada	10
§ 10 Zgodność przetwarzania danych osobowych z prawem	10
§ 11 Zgoda osoby, której dane dotyczą	10
§ 12 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie	10
§ 13 Przetwarzanie danych osobowych do celów marketingu bezpośredniego	11
§ 14 Szczególne kategorie danych osobowych.....	11
§ 15 Minimalizacja danych, ograniczenie celu, ograniczenie przechowywania, anonimizacja i pseudonimizacja.....	11
§ 16 Przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych	11
§ 17 Zakaz uzależniania świadczenia usług od udzielenia zgody.....	11
Sekcja 3 Przekazywanie danych osobowych	12
§ 18 Charakter i cel przekazywania danych osobowych.....	12
§ 19 Transfer danych, w tym dalszy transfer danych.....	12
§ 20 Obowiązki odbiorcy w przypadku dostępu władz publicznych do danych	12
§ 21 Przetwarzanie danych w imieniu administratora danych.....	13
Sekcja 4 Jakość danych i bezpieczeństwo danych.....	15

§ 22 Prawidłowość danych	15
§ 23 Bezpieczeństwo danych – środki techniczne i organizacyjne – ochrona danych już w fazie projektowania i domyślna ochrona danych	15
Część trzecia: Prawa osób, których dane dotyczą.....	16
§ 24 Prawo dostępu	16
§ 25 Prawo sprzeciwu, prawo do usunięcia danych lub ograniczenia przetwarzania oraz prawo do sprostowania danych	16
§ 26 Prawo do wyjaśnienia, zgłoszenia uwag i podjęcia działań naprawczych.....	16
§ 27 Prawo do zadawania pytań i zgłaszania skarg	17
§ 28 Wykonywanie praw osób, których dane dotyczą	17
§ 29 Dostęp do Wiążących Reguł Korporacyjnych dotyczących Prywatności	17
Część czwarta: Organizacja ochrony danych	18
§ 30 Odpowiedzialność za przetwarzanie danych.....	18
§ 31 Inspektor Ochrony Danych.....	18
§ 32 Inspektor Ochrony Danych Grupy	18
§ 33 Obowiązek informowania w przypadku naruszeń lub zmiany przepisów i praktyk mających zastosowanie do spółki	19
§ 34 Przegląd poziomu prywatności danych	19
§ 35 Ocena skutków dla ochrony danych.....	20
§ 36 Zaangażowanie i szkolenia pracowników	20
§ 37 Współpraca z organami nadzoru.....	20
§ 38 Odpowiedzialna osoba kontaktowa ds. pytań.....	20
Część piąta: Odpowiedzialność.....	21
§ 39 Obszar zastosowania zasad dotyczących odpowiedzialności	21
§ 40 Zwolnienia z odpowiedzialności.....	21
§ 41 Ciężar dowodu	21
§ 42 Korzyści osoby trzeciej dla osób, których dane dotyczą	21
§ 43 Miejsce jurysdykcji.....	21
§ 44 Rozstrzygnięcie pozasądowe	22
Część szósta: Postanowienia końcowe	23
§ 45 Przegląd i zmiany do niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności	23
§ 46 Wykaz danych kontaktowych i spółek	23
§ 47 Prawo procesowe/klauzula salwatoryjna.....	23
§ 48 Publikacja	23

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 uzależniony jest 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 spółki i wspierania deklaracji głoszącej, że Grupa Deutsche Telekom jest dostawcą wysokiej jakości produktów i innowacyjnych usług poprzez wdrożenie niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
- (4) Wdrażając niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności, Grupa Deutsche Telekom ustanawia jednolity i wysoki poziom prywatności danych w skali globalnej, mający zastosowanie do przetwarzania danych zarówno w jednej spółce, jak i pomiędzy spółkami, a także do przekazywania danych w Niemczech i w skali międzynarodowej. Spółki z Grupy Deutsche Telekom będące odbiorcami danych mają obowiązek przetwarzać dane osobowe zgodnie z zasadami określonymi przez przepisy dotyczące ochrony danych, które mają zastosowanie do strony przekazującej.

Uwaga:

Nawet jeśli niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności zostaną wdrożone w spółkach na indywidualnych zasadach, to i tak muszą być przestrzegane wszystkie istniejące układy zbiorowe i prawa uczestnictwa odpowiedniego organu reprezentującego pracowników.

Część pierwsza: Zakres

§ 1 Charakter prawny Wiążących Reguł Korporacyjnych dotyczących Prywatności

Wiążące Reguły Korporacyjne dotyczące Prywatności będą obowiązywać w zakresie przetwarzania danych osobowych (zgodnie z Zaleceniami nr 1/2022 Europejskiej Rady Ochrony Danych) przez wszystkie spółki Grupy Deutsche Telekom, które przyjęły je do stosowania jako prawnie wiążące.

§ 2 Zakres zastosowania

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

- a) Do zarządzania danymi pracowników podczas inicjowania, realizacji i wykonywania umów o pracę oraz do przedstawiania pracownikom produktów i usług oferowanych im przez Grupę Deutsche Telekom lub strony trzecie.
- b) Do inicjowania, realizacji i wykonywania 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 strony trzecie.
- c) Do inicjowania i realizacji umów z usługodawcami Grupy Deutsche Telekom w ramach świadczenia usług na rzecz Grupy Deutsche Telekom.
- d) W celu umożliwienia utrzymywania odpowiednich relacji z innymi stronami trzecimi, w szczególności z udziałowcami, partnerami lub odwiedzającymi oraz w celu przestrzegania obowiązujących przepisów prawnych.

Dane przetwarzane 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 prawne, które powinny być przestrzegane przez poszczególne spółki w zakresie przetwarzania danych osobowych, wykraczające poza zasady zawarte w niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności lub zawierające dodatkowe ograniczenia w zakresie przetwarzania danych osobowych.
- (2) Dane zbierane w Europejskim Obszarze Gospodarczym są przetwarzane zasadniczo zgodnie z przepisami prawa kraju, w którym dane zostały zebrane, niezależnie od miejsca przetwarzania 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.
- (4) Jeżeli spółka stwierdzi, że istotne fragmenty niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności są sprzeczne z krajowymi przepisami dotyczącymi ochrony danych, uniemożliwiają stronom przestrzeganie niniejszych Wiążących Reguł Korporacyjnych dotyczących

Prywatności, Inspektor Ochrony Danych w Grupie Deutsche Telekom zostanie o tym niezwłocznie poinformowany. Organ nadzoru właściwy dla spółki powinien pełnić 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 przetwarzanie danych, które zostały już przekazane. Dalsze przekazanie danych przez tę spółkę lub do tej spółki może nastąpić wyłącznie pod warunkiem zapewnienia innych odpowiednich zabezpieczeń, zgodnie z wymaganiami prawa europejskiego.

Część druga: Zasady

Sekcja 1

Przejrzystość przetwarzania danych

§ 5 Obowiązek informowania

Osoby, których dane dotyczą są informowane o sposobie przetwarzania ich danych osobowych zgodnie z obowiązującymi przepisami i określonymi poniżej warunkami.

§ 6 Treść i forma informacji

- (1) Spółka informuje w odpowiedni sposób osoby, których dane dotyczą o następujących sprawach:
 - a) tożsamość administratora/administratorów danych i ich dane kontaktowe;
 - b) dane kontaktowe inspektora ochrony danych;
 - c) cele przetwarzania danych, jak również podstawa prawna przetwarzania oraz okres ich przetwarzania w tym okres, przez który dane osobowe będą przechowywane;
 - d) jeżeli dane osobowe są przekazywane do podmiotów trzecich, powinny być znane takie szczegóły jak odbiorca, zakres i cel(e) przekazywania;
 - e) prawa osób, których dane dotyczą w związku z przetwarzaniem 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.

§ 8 Rejestr wszystkich kategorii czynności przetwarzania

Spółki prowadzą rejestr wszystkich kategorii prowadzonych czynności przetwarzania. Rejestr zawiera następujące informacje:

- a) nazwa spółki oraz dane kontaktowe jej przedstawiciela, a także Inspektora Ochrony Danych;
- b) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych oraz cele przetwarzania;
- c) kategorie odbiorców, którym dane osobowe zostały lub zostaną przekazane lub ujawnione, w tym odbiorców w państwach trzecich;
- d) nazwy państw trzecich oraz dokumentacja odpowiednich zabezpieczeń, jeżeli niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności nie mają zastosowania;
- e) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- f) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Sekcja 2

Warunki dopuszczalności przetwarzania danych osobowych

§ 9 Zasada

- (1) Dane osobowe są przetwarzane wyłącznie po spełnieniu następujących warunków i są przetwarzane wyłącznie zgodnie z celami, do których zostały pierwotnie zebrane.
- (2) Przetwarzanie zebranych danych do innych celów jest dozwolone wyłącznie, jeżeli spełnione zostały wymogi dopuszczalności, zgodne z następującymi warunkami (ograniczenie celu).

§ 10 Zgodność przetwarzania danych osobowych z prawem

Dane osobowe mogą być przetwarzane, jeżeli spełniony jest co najmniej jeden lub więcej z poniższych warunków:

- a) przetwarzanie danych w planowany sposób jest wyraźnie dopuszczone przez prawo;
- b) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- c) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- d) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na spółce;
- e) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- f) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- g) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

§ 11 Zgoda osoby, której dane dotyczą

Przyjmuje się, że osoba, której dane dotyczą udzieliła zgody na podstawie § 10 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 dokumentowej). W wyjątkowych przypadkach może zostać uzyskana ustnie, jeżeli fakt wyrażenia zgody i szczególne okoliczności uzasadniające ustną zgodę są odpowiednio udokumentowane.

§ 12 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

- (1) Decyzje oceniające indywidualne aspekty dotyczące danej osoby (profilowanie) 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 zautomatyzowanym przetwarzaniu danych. Obejmuje to w

szczególności decyzje, dla których istotne są dane dotyczące wiarygodności kredytowej, predyspozycji zawodowych lub stanu zdrowia osoby, której dane dotyczą.

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

§ 13 Przetwarzanie 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 przetworzone do celów marketingu bezpośredniego;
- b) są informowane o przysługującym im prawie do wyrażenia sprzeciwu wobec przetwarzania 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.

§ 14 Szczególne kategorie danych osobowych

- (1) Przetwarzanie szczególnych kategorii danych jest dopuszczalne wyłącznie, jeżeli jest wprost uregulowane w przepisach lub jeżeli uzyskano uprzednio wyraźną zgodę osoby, której dane dotyczą. Przetwarzanie tego rodzaju danych jest również dopuszczalne, jeżeli jest ono 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.
- (2) Przed rozpoczęciem przetwarzania szczególnych kategorii danych osobowych spółka poinformuje swojego Inspektora Ochrony Danych i udokumentuje takie działania. Podczas oceny dopuszczalności należy zwrócić szczególną uwagę na charakter, zakres, cel, konieczność i podstawę prawną przetwarzania danych.

§ 15 Minimalizacja danych, ograniczenie celu, ograniczenie przechowywania, anonimizacja i pseudonimizacja

- (1) Dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych). zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, wyłącznie jeżeli jest to niezbędne (ograniczenie celu). Muszą być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (ograniczenie przechowywania).
- (2) Jeżeli jest to możliwe i uzasadnione z ekonomicznego punktu widzenia, należy stosować procedury usuwania cech identyfikujących osoby, których dane dotyczą (anonimizacja) lub zastępować cechy identyfikujące innymi charakterystykami (pseudonimizacja).

§ 16 Przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych

Przetwarzanie danych osobowych zebranych w Europejskim Obszarze Gospodarczym w związku z wyrokami skazującymi i czynami zabronionymi lub powiązanymi środkami bezpieczeństwa na podstawie § 10 BCRP odbywa się wyłącznie pod nadzorem władz publicznych lub gdy przetwarzanie jest dozwolone na mocy prawa Unii lub prawa państwa członkowskiego przewidującego odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących prowadzone są wyłącznie pod nadzorem władz publicznych.

§ 17 Zakaz uzależnienia świadczenia usług od udzielenia zgody

Możliwość korzystania z usług lub otrzymania produktów i/lub usług nie powinna być uzależniona od wyrażenia przez osoby, których dane dotyczą zgody na przetwarzanie ich danych do innych celów niż zawarcie lub wykonanie umowy. Powyższe postanowienie będzie miało zastosowanie wyłącznie w przypadku, gdy osoba której dane dotyczą, nie będzie miała możliwości, w granicach rozsądku, skorzystania z porównywalnych usług lub porównywalnych produktów.

Sekcja 3

Przekazywanie danych osobowych

§ 18 Charakter i cel przekazywania danych osobowych

- (1) Dane osobowe mogą być przekazywane, gdy odbiorca samodzielnie określa cele i sposoby przetwarzania danych, albo gdy odbiorca przetwarza dane wyłącznie w imieniu administratora danych.
- (2) Dane osobowe mogą być przekazywane wyłącznie w dozwolonych celach, zgodnie z § 10 niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności w ramach działalności gospodarczej spółki lub obowiązków prawnych, lub po uzyskaniu zgody osób, których dane dotyczą.
- (3) Dane osobowe mogą być przekazywane tylko wtedy, gdy przed przekazaniem danych z odbiorcą uzgodniono odpowiednie środki w zakresie ochrony danych i bezpieczeństwa danych.

§ 19 Transfer danych, w tym dalszy transfer danych

- (1) Dane osobowe zebrane na terenie Europejskiego Obszaru Gospodarczego są przekazywane administratorom danych lub podmiotom przetwarzającym w państwie trzecim wyłącznie, jeżeli zapewniono odpowiedni poziom ochrony danych przy użyciu niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności lub innych odpowiednich zabezpieczeń, takich jak standardowe klauzule umowne UE lub indywidualne umowy spełniające odpowiednie wymogi prawa europejskiego oraz, gdy zapewniono egzekwowalne prawa osób, których dane dotyczą, oraz skuteczne środki prawne przysługujące osobom, których dane dotyczą, w rozumieniu części 5 niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
- (2) Obejmuje to postanowienie, że niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności będą wykorzystywane jako narzędzie transferu danych po dokonaniu oceny skutków transferu (transfer impact assessment) wyłącznie w przypadku, gdy spółka oceni, że przepisy i praktyki obowiązujące w państwie trzecim przeznaczenia, mające zastosowanie do przetwarzania danych osobowych przez odbiorcę, nie uniemożliwiają odbiorcy wypełnienia jego zobowiązań wynikających z niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Przegląd ten uwzględnia również wszelkie wymogi dotyczące ujawniania danych osobowych lub środków zezwalających organom władzy publicznej na dostęp do nich. Dotyczy to wszystkich danych osobowych przekazywanych spółkom spoza Europejskiego Obszaru Gospodarczego, a następnie przekazywanych przez spółki z państw trzecich spółkom z tego samego lub z innego państwa trzeciego.
- (3) Spółka przekazująca (transferująca) dane osobowe zawiesza transfer danych, jeżeli uzna, że nie można zastosować się do Wiążących Reguł Korporacyjnych dot. Prywatności lub jeżeli otrzyma stosowne polecenie właściwego organu nadzoru. Spółka musi zakończyć transferowanie danych lub zestaw operacji transferu, jeżeli zgodnie z Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności nie zostanie przywrócona w ciągu jednego miesiąca od zawieszenia transferu danych. W takim przypadku dane osobowe, które zostały przekazane przed zawieszeniem transferu, a także wszelkie ich kopie, powinny, zgodnie z wyborem spółki transferującej dane osobowe, zostać jej zwrócone lub zniszczone w całości.
- (4) Na podstawie wymagań Grupy Deutsche Telekom i powszechnie uznanych standardów dotyczących technicznych i organizacyjnych środków bezpieczeństwa wdrażane są odpowiednie środki techniczne i organizacyjne w celu zagwarantowania bezpieczeństwa danych osobowych, w tym podczas ich przekazywania (transferu) do innej strony.

§ 20 Obowiązki odbiorcy w przypadku dostępu władz publicznych do danych

- (1) Odbiorca zobowiązuje się niezwłocznie powiadomić spółkę transferującą dane osobowe, jeżeli:
 - a) otrzyma od organu władz publicznych, w tym organów sądowych, zgodny z prawem kraju przeznaczenia, prawnie wiążący wniosek o ujawnienie danych osobowych przekazywanych

na podstawie Wiążących Reguł Korporacyjnych dotyczących Prywatności; powiadomienie takie zawiera informacje o żądanych danych osobowych, organie wnioskującym, podstawie prawnej wniosku i udzielonej odpowiedzi; lub

- b) dowie się o jakimkolwiek bezpośrednim dostępie władz publicznych do danych osobowych transferowanych zgodnie z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności zgodnie z prawem kraju przeznaczenia; powiadomienie takie zawiera wszystkie informacje dostępne odbiorcy.
- (2) W przypadku zakazu zawiadamiania spółki transferującej dane osobowe przez odbiorcę wynikającego z prawa kraju przeznaczenia, odbiorca zobowiązuje się dołożyć wszelkich starań, aby uzyskać zwolnienie z zakazu, w celu jak najszybszego przekazania możliwie największej ilości informacji. Odbiorca zobowiązuje się udokumentować dołożenie wszelkich starań i udowodnienia tego na żądanie spółki transferującej dane osobowe.
 - (3) Jeżeli zezwala na to prawo kraju przeznaczenia, odbiorca zgadza się dostarczać spółce transferującej dane osobowe, w regularnych odstępach czasu przez okres obowiązywania umowy, jak najwięcej istotnych informacji na temat otrzymanych wniosków (w szczególności o liczbie wniosków, rodzaju wnioskowanych danych, organie lub organach wnioskujących, czy wobec wniosku wniesiono sprzeciw oraz o wyniku takiego sprzeciwu itp.).
 - (4) Odbiorca zgadza się zachować informacje zgodnie z ust. 1-3 przez okres obowiązywania umowy i udostępnić je na żądanie właściwemu organowi nadzoru.
 - (5) Ustępy 1-3 pozostają bez uszczerbku dla obowiązku niezwłocznego poinformowania spółki transferującej dane osobowe przez odbiorcę, jeżeli nie jest w stanie przestrzegać niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
 - (6) Odbiorca zgadza się dokonać kontroli zgodności z prawem wniosku o ujawnienie informacji, w szczególności w zakresie tego, czy mieści się on w zakresie uprawnień przyznanych wnioskującemu organowi władzy publicznej, a także wnieść sprzeciw wobec tego wniosku, jeżeli po starannej ocenie stwierdzi, że istnieją uzasadnione podstawy do uznania wniosku za niezgodny z prawem na mocy przepisów państwa przeznaczenia, mających zastosowanie zobowiązań wynikających z prawa międzynarodowego oraz zasad wzajemnego poszanowania prawa międzynarodowego. Odbiorca korzysta z możliwości odwołania się na tych samych warunkach. Zgłaszając sprzeciw wobec wniosku, odbiorca zwraca się o zastosowanie środków tymczasowych w celu zawieszenia skutków wniosku do czasu podjęcia decyzji co do jego zasadności przez właściwy organ sądowy. Odbiorca nie ujawni żądanych danych osobowych do czasu, gdy będzie to wymagane zgodnie z obowiązującymi przepisami proceduralnymi. Wymogi te pozostają bez uszczerbku dla innych zobowiązań odbiorcy wynikających z niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
 - (7) Odbiorca zobowiązuje się udokumentować swoją ocenę prawną oraz wszelkie sprzeciwy wobec wniosku o ujawnienie oraz, w zakresie dozwolonym prawem kraju przeznaczenia, udostępnić dokumentację spółce transferującej dane osobowe. Udostępnia je również na żądanie właściwemu organowi nadzoru.
 - (8) Odbiorca zgadza się na podanie minimalnej dopuszczalnej ilości informacji w odpowiedzi na wniosek o ujawnienie informacji, w oparciu o zasadną interpretację tego wniosku.

§ 21 Przetwarzanie danych w imieniu administratora danych¹

- (1) Jeżeli spółka (administrator danych) zleca stronie trzeciej (podmiotowi przetwarzającemu) świadczenie usług w jej imieniu, zgodnie z jej instrukcjami, wówczas, oprócz umowy o świadczenie usług obejmującej prace do wykonania, umowa powinna również określać obowiązki podmiotu przetwarzającego jako strony, której powierzono przetwarzanie danych. Powyższe obowiązki określają instrukcje administratora danych dotyczące rodzaju i sposobu przetwarzania danych osobowych, celu przetwarzania oraz środków technicznych i organizacyjnych wymaganych dla ochrony danych.

Podmiot przetwarzający nie będzie przetwarzać danych osobowych (powierzonych mu w celu wykonania zlecenia) do jego własnych celów lub celów strony trzeciej związanych z przetwarzaniem

bez uprzedniej zgody administratora danych. Podmiot przetwarzający poinformuje uprzednio administratora danych o planach zlecenia podwykonawstwa prac innym osobom trzecim w celu wypełnienia jego obowiązków umownych. Administrator danych ma prawo sprzeciwić się powyższemu wykorzystaniu dalszych podmiotów przetwarzających. Jeżeli korzystanie z usług dalszych podmiotów przetwarzających będzie dopuszczalne, to podmiot przetwarzający zobowiąże ich do spełniania wymagań wynikających z umów zawartych pomiędzy podmiotem przetwarzającym a administratorem danych.

- (2) Spółki działające w charakterze podmiotu przetwarzającego powiadamiają administratora danych bez zbędnej zwłoki po powzięciu wiadomości o incydencie
- (3) Wyboru dalszych podmiotów przetwarzających dokonuje się na podstawie możliwości spełnienia przez nich powyższych wymagań.

¹ Niniejszy § nie jest przepisem w rozumieniu dokumentu roboczego nr 195 Grupy Roboczej art. 29 Komisji Europejskiej.

Sekcja 4

Jakość danych i bezpieczeństwo danych

§ 22 Prawdliwość danych

- (1) Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane gdy będzie to niezbędne (prawidłowość danych).
- (2) Ze względu na cel (cele), dla którego dane są przetwarzane należy podjąć odpowiednie środki dla zapewnienia, że wszelkie nieprawidłowe lub niekompletne informacje zostaną usunięte, zablokowane lub jeżeli zajdzie taka potrzeba poprawione.

§ 23 Bezpieczeństwo danych – środki techniczne i organizacyjne – ochrona danych w fazie projektowania i domyślna ochrona danych

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 oraz zapewni regularną ocenę skuteczności stosowanych środków.

Środki te obejmują:

- a) uniemożliwienie nieupoważnionym osobom uzyskania dostępu do systemów przetwarzania danych, w których dane osobowe są przetwarzane lub wykorzystywane (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 systemów, w których przetwarzane są dane osobowe będą miały dostęp wyłącznie do danych, do przetwarzania których zostali autoryzowani (kontrola dostępu do danych), a podczas przetwarzania dane osobowe nie mogą zostać odczytane, skopiowane, zmienione lub usunięte przez osoby nieupoważnione (np. poprzez szyfrowani);
- d) zapewnienie, że w trakcie przekazywania danych drogą elektroniczną lub podczas przenoszenia danych lub nagrywania danych na nośnik, dane osobowe nie mogą zostać odczytane, skopiowane, zmienione lub usunięte przez osoby nieupoważnione oraz, że będzie możliwe jednoznaczne ustalenie oraz zweryfikowanie odbiorców, którym dane mogą zostać przekazane za pomocą sprzętu do przesyłania danych (kontrola przekazywania danych);
- e) zapewnienie, że istnieje możliwość późniejszego sprawdzenia i ustalenia, czy i przez kogo dane osobowe zostały wprowadzone do systemów przetwarzania danych, zmienione lub usunięte (kontrola wprowadzania danych);
- f) zapewnienie, że dane osobowe które zostały powierzone do przetwarzania mogą być przetwarzane wyłącznie zgodnie z instrukcjami administratora (kontrola podmiotu przetwarzającego);
- g) zapewnienie, że dane osobowe są chronione przed przypadkowym zniszczeniem lub utratą (kontrola dostępności);
- h) zapewnienie, że dane, które były zbierane w różnych celach mogą być przetwarzane odrębnie (zasada rozdzielności).

Część trzecia:

Prawa osób, których dane dotyczą

§ 24 Prawo dostępu

- (1) Osoby, których dane dotyczą, mogą się w dowolnym czasie skontaktować ze spółką, która przetwarza ich dane i domagać się podania następujących informacji:
 - a) dotyczących ich danych osobowych znajdujących się w posiadaniu spółki, wraz z ich pochodzeniem i odbiorcą/odbiorcami;
 - b) na temat celu przetwarzania danych;
 - c) dotyczących odbiorcy/ów, którym ich dane są lub zostały przekazane, w szczególności jeżeli dane te są przekazywane do państwa trzeciego;
 - d) postanowień niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
- (2) Odpowiednie informacje powinny zostać udzielone osobie, której dane dotyczą, w zrozumiałej formie i w odpowiednim terminie. Następuje to zwykle w formie pisemnej lub elektronicznie. W każdym przypadku osoba, której dane dotyczą, musi otrzymać informacje w ciągu miesiąca od otrzymania złożonego przez nią wniosku. W razie potrzeby termin udzielenia odpowiedzi może zostać przedłużony o kolejne dwa miesiące, biorąc pod uwagę złożoność danej sprawy i liczbę wniosków. Osoba, której dane dotyczą, jest informowana o każdym takim wydłużeniu terminu, w którym może spodziewać się odpowiedzi. Przekazanie wydruku niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności jest wystarczające jako sposób przekazania informacji o ich wymaganiach.
- (3) Jeżeli dopuszczają to odpowiednie przepisy krajowe, spółka może naliczyć opłatę za przekazanie dodatkowych kopii odpowiednich informacji, o które wnioskuje osoba, której dane dotyczą.

§ 25 Prawo sprzeciwu, prawo do usunięcia danych lub ograniczenia przetwarzania oraz prawo do sprostowania danych

- (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 wiążące.
- (2) Prawo sprzeciwu przysługuje również w przypadku, gdy osoby, których dane dotyczą wyraziły uprzednio zgodę na przetwarzanie ich danych.
- (3) Uzasadnione wnioski o usunięcie lub ograniczenie przetwarzania danych zostaną niezwłocznie zrealizowane. Powyższe wnioski są uzasadnione zwłaszcza w przypadku, gdy podstawa prawna przetwarzania danych przestanie obowiązywać. 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.

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

- (1) Jeżeli osoba, której dane dotyczą twierdzi, że jej/jego prawa zostały naruszone przez bezprawne przetwarzanie jej/jego danych, w szczególności przedstawiając dowody znajdującego potwierdzenie w faktach naruszenia niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, odpowiedzialne spółki wyjaśnią sytuację bez zbędnej zwłoki. W przypadku danych przekazywanych w szczególności do spółek poza terytorium Europejskiego Obszaru Gospodarczego, spółka mająca siedzibę w Europejskim Obszarze Gospodarczym wyjaśni sytuację i przedstawi dowody, że odbiorca nie naruszył 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 skargę 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 o statusie przetwarzania w terminie nie później niż miesiąc od zgłoszenia zażalenia. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące, biorąc pod uwagę złożoność sprawy i liczbę wniosków, a osoba, której dane dotyczą, musi zostać o tym wydłużeniu terminu odpowiednio poinformowana.
- (3) Jeżeli skarga dotyczy kilku spółek, Inspektor Ochrony Danych spółki, która jest najlepiej zaznajomiona z przedmiotem, będzie koordynować całość odpowiedniej korespondencji z osobą, której dane dotyczą. Inspektor Ochrony Danych Grupy będzie upoważniony w dowolnym czasie do skorzystania z przysługującego mu prawa wstąpienia (subrogacji) i przejęcia sprawy.
- (4) Udostępnione zostaną odpowiednie kanały do zgłaszania incydentów w zakresie prywatności danych (takie jak specjalne konta e-mail udostępniane przez Inspektora Ochrony Danych lub bezpośrednia osoba kontaktowa, z którą można się skontaktować elektronicznie).
- (5) Inspektor Ochrony Danych zainteresowanej spółki poinformuje niezwłocznie Inspektora Ochrony Danych Grupy o incydencie w zakresie prywatności danych za pomocą odpowiednich procesów raportowania oraz zabezpieczy dokumentację dotyczącą incydentu związanego z prywatnością danych i udostępni tę dokumentację organom nadzoru na żądanie.
- (6) Osoby, których dane dotyczą mogą wystąpić z roszczeniem zgodnie z Częścią Piątą niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności, jeżeli ich prawa zostały naruszone lub poniosły one jakiegokolwiek straty.

§ 27 Prawo do zadawania pytań i zgłaszania skarg

Każda osoba, której dane dotyczą ma prawo do skontaktowania się w dowolnym czasie z Inspektorem Ochrony Danych spółki przetwarzającej 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.

§ 28 Wykonywanie praw osób, 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.

§ 29 Dostęp do Wiążących Reguł Korporacyjnych dotyczących Prywatności

Obecna wersja niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności oraz wykaz spółek, które je przyjęły z prawnie wiążącym skutkiem, są publikowane na www.telekom.com.

Część czwarta:

Organizacja ochrony danych

§ 30 Odpowiedzialność za przetwarzanie danych

Spółki są zobowiązane do zapewnienia zgodności z przepisami prawa dotyczącymi ochrony danych oraz z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności i są zobowiązane do wykazania tego w każdym czasie.

§ 31 Inspektor Ochrony Danych

- (1) Każda spółka mianuje niezależnego Inspektora Ochrony Danych, którego zadaniem jest zapewnienie, że poszczególne jednostki organizacyjne tej spółki są informowane o ustawowych i wewnętrznych wymaganiach spółki/Grupy w zakresie ochrony danych oraz w szczególności o niniejszych Wiążących Regułach Korporacyjnych dotyczących Prywatności. Inspektor Ochrony Danych stosuje odpowiednie środki, w szczególności prowadzi wyrywkowe inspekcje, w celu monitorowania zgodności z przepisami dotyczącymi ochrony danych.
- (2) Spółka skonsultuje się z Inspektorem Ochrony Danych Grupy przed mianowaniem lub odwołaniem Inspektora Ochrony Danych.
- (3) Spółka zapewnia, aby zadania i obowiązki Inspektora Ochrony Danych nie prowadziły do konfliktu interesów.
- (4) Spółka zapewnia, że Inspektor Ochrony Danych posiada odpowiednie kompetencje do oceny aspektów prawnych, technicznych i organizacyjnych środków ochrony prywatności danych.
- (5) Spółka udostępnia Inspektorowi Ochrony Danych zasoby finansowe i osobowe niezbędne do wykonywania jego obowiązków.
- (6) Inspektor Ochrony Danych otrzyma prawo do raportowania bezpośrednio do zarządu spółki i będzie powiązany organizacyjnie z kierownictwem spółki.
- (7) Inspektor Ochrony Danych każdej spółki jest odpowiedzialny za wdrożenie wymagań Inspektora Ochrony Danych Grupy i strategii prywatności danych Grupy Deutsche Telekom.
- (8) Wszystkie departamenty każdej spółki są zobowiązane do informowania Inspektora Ochrony Danych w ich spółce o sytuacji w zakresie infrastruktury informatycznej, infrastruktury sieciowej, modeli biznesowych, produktów, przetwarzania danych pracowników i odpowiednich planach strategicznych. Inspektor Ochrony Danych jest powiadamiany o zaistniałej sytuacji we wczesnej fazie w celu zapewnienia, że wszelkie sprawy dotyczące ochrony danych zostaną rozpatrzone i poddane ocenie.

§ 32 Inspektor Ochrony Danych Grupy

- (1) Inspektor Ochrony Danych Grupy 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 Inspektora Ochrony Danych Grupy jest opracowanie i rozwijanie polityki prywatności danych Grupy Deutsche Telekom oraz przeprowadzanie w razie potrzeby konsultacji z Inspektorami Ochrony Danych spółek Grupy. Inspektorzy Ochrony Danych opracowują politykę prywatności danych dla ich spółek zgodnie z polityką Grupy dotyczącą prywatności danych. Inspektor Ochrony Danych Grupy i Inspektor Ochrony Danych ze spółek krajowych spotykają się co roku w celu wymiany informacji na bezpośrednich spotkaniach.

§ 33 Obowiązek informowania w przypadku naruszeń lub zmiany przepisów i praktyk mających zastosowanie do spółki

Zainteresowana spółka niezwłocznie informuje jej Inspektora Ochrony Danych o wszelkich naruszeniach lub sytuacjach wskazujących wyraźnie na naruszenie przepisów dotyczących ochrony danych, w szczególności niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Inspektor Ochrony Danych z kolei informuje niezwłocznie Inspektora Ochrony Danych Grupy, 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. Inspektor Ochrony Danych Grupy musi być zawsze informowany, gdy właściwy organ nadzoru nałożył na spółkę administracyjną karę pieniężną.

Inspektor Ochrony Danych spółki informuje również Inspektora Ochrony Danych Grupy w przypadku wprowadzenia zmian do przepisów i praktyk mających zastosowanie do spółki, które są w znacznym stopniu niekorzystne w aspekcie zgodności z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności.

Spółki działające w charakterze administratora danych informują bez zbędnej zwłoki osoby, których dane dotyczą, jeżeli incydent może spowodować wysokie ryzyko naruszenia ich praw i wolności.

§ 34 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 Inspektora Ochrony Danych Grupy w ramach rocznego planu inspekcji oraz za pomocą innych środków, takich jak inspekcje przeprowadzane spółek przez Inspektorów Ochrony Danych i sprawozdania. Roczny plan inspekcji uwzględnia ryzyko związane z czynnościami przetwarzania wchodzącymi w zakres niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Wewnętrzni i zewnętrzni audytorzy przeprowadzają inspekcje dotyczące Inspektora Ochrony Danych Grupy. W ramach Grupy Deutsche Telekom przeprowadzane mogą być również regularne procesy samooceny koordynowane przez Inspektora Ochrony Danych Grupy.
- (2) Prezes Grupy Deutsche Telekom Holding jest informowany o wynikach najważniejszych inspekcji i środkach uzgadnianych po ich przeprowadzeniu. 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 Inspektor Ochrony Danych Grupy będzie monitorować wdrożenie tych środków. W przypadku niewdrożenia przez spółkę takich środków bez odpowiedniego uzasadnienia, Inspektor Ochrony Danych Grupy oceni wpływ na prywatność danych i podejmie niezbędne działania, eskalując sprawę w razie potrzeby.
- (4) Inspektorzy Ochrony Danych spółek lub innych jednostek organizacyjnych, którym zlecono przeprowadzenie inspekcji przeprowadzą również kontrole na podstawie dedykowanych planów audytu udokumentowanych w formie pisemnej w celu stwierdzenia, czy spółki spełniają wymagania w zakresie ochrony danych. Inspektorzy Ochrony Danych nie są odpowiedzialni za kontrolę zgodności z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności, jeżeli taka sytuacja może skutkować konfliktem interesów.
- (5) Jeżeli nie istnieją ograniczenia prawne w tym zakresie, Inspektor Ochrony Danych Grupy i Inspektorzy Ochrony Danych są upoważnieni do sprawdzenia, odpowiednio we wszystkich spółkach i w ich spółce, czy dane osobowe są wykorzystywane prawidłowo. Odpowiednie spółki zapewnią Inspektorowi Ochrony Danych Grupy i Inspektorom Ochrony Danych nieograniczony dostęp do informacji, które są im niezbędne w celu wyjaśnienia i oceny sytuacji. Inspektor Ochrony Danych Grupy i Inspektorzy Ochrony Danych są upoważnieni do wydania instrukcji w tym zakresie.
- (6) W ramach przeprowadzanych przez nich inspekcji, Inspektorzy Ochrony Danych spółek korzystają ze standardowych procedur obowiązujących w całej Grupie, np. wspólnych audytów ochrony danych, jeżeli jest to możliwe. Powyższe procedury mogą zostać udostępnione przez Inspektora Ochrony Danych Grupy.

§ 35 Ocena skutków dla ochrony danych

Spółki przeprowadzają ustrukturyzowaną i udokumentowaną ocenę skutków dla ochrony danych dla operacji przetwarzania danych osobowych. Deutsche Telekom Group Holding zapewnia centralnie dostępny proces oceny prywatności i bezpieczeństwa o nazwie Privacy and Security Assessment (PSA), który musi zostać wdrożony w obecnej wersji w sposób jednolity we wszystkich spółkach. Odstępstwa od stosowania procesu PSA mogą być dokonywane w porozumieniu z Inspektorem Ochrony Danych Grupy i za jego uprzednią zgodą, jeżeli spółki są bardzo małe lub przetwarzanie danych w ramach ich działalności nie ma istotnego znaczenia.

§ 36 Zaangażowanie i szkolenia pracowników

- (1) Spółki zobowiązują swoich pracowników do zachowania w poufności danych osobowych, w tym w szczególności danych objętych tajemnicą telekomunikacyjną 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 ochrony danych regularnie lub co najmniej raz na dwa lata. Spółki są upoważnione do opracowania i prowadzenia dedykowanych szkoleń dla ich własnych pracowników. Inspektor Ochrony Danych każdej spółki dokumentuje przeprowadzenie powyższych szkoleń i informuje co roku Inspektora Ochrony Danych Grupy.
- (3) Inspektor Ochrony Danych Grupy może udostępnić centralnie zasoby i procesy w celu zobowiązania i przeszkolenia pracowników Grupy Deutsche Telekom.

§ 37 Współpraca z organami nadzoru

- (1) Spółki zobowiązują się do współpracy na zasadzie zaufania z organem nadzoru właściwym miejscowo dla nich lub dla spółki przekazującej 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 Reguł Korporacyjnych dotyczących Prywatności, odpowiednia spółka powiadomi o zmianie właściwy organ nadzoru.
- (3) Wszelkie spory związane z wykonywaniem nadzoru nad przestrzeganiem niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności przez organ nadzoru będą rozstrzygane przez sądy państwa członkowskiego właściwego dla danego organu nadzoru, zgodnie z prawem proceduralnym tego państwa członkowskiego. Spółki zgadzają się poddać się jurysdykcji tych sądów.

§ 38 Odpowiedzialna osoba kontaktowa ds. pytań

Inspektorzy Ochrony Danych spółek lub Inspektor Ochrony Danych Grupy są osobami kontaktowymi odpowiedzialnymi za udzielanie odpowiedzi na pytania dotyczące niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności. Inspektor Ochrony Danych Grupy przekaze dane kontaktowe Inspektorom Ochrony Danych spółek na żądanie.

Z Inspektorem Ochrony Danych Grupy można się kontaktować pod adresem

datenschutz@telekom.de

privacy@telekom.de

Friedrich-Ebert-Allee 140,

53113 Bonn

Część piąta: Odpowiedzialność

§ 39 Obszar zastosowania zasad dotyczących odpowiedzialności

- (1) Niniejsza część piąta Wiążących Reguł Korporacyjnych dotyczących Prywatności dotyczy wyłącznie przetwarzania danych osobowych, wobec którego stosuje się przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Wobec spółek znajdujących się na terytorium Europejskiego Obszaru Gospodarczego obowiązują stosuje się prawo kraju, w którym ma siedzibę spółka. W przypadku danych, które nie podlegają § 9, Sekcja 1 Wiążących Reguł Korporacyjnych dotyczących Prywatności, 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.
- (2) Zapłata odszkodowania zawiązka, w przypadku której spółka musi zapłacić osobie, której dane dotyczą kwotę przewyższającą wartość szkody, zostanie wyraźnie wykluczona.

§ 40 Zwolnienia z odpowiedzialności

- (1) Osoba, której dane dotyczą, 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 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 z holdingu 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 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. Odbiorca nie jest uprawniony do odstąpienia od odpowiedzialności przez odwołanie się do odpowiedzialności podmiotu przetwarzającego w przypadku naruszenia.
- (4) Osoba, której dane dotyczą jest również uprawniona do wniesienia w dowolnym czasie skargi do właściwego organu nadzoru w państwie członkowskim zamieszkania, pracy lub zarzucanego naruszenia bądź do organu nadzoru odpowiedzialnego za spółkę holdingową Grupy Deutsche Telekom.
- (5) Osoba, której dane dotyczą, ma prawo wnieść skargę do właściwych sądów na terytorium Europejskiego Obszaru Gospodarczego, jeżeli uzna, że jej prawa wynikające z niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności zostały naruszone w wyniku przetwarzania jej danych osobowych niezgodnie z postanowieniami niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności.
- (6) Osoba, której dane dotyczą, ma prawo upoważnić organ, organizację lub stowarzyszenie non-profit do wykonywania wyżej wymienionych praw w jej imieniu.

§ 41 Ciężar dowodu

Ciężar dowodu prawidłowego przetwarzania danych osoby, której dane dotyczą, spoczywa na spółkach odpowiedzialnych za ten proces.

§ 42 Korzyści osoby trzeciej dla osób, których dane dotyczą

Jeżeli osobie, której dane dotyczą nie przysługują żadne bezpośrednie roszczenia, 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.

§ 43 Miejsce jurysdykcji

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

- a) miejsce zwykłego pobytu danej osoby fizycznej lub
- b) miejsce w jurysdykcji, w której członek grupy ma siedzibę, lub
- c) siedziba na terytorium UE lub europejskiego członka grupy, na którym spoczywają obowiązki związane z ochroną danych.

§ 44 Rozstrzygnięcie pozasądowe

- (1) Osoby trzecie, które uważają, że ich indywidualne prawo do prywatności zostało naruszone w wyniku rzeczywistego lub podejrzanego przetwarzania ich danych osobowych mają prawo domagać się od Inspektora Ochrony Danych odpowiedniej spółki rozstrzygnięcia tej sprawy. Inspektor Ochrony Danych jest uprawniony do zbadania skargi i poinformowania osoby, której dane dotyczą, o przysługujących jej/jemu prawach. Podczas wykonywania tych czynności Inspektor Ochrony Danych jest zobowiązany do zachowania poufności innych danych osobowych skarżącego, chyba że skarżący zwolni Inspektora Ochrony Danych z tego obowiązku. Na wniosek zainteresowanej osoby podjęta zostanie próba osiągnięcia porozumienia w sprawie skargi, z udziałem osoby, której dane dotyczą i Inspektora Ochrony 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 wniesienia skargi do właściwego organu nadzoru albo przed organem nadzoru w państwie członkowskim w państwie członkowskim zamieszkania, pracy lub zarzucanego naruszenia, albo do podjęcia działań prawnych pozostaje nienaruszone.

Część szósta: Postanowienia końcowe

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

- (1) Inspektor Ochrony Danych Grupy bada Wiążące Reguły Korporacyjne dotyczące Prywatności w regularnych odstępach czasu, lecz co najmniej raz w roku, w celu weryfikacji ich zgodności z obowiązującym środowiskiem regulacyjnym 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) Inspektor Ochrony Danych Grupy poinformuje wszystkie spółki, które wprowadziły Wiążące Reguły Korporacyjne dotyczące Prywatności o zmienionej treści.
- (4) Inspektorzy Ochrony Danych spółek mają obowiązek zbadania, czy zmiany wprowadzone do niniejszych Wiążących Reguł Korporacyjnych dotyczących Prywatności mają implikacje dla zgodności z przepisami w ich własnym kraju lub czy są sprzeczne z przepisami prawa lub praktyką w ich odpowiednim kraju. Jeżeli spółka nie ma możliwości wprowadzenia zmian ze względu na obowiązujące uwarunkowania prawne, spółka poinformuje niezwłocznie Inspektora Ochrony Danych Grupy i właściwy organ nadzoru, a w razie potrzeby niniejsze Wiążące Reguły Korporacyjne dotyczące Prywatności zostaną czasowo zawieszona w odniesieniu do tej spółki.
- (5) Spółki przekazujące dane osobowe w państwach trzecich na bieżąco monitorują, w stosownych przypadkach we współpracy z odbiorcami, rozwój sytuacji w odpowiednich państwach trzecich, który może mieć wpływ na istniejące oceny skutków transferu i zgodność z niniejszymi Wiążącymi Regułami Korporacyjnymi dotyczącymi Prywatności.

§ 46 Wykaz danych kontaktowych i spółek

Inspektor Ochrony Danych Grupy 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 na żądanie. Raz w roku właściwy organ nadzoru otrzymuje aktualny wykaz spółek, które wprowadziły Wiążące Reguły Korporacyjne dotyczące Prywatności w sposób wiążący.

§ 47 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.

§ 48 Publikacja

Spółki udostępniają publicznie informacje dotyczące praw osób, których dane dotyczą i klauzuli korzyści dla osoby trzeciej w odpowiedniej formie, np. w zakładkach 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 warunki

Anonimizacja

oznacza proces zmiany informacji w taki sposób, że dane osobowe i inne fakty nie pozwalają na doprowadzenie do 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 osiągnięte 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 danych

oznacza osobę fizyczną lub prawną, która ustala cele i sposoby przetwarzania danych osobowych.

Osoba, której dane dotyczą

oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną, której dane osobowe są przetwarzane w ramach Grupy Deutsche Telekom.

Grupa Deutsche Telekom

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.

Europejski Obszar Gospodarczy

składa się z państw członkowskich Unii Europejskiej i trzech państw Europejskiego Stowarzyszenia Wolnego Handlu (Islandia, Liechtenstein i Norwegia; z wyłączeniem Szwajcarii).

Spółka Holdingowa Grupy

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

Dalsze przekazanie

oznacza przekazywanie danych osobowych z państwa trzeciego do innego państwa trzeciego.

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.

Pseudonimizacja

oznacza przetwarzanie danych osobowych w taki sposób, aby dane osobowe nie mogły być już przypisane konkretnej osobie, której dane dotyczą, bez wykorzystania dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym oraz organizacyjnym służącym do zapewnienia, że dane osobowe nie są przypisane zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Przetwarzanie

oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Podmiot przetwarzający

oznacza spółkę przetwarzającą dane osobowe w imieniu administratora danych.

Odbiorca

oznacza osobę fizyczną lub prawną, organ władzy publicznej, agencję lub inny organ, któremu ujawniane są dane osobowe, będące lub niebędące osobą trzecią. Jednak władze publiczne, które mogą otrzymywać dane w ramach pojedynczego dochodzenia, 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, a także dane genetyczne, dane biometryczne służące do celów jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia lub dane dotyczące życia seksualnego bądź orientacji seksualnej osoby fizycznej.

Strona trzecia

oznacza osobę fizyczną lub prawną, organ władzy publicznej, agencję lub podmiot inny niż osoba, której dane dotyczą, administrator danych, podmiot przetwarzający i osoby, które są upoważnione do przetwarzania danych osobowych pod bezpośrednim zwierzchnictwem administratora danych lub podmiotu przetwarzającego.