

ΠΟΛΙΤΙΚΗ	
Τίτλος:	ΔΕΣΜΕΥΤΙΚΟΙ ΚΑΝΟΝΕΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΝΤΟΣ ΤΟΥ ΟΜΙΛΟΥ DT
Τομέας:	ΔΙΑΧΕΙΡΙΣΗ ΕΤΑΙΡΙΚΩΝ ΡΙΣΚΩΝ
Υπεύθυνη Επιχειρησιακή Μονάδα (Process Owner):	ΔΙΕΥΘΥΝΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ & ΑΠΟΤΡΟΠΗΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΗΣ ΑΠΑΤΗΣ ΟΜΙΛΟΥ ΟΤΕ
Ημερομηνία Ισχύος:	15/10/2015
Περίληψη:	<p>Η προστασία των προσωπικών δεδομένων των πελατών, των εργαζομένων κι άλλων φυσικών προσώπων που συνδέονται με τον Όμιλο Deutsche Telekom αποτελεί ύψιστη προτεραιότητα για όλες τις εταιρείες του Ομίλου.</p> <p>Οι εταιρείες του Ομίλου Deutsche Telekom έχουν επίγνωση ότι η επιτυχία του Ομίλου Deutsche Telekom στο σύνολό του εξαρτάται και από τον αξιόπιστο και ασφαλή χειρισμό των προσωπικών δεδομένων.</p> <p>Ο Όμιλος Deutsche Telekom θεωρείται από τους πελάτες του και το ευρύ κοινό ως μια ενιαία νομική οντότητα. Ως εκ τούτου, είναι κοινό μέλημα όλων των εταιρειών του να συμβάλλουν σημαντικά στην συλλογική επιτυχία του Ομίλου και να ενισχύσουν την κοινή αντίληψη ότι ο Όμιλος προσφέρει υψηλής ποιότητας προϊόντα και καινοτόμες υπηρεσίες εφαρμόζοντας τους παρόντες Δεσμευτικούς Εταιρικούς Κανόνες Προστασίας Προσωπικών Δεδομένων (Binding Corporate Rules Privacy, εφεξής BCRP).</p> <p>Με την εφαρμογή των BCRP ο Όμιλος Deutsche Telekom δημιουργεί ένα τυποποιημένο και υψηλό επίπεδο προστασίας των προσωπικών δεδομένων σε παγκόσμιο επίπεδο κατά την επεξεργασία των προσωπικών δεδομένων εντός μιας εταιρείας και μεταξύ των εταιρειών, καθώς και κατά την διαβίβαση των δεδομένων στο εσωτερικό της Γερμανίας και σε διεθνές επίπεδο. Εντός του Ομίλου Deutsche Telekom, τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία από τον αποδέκτη τους σύμφωνα με την νομοθεσία περί προστασίας των προσωπικών δεδομένων, που ισχύουν στην δικαιοδοσία του μέρους από όπου μεταφέρονται.</p>

	ΘΕΣΗ	ΥΠΟΓΡΑΦΗ
Σύνταξη:		
Ανασκόπηση:		
Έγκριση:	Συνεδρίαση Διοικητικού Συμβουλίου ΟΤΕ αρ. 2989 της 15/10/2015 Συνεδρίαση Διοικητικού Συμβουλίου COSMOTE αρ. 440 της 02/11/2015	

ΙΣΤΟΡΙΚΟ ΑΛΛΑΓΩΝ		
Έκδοση	Ημερομηνία	Περιγραφή Αλλαγών
1.0	15/10/2015	Έναρξη ισχύος εγγράφου με τίτλο «Δεσμευτικοί Κανόνες Προστασίας Προσωπικών Δεδομένων εντός του Ομίλου DT» σε αντικατάσταση της έκδοσης 1.0-01/07/09 του ΟΤΕ και της 1.1-17/02/11 της COSMOTE του εγγράφου «Κώδικας Δεοντολογίας για την Προστασία των Δικαιωμάτων του Ατόμου κατά την Επεξεργασία των Προσωπικών Δεδομένων του εντός του Ομίλου ΟΤΕ» .

Περιεχόμενα

ΜΕΡΟΣ ΠΡΩΤΟ – Σκοπός.....	5
1) Νομική Φύση των Δεσμευτικών Εταιρικών Κανόνων Προστασίας Δεδομένων	5
2) Πεδίο Εφαρμογής	5
3) Σχέση με άλλες νομικές διατάξεις.....	5
4) Λήξη ισχύος και καταγγελία	6
4.1) Είδος Πρόσβασης.....	6
ΜΕΡΟΣ ΔΕΥΤΕΡΟ - Γενικές Αρχές.....	7
Κεφάλαιο 1 – Διαφάνεια στην Επεξεργασία Δεδομένων	7
5) Δικαίωμα Ενημέρωσης.....	7
6) Περιεχόμενο και Μορφή Ενημέρωσης.....	7
7) Διαθεσιμότητα της Ενημέρωσης.....	7
Κεφάλαιο 2 – Κανόνες Αποδεκτής Χρήσης Προσωπικών Δεδομένων	8
8) Αρχή.....	8
9) Προϋποθέσεις Αποδεκτής Χρήσης Προσωπικών Δεδομένων	8
10) Συγκατάθεση του υποκειμένου των δεδομένων	8
11) Αυτοματοποιημένη Χρήση Προσωπικών Δεδομένων	9
12) Χρήση Προσωπικών Δεδομένων με Σκοπό την Απευθείας Προώθηση Προϊόντων/ Υπηρεσιών 9	
13) Ειδικές Κατηγορίες Προσωπικών Δεδομένων (ευαίσθητα προσωπικά δεδομένα)	9
14) Ελαχιστοποίηση Χρήσης, Αποφυγή Χρήσης, Χρήση Ανώνυμων και Ψευδώνυμων Δεδομένων 9	
15) Απαγόρευση Δέσμευσης.....	10
Κεφάλαιο 3- Διαβίβαση Προσωπικών Δεδομένων	11
16) Φύση και Σκοπός της Διαβίβασης Προσωπικών Δεδομένων	11
17) Διαβίβαση Δεδομένων	11
18) Ανάθεση Επεξεργασίας των Δεδομένων.....	11
Κεφάλαιο 4 – Ποιότητα & Ασφάλεια Δεδομένων.....	12
19) Ποιότητα στην Επεξεργασία των Δεδομένων	12
20) Ασφάλεια Δεδομένων – Τεχνικά και Οργανωτικά Μέτρα.....	12
ΜΕΡΟΣ ΤΡΙΤΟ- ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ.....	13
21) Δικαίωμα Ενημέρωσης.....	13
22) Δικαίωμα Αντίρρησης, Δικαίωμα Διαγραφής ή Αποκλεισμού των Δεδομένων/ Δικαίωμα Διόρθωσης	13
23) Δικαίωμα Υποβολής Αιτήματος για Παροχή Διευκρινίσεων, Παρατηρήσεων και Αποκατάστασης Σχολιασμού.....	13
24) Δικαίωμα Υποβολής Ερωτήσεων και Παραπόνου	14
25) Τρόπος Άσκησης των Δικαιωμάτων των Υποκειμένων.....	14
26) Αντίγραφο των BCRP	14
ΜΕΡΟΣ ΤΕΤΑΡΤΟ - ΔΙΟΙΚΗΤΙΚΗ ΟΡΓΑΝΩΣΗ	15
27) Αρμοδιότητα για την Επεξεργασία Δεδομένων	15
28) Υπεύθυνος Προστασίας Προσωπικών Δεδομένων	15
29) Υπεύθυνος Προστασίας Προσωπικών Δεδομένων Ομίλου.....	15

30)	Καθήκον Ενημέρωσης σε Περίπτωση Παραβίασης	16
31)	Επιθεώρηση του Επιπέδου Προστασίας Δεδομένων	16
32)	Δέσμευση και Εκπαίδευση Εργαζομένων	17
33)	Συνεργασία με τις Εποπτικές Αρχές	17
34)	Υπεύθυνος Επικοινωνίας για Ερωτήματα	17
ΜΕΡΟΣ ΠΕΜΠΤΟ – ΕΥΘΥΝΗ		18
35)	Πεδίο Εφαρμογής των Διατάξεων Περί Ευθύνης	18
36)	Αποζημίωση	18
37)	Βάρος Απόδειξης	18
38)	Ρήτρα Υπέρ Τρίτου	18
39)	Αρμοδιότητα Δικαστηρίων	19
40)	Εξωδικαστική Διατησία	19
ΜΕΡΟΣ ΕΚΤΟ-ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ		20
41)	Τροποποίηση	20
42)	Λίστα Επαφών και Εταιρειών	20
43)	Δικονομικά Θέματα / Ρήτρα Διαχωρισμού (Severability Clause)	20
44)	Δημοσίευση	20
Όροι – Συντομογραφίες		21

ΜΕΡΟΣ ΠΡΩΤΟ – Σκοπός

1) Νομική Φύση των Δεσμευτικών Εταιρικών Κανόνων Προστασίας Δεδομένων

Οι BCRP είναι δεσμευτικοί κανόνες σχετικοί με την επεξεργασία προσωπικών δεδομένων (με βάση το έγγραφο εργασίας 133, της Ομάδας Εργασίας του Άρθρου 29 της Ευρωπαϊκής Επιτροπής) από όλες τις εταιρίες του Ομίλου DT που τους έχουν υιοθετήσει με νομικά δεσμευτική ισχύ. Οι BCRP είναι επίσης δεσμευτικοί για όλες τις εταιρίες, που τους έχουν υιοθετήσει μετά από σχετικό αίτημα της Deutsche Telekom, καθώς και για όλες τις εταιρίες που τους έχουν υιοθετήσει οικειοθελώς, ανεξαρτήτως του τόπου στον οποίο συλλέγονται τα δεδομένα.

2) Πεδίο Εφαρμογής

Η παρούσα Πολιτική ισχύει για τον ΟΤΕ και την COSMOTE (εφεξής «Εταιρεία»).

Οι BCRP ισχύουν σε κάθε είδους επεξεργασία όλων των ειδών των προσωπικών δεδομένων εντός του Ομίλου Deutsche Telekom, ανεξάρτητα από το πού συλλέγονται τα δεδομένα. Τα προσωπικά δεδομένα χρησιμοποιούνται από τον Όμιλο Deutsche Telekom κυρίως για τους ακόλουθους σκοπούς:

- (1) Διαχείριση των δεδομένων των εργαζομένων κατά την σύναψη και την λειτουργία της σύμβασης εργασίας τους και την παροχή προϊόντων και υπηρεσιών που προσφέρονται στους εργαζομένους από τον Όμιλο Deutsche Telekom ή τρίτα μέρη.
- (2) Έναρξη, υλοποίηση κι επεξεργασία συμβάσεων με εταιρικούς και οικιακούς πελάτες, καθώς και για σκοπούς διαφήμισης και έρευνας αγοράς με στόχο την ενημέρωση των πελατών και των ενδιαφερομένων τρίτων μερών σχετικά με τα προϊόντα και τις υπηρεσίες που προσφέρονται από τον Όμιλο Deutsche Telekom ή τρίτα μέρη.
- (3) Σύναψη και υλοποίηση συμφωνιών με τους παρόχους υπηρεσιών προς τον Όμιλο Deutsche Telekom ως μέρος της παροχής υπηρεσιών.
- (4) Σύναψη κατάλληλων συμφωνιών με άλλα τρίτα μέρη, κυρίως με μετόχους, συνεργάτες ή επισκέπτες, και συμμόρφωση με νομικές δεσμεύσεις.

Τα προσωπικά δεδομένα χρησιμοποιούνται για την εξυπηρέτηση των σκοπών -τωνωνών ή μελλοντικών - των εταιρειών του Ομίλου Deutsche Telekom, οι οποίοι περιλαμβάνουν την παροχή τηλεπικοινωνιακών υπηρεσιών, ψηφιακών υπηρεσιών για εταιρικούς και οικιακούς πελάτες, υπηρεσιών πληροφορικής (συμπεριλαμβανομένων υπηρεσιών data center) και συμβουλευτικών υπηρεσιών.

3) Σχέση με άλλες νομικές διατάξεις

- (1) Οι διατάξεις των BCRP έχουν σκοπό την εξασφάλιση υψηλού και τυποποιημένου επιπέδου προστασίας των προσωπικών δεδομένων σε όλο τον Όμιλο Deutsche Telekom. Ως εκ τούτου, κανονισμοί, διαδικασίες κτλ, που ισχύουν στις εταιρίες του Ομίλου Deutsche Telekom και υπερβαίνουν τις αρχές που προβλέπονται από τους BCRP ή που θέτουν επιπλέον περιορισμούς κατά την επεξεργασία των προσωπικών δεδομένων, εξακολουθούν να ισχύουν ως έχουν.
- (2) Τα δεδομένα που συλλέγονται στην Ευρώπη χρησιμοποιούνται σύμφωνα με τις νομικές διατάξεις της χώρας στην οποία συλλέχθηκαν τα δεδομένα, ανεξάρτητα από το πού αυτά χρησιμοποιούνται, αλλά κατ' ελάχιστον σύμφωνα με τις απαιτήσεις των παρόντων BCRP.

- (3) Η εφαρμογή της εθνικής νομοθεσίας, που θεσπίστηκε για λόγους εθνικής ασφάλειας, εθνικής άμυνας ή δημόσιας ασφάλειας, ή για την πρόληψη και τη διερεύνηση εγκλημάτων και τη δίωξη εγκληματιών, και η οποία απαιτεί τη διαβίβαση δεδομένων σε τρίτα μέρη, δε θίγεται από τις διατάξεις των BCRP. Εάν μια εταιρεία διαπιστώσει ότι διατάξεις των BCRP αντιβαίνουν στην εθνική νομοθεσία περί προστασίας προσωπικών δεδομένων τότε ενημερώνεται αμελλητί ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου Deutsche Telekom (Group Data Privacy Officer). Η αρμόδια εποπτική Αρχή της εταιρείας αναλαμβάνει ρόλο μεσολάβησης μεταξύ των μερών.

4) Λήξη ισχύος και καταγγελία

Οι BCRP παύουν να είναι δεσμευτικοί για μια εταιρεία εάν αυτή αποχωρήσει από τον Όμιλο Deutsche Telekom ή τους καταγγείλει. Ωστόσο, η λήξη ισχύος ή η καταγγελία των BCRP δεν απαλλάσσει την εταιρεία από τις υποχρεώσεις που απορρέουν από αυτούς και αφορούν τη χρήση των δεδομένων που έχουν ήδη διαβιβαστεί. Περαιτέρω διαβίβαση προσωπικών δεδομένων από ή προς την εν λόγω εταιρεία μπορεί να πραγματοποιηθεί μόνο εάν παρέχονται άλλες κατάλληλες διαδικαστικές εγγυήσεις σύμφωνα με τις απαιτήσεις της ευρωπαϊκής νομοθεσίας.

4.1) Είδος Πρόσβασης

Η παρούσα Πολιτική είναι αναρτημένη στο Process Web και στην ιστοσελίδα της Εταιρείας και ελεύθερα προσβάσιμη από όλο το απασχολούμενο προσωπικό της Εταιρείας, συνεργάτες και πελάτες.

ΜΕΡΟΣ ΔΕΥΤΕΡΟ - Γενικές Αρχές

Κεφάλαιο 1 – Διαφάνεια στην Επεξεργασία Δεδομένων

5) Δικαίωμα Ενημέρωσης

Τα υποκείμενα των δεδομένων ενημερώνονται σχετικά με τον τρόπο χρήσης των προσωπικών τους δεδομένων σύμφωνα με την ισχύουσα νομοθεσία και τους παρακάτω όρους:

6) Περιεχόμενο και Μορφή Ενημέρωσης

(1) Η εταιρεία ενημερώνει επαρκώς τα υποκείμενα των δεδομένων για τα εξής στοιχεία:

- a. Την ταυτότητα του εκτελούντος την επεξεργασία (ή των εκτελούντων την επεξεργασία) και τα στοιχεία επικοινωνίας του (τους).
- b. την προβλεπόμενη χρήση και τον σκοπό χρήσης των δεδομένων και συγκεκριμένα ποια δεδομένα καταγράφονται και / ή είναι αντικείμενο επεξεργασίας/ ή χρησιμοποιούνται, για ποιο σκοπό και για ποιο χρονικό διάστημα.
- c. Εάν προσωπικά δεδομένα διαβιβάζονται σε τρίτα μέρη, το υποκείμενο των δεδομένων ενημερώνεται για τον αποδέκτη, το εύρος και τον σκοπό της διαβίβασης.
- d. Τα δικαιώματα του υποκειμένου σχετικά με τη χρήση των δεδομένων του.

(2) Ανεξάρτητα από το μέσο παροχής της ενημέρωσης, οι σχετικές πληροφορίες θα πρέπει να παρέχονται στο υποκείμενο των δεδομένων σε σαφή και κατανοητή μορφή.

7) Διαθεσιμότητα της Ενημέρωσης

Η ενημέρωση είναι διαθέσιμη στα υποκείμενα των δεδομένων, όταν τα δεδομένα συλλέγονται για πρώτη φορά και ακολούθως, οποτεδήποτε αυτή ζητηθεί.

Κεφάλαιο 2 – Κανόνες Αποδεκτής Χρήσης Προσωπικών Δεδομένων

8) Αρχή

Τα προσωπικά δεδομένα χρησιμοποιούνται μόνον υπό τους ακόλουθους όρους και δεν πρέπει να χρησιμοποιούνται για σκοπούς άλλους από εκείνους για τους οποίους συλλέχθηκαν αρχικά.

Η χρήση των συλλεγόμενων δεδομένων για άλλους σκοπούς, επιτρέπεται μόνο εάν πληρούνται οι προϋποθέσεις αποδεκτής χρήσης σε συμφωνία με τις ακόλουθες προϋποθέσεις.

9) Προϋποθέσεις Αποδεκτής Χρήσης Προσωπικών Δεδομένων

Τα προσωπικά δεδομένα μπορούν να χρησιμοποιηθούν εάν μια ή περισσότερες από τις ακόλουθες προϋποθέσεις πληρούνται:

- a) Η ισχύουσα νομοθεσία σαφώς επιτρέπει την χρήση των προσωπικών δεδομένων για τον συγκεκριμένο σκοπό.
- b) Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για τη χρήση των δεδομένων του.
- c) Είναι απαραίτητη η χρήση των δεδομένων με τον τρόπο αυτό, ώστε η εταιρεία να εκπληρώσει τις συμβατικές υποχρεώσεις της προς το υποκείμενο των δεδομένων ή για να υλοποιήσει μέτρα για την έναρξη ή επεξεργασία σύμβασης που έχει ζητηθεί από το υποκείμενο των δεδομένων.
- d) Τα δεδομένα χρησιμοποιούνται για να εκπληρωθεί νομική υποχρέωση της εταιρείας.
- e) Είναι απαραίτητη η χρήση των δεδομένων για τη διασφάλιση ζωτικών συμφερόντων του υποκειμένου των δεδομένων.
- f) Είναι απαραίτητη η χρήση των δεδομένων για να ολοκληρωθεί ένα έργο δημοσίου συμφέροντος ή έργο που αποτελεί μέρος άσκησης δημόσιας εξουσίας και η εταιρεία ή το τρίτο μέρος στο οποίο μεταφέρονται τα δεδομένα έχει επιφορτιστεί με την εκτέλεσή του συγκεκριμένου έργου.

Είναι απαραίτητη η επεξεργασία των δεδομένων, για τη διαφύλαξη των νόμιμων συμφερόντων της εταιρείας ή του τρίτου μέρους στο οποίο πραγματοποιείται η διαβίβαση των δεδομένων, υπό την προϋπόθεση ότι τα συμφέροντα του υποκειμένου των δεδομένων δεν υπερτερούν προφανώς των συμφερόντων της εταιρείας.

10) Συγκατάθεση του υποκειμένου των δεδομένων

Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του σύμφωνα με την παράγραφο § 9, εδάφιο b) των εν λόγω BCRP, εφόσον:

- a) Η συγκατάθεση έχει δοθεί ρητά, οικειοθελώς και κατόπιν ενημέρωσης του υποκειμένου, με τρόπο τέτοιο ώστε το υποκείμενο των δεδομένων να γνωρίζει τον σκοπό της συγκατάθεσης. Το κείμενο της δήλωσης συγκατάθεσης είναι ακριβές και ενημερώνει τα υποκείμενα των δεδομένων για το δικαίωμά τους να αποσύρουν τη συγκατάθεσή τους οποιαδήποτε στιγμή. Σε περίπτωση που η άρση της συγκατάθεσης συνεπάγεται την μη εκπλήρωση των συμβατικών υποχρεώσεων, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται σχετικά.
- b) Η συναίνεση έχει ληφθεί σε μορφή κατάλληλη για την περίπτωση (εγγράφως). Σε εξαιρετικές περιπτώσεις, μπορεί να ληφθεί και προφορική συγκατάθεση, εάν καταγραφούν επαρκώς το γεγονός της παροχής συγκατάθεσης, καθώς και οι ειδικές περιστάσεις, που καθιστούν την προφορική συγκατάθεση επαρκή

11) Αυτοματοποιημένη Χρήση Προσωπικών Δεδομένων

- a) Οι αποφάσεις που αξιολογούν επιμέρους πτυχές ενός ατόμου και οι οποίες ενδέχεται να επιφέρουν νομικές συνέπειες ή σημαντικό αρνητικό αντίκτυπο, δεν πρέπει να βασίζονται αποκλειστικά σε αυτοματοποιημένη χρήση προσωπικών δεδομένων. Αυτό περιλαμβάνει, ιδίως, αποφάσεις σχετικά με την φερεγγυότητα, επαγγελματική καταλληλότητα ή την κατάσταση της υγείας του υποκειμένου των δεδομένων.
- b) Εάν, σε μεμονωμένες περιπτώσεις, υπάρχει αντικειμενική ανάγκη για αυτοματοποιημένη χρήση προσωπικών δεδομένων, το υποκείμενο των δεδομένων ενημερώνεται χωρίς καθυστέρηση για το αποτέλεσμα της αυτοματοποιημένης επεξεργασίας, και του δίνεται η δυνατότητα να υποβάλει τις παρατηρήσεις του εντός της κατάλληλης χρονικής περιόδου. Τα σχόλια του υποκειμένου των δεδομένων, λαμβάνονται υπόψη πριν την τελική απόφαση.

12) Χρήση Προσωπικών Δεδομένων με Σκοπό την Απευθείας Προώθηση Προϊόντων/ Υπηρεσιών

Σε περίπτωση που δεδομένα χρησιμοποιούνται για σκοπούς απευθείας εμπορικής προώθησης προϊόντων/υπηρεσιών, τα υποκείμενα των δεδομένων πρέπει να:

- a) Ενημερώνονται για τον τρόπο με τον οποίο τα δεδομένα θα χρησιμοποιηθούν για την προώθηση προϊόντων/υπηρεσιών
- b) Ενημερώνονται για το δικαίωμά τους να προβάλλουν αντιρρήσεις στην χρήση των δεδομένων τους για τους σκοπούς αυτούς.
- c) Τους δίνονται τα κατάλληλα εργαλεία για την άσκηση του δικαιώματός τους αυτού. Συγκεκριμένα, θα πρέπει να λαμβάνουν πληροφορίες για την εταιρεία, στην οποία μπορούν να υποβάλλουν το αίτημα αντίρρησής τους.

13) Ειδικές Κατηγορίες Προσωπικών Δεδομένων (ευαίσθητα προσωπικά δεδομένα)

- a) Η χρήση ειδικών κατηγοριών προσωπικών δεδομένων επιτρέπεται μόνο εάν αυτή προβλέπεται από την ισχύουσα νομοθεσία ή εφόσον το υποκείμενο έχει δώσει εκ των προτέρων τη ρητή συγκατάθεσή του. Επίσης, επιτρέπεται η επεξεργασία τους σε περίπτωση που αυτή είναι απαραίτητη για την εκπλήρωση υποχρεώσεων, που πηγάζουν από την εργατική νομοθεσία, υπό την προϋπόθεση ότι αυτό επιτρέπεται από το εκάστοτε ισχύον εθνικό δίκαιο και λαμβάνονται κατάλληλα μέτρα προστασίας τους.
- b) Πριν από την έναρξη της συλλογής, επεξεργασίας ή χρήσης ευαίσθητων προσωπικών δεδομένων, η εταιρεία ενημερώνει σχετικά τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων και καταγράφει το γεγονός. Κατά την αξιολόγηση της αποδεκτής χρήσης των δεδομένων, ιδιαίτερη προσοχή πρέπει να δοθεί στη φύση, το εύρος, το σκοπό, την αναγκαιότητα και τη νομική βάση της χρήσης των ευαίσθητων προσωπικών δεδομένων.

14) Ελαχιστοποίηση Χρήσης, Αποφυγή Χρήσης, Χρήση Ανώνυμων και Ψευδώνυμων Δεδομένων

1. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με τον σκοπό χρήσης τους (ελαχιστοποίηση χρήσης δεδομένων – data minimization). Τα δεδομένα υποβάλλονται σε επεξεργασία μόνον στα πληροφοριακά συστήματα που είναι απαραίτητα για την εκπλήρωση του σκοπού χρήσης των δεδομένων (αποφυγή χρήσης δεδομένων – data avoidance).

2. Όπου αυτό είναι εφικτό και οικονομικά εύλογο, χρησιμοποιούνται διαδικασίες για τη διαγραφή στοιχείων ταυτοποίησης των υποκειμένων των δεδομένων (χρήση ανώνυμων δεδομένων - anonymization) ή αντικατάστασή τους με άλλα χαρακτηριστικά (χρήση ψευδώνυμων δεδομένων - aliasing).

15) Απαγόρευση Δέσμευσης

Τα προϊόντα και οι υπηρεσίες δεν πρέπει να παρέχονται υπό την προϋπόθεση ότι το υποκείμενο των δεδομένων συναινεί στην επεξεργασία των προσωπικών του δεδομένων για σκοπούς άλλους από αυτούς που προβλέπονται κατά την σύναψη σύμβασης ή για την εκπλήρωση των συμβατικών υποχρεώσεων των μερών. Η απαγόρευση αυτή ισχύει μόνο εάν δεν είναι δυνατόν ή δεν είναι ευλόγως δυνατόν στο υποκείμενο των δεδομένων να χρησιμοποιήσει παρόμοια προϊόντα ή παρόμοιες υπηρεσίες.

Κεφάλαιο 3- Διαβίβαση Προσωπικών Δεδομένων

16) Φύση και Σκοπός της Διαβίβασης Προσωπικών Δεδομένων

- (1) Τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται μόνον εφόσον ο αποδέκτης των δεδομένων αναλαμβάνει την ευθύνη για τα δεδομένα που λαμβάνει ή όταν ο αποδέκτης χρησιμοποιεί τα δεδομένα αποκλειστικά σύμφωνα με τις οδηγίες και τις απαιτήσεις του αποστολέα (συμφωνία ανάθεσης επεξεργασίας δεδομένων - commissioned data processing agreement).
- (2) Τα δεδομένα προσωπικού χαρακτήρα επιτρέπεται να διαβιβάζονται μόνο για τους σκοπούς που περιγράφονται στην παράγραφο 9 των παρόντων BCRP στο πλαίσιο των επιχειρηματικών δραστηριοτήτων της εταιρείας ή εξαιτίας σχετικής νομικής υποχρέωσης ή μετά από τη συγκατάθεση των υποκειμένων των δεδομένων.

17) Διαβίβαση Δεδομένων

- 1) Αν η εταιρεία διαβιβάσει δεδομένα σε μέρη που έχουν την έδρα τους σε τρίτη χώρα ή σε μέρη που διαβιβάζουν δεδομένα εκτός εθνικών συνόρων, λαμβάνονται κατάλληλα μέτρα για να διασφαλιστεί ότι τα δεδομένα διαβιβάζονται κατάλληλα. Οι απαιτήσεις προστασίας και ασφάλειας των δεδομένων συμφωνούνται με τον αποδέκτη των δεδομένων πριν την διαβίβασή τους. Επιπλέον, τα δεδομένα προσωπικού χαρακτήρα, ιδίως τα στοιχεία που συλλέγονται στην ΕΕ ή στον ΕΟΧ, μπορούν να διαβιβάζονται σε υπεύθυνους επεξεργασίας εκτός Ευρωπαϊκής Ένωσης, μόνο εάν διασφαλίζεται το κατάλληλο επίπεδο προστασίας των προσωπικών δεδομένων με τη εφαρμογή των BCRP ή άλλων κατάλληλων μέτρων, όπως το πρότυπο της ΕΕ περί συμβατικών ρητρών ή μέσω συμβάσεων, που πληρούν τις σχετικές απαιτήσεις της ευρωπαϊκής νομοθεσίας.
- 2) Κατά τη διαβίβασή προσωπικών δεδομένων σε τρίτο μέρος εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας τους με βάση τις απαιτήσεις του Ομίλου Deutsche Telekom και τα ευρέως αποδεκτά τεχνικά και οργανωτικά πρότυπα.

18) Ανάθεση Επεξεργασίας των Δεδομένων

- 1) Όταν η εταιρεία (πελάτης) αναθέτει σε τρίτο μέρος (ανάδοχο) την παροχή υπηρεσιών για λογαριασμό της και σύμφωνα με τις οδηγίες της, τότε συμπληρωματικά στη σύμβαση παροχής υπηρεσιών που καθορίζει το αντικείμενο της υπηρεσίας, η σύμβαση πρέπει να αναφέρεται στις υποχρεώσεις του ανάδοχου αναφορικά με την επεξεργασία των προσωπικών δεδομένων που αναλαμβάνει. Οι εν λόγω υποχρεώσεις πρέπει να περιλαμβάνουν τις οδηγίες του πελάτη σχετικά με τον τύπο και τον τρόπο της επεξεργασίας των προσωπικών δεδομένων, τον σκοπό της επεξεργασίας και τα τεχνικά και οργανωτικά μέτρα που απαιτούνται για την προστασία τους.
- 2) Ο ανάδοχος δεν πρέπει να χρησιμοποιεί τα προσωπικά δεδομένα (που του έχουν διαβιβαστεί για την εκτέλεση της σύμβασης) για σκοπούς δικούς του ή άλλων τρίτων μερών, χωρίς την προηγούμενη συγκατάθεση του πελάτη. Ο ανάδοχος πρέπει να ενημερώνει τον πελάτη εκ των προτέρων σε περίπτωση που σχεδιάζει να χρησιμοποιήσει υπεργολάβους, προκειμένου να εκπληρώσει τις συμβατικές του υποχρεώσεις. Ο πελάτης πρέπει να έχει το δικαίωμα να αρνηθεί την χρήση υπεργολάβων. Σε περίπτωση υπεργολαβίας, ο ανάδοχος οφείλει να υποχρεώνει τον υπεργολάβο του να συμμορφώνονται με τις απαιτήσεις, που έχουν συμφωνηθεί στην σύμβαση μεταξύ αναδόχου και πελάτη.
- 3) Οι ανάδοχοι πρέπει να επιλέγονται βάσει της ικανότητάς τους να πληρούν τις προαναφερθείσες απαιτήσεις.

Κεφάλαιο 4 – Ποιότητα & Ασφάλεια Δεδομένων

19) Ποιότητα στην Επεξεργασία των Δεδομένων

- (1) Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι σωστά και όπου είναι αναγκαίο να τηρούνται ενημερωμένα (ποιότητα των δεδομένων).
- (2) Ανάλογα με τον σκοπό για τον οποίο χρησιμοποιούνται τα δεδομένα, λαμβάνονται τα κατάλληλα μέτρα ώστε να διασφαλίζεται ότι κάθε λανθασμένη ή ελλιπής πληροφορία διαγράφεται, εμποδίζεται η χρήση της ή, αν είναι απαραίτητο, διορθώνεται.

20) Ασφάλεια Δεδομένων – Τεχνικά και Οργανωτικά Μέτρα

Η εταιρεία προβλέπει στις εταιρικές διαδικασίες τα κατάλληλα τεχνικά και οργανωτικά μέτρα και τα εφαρμόζει στα συστήματα πληροφορικής και τις πλατφόρμες, οι οποίες χρησιμοποιούνται για τη συλλογή, επεξεργασία ή χρήση δεδομένων με σκοπό την προστασία τους.

Τα μέτρα αυτά πρέπει να περιλαμβάνουν:

- a) μέτρα για την αποτροπή πρόσβασης μη εξουσιοδοτημένων ατόμων στα συστήματα επεξεργασίας δεδομένων (έλεγχος άδειας εισόδου).
- b) μέτρα που εξασφαλίζουν ότι τα συστήματα επεξεργασίας δεδομένων δεν μπορούν να χρησιμοποιηθούν από μη εξουσιοδοτημένα πρόσωπα (έλεγχος άρνησης πρόσβασης).
- c) μέτρα που εξασφαλίζουν ότι τα πρόσωπα που είναι εξουσιοδοτημένα να χρησιμοποιούν τα συστήματα επεξεργασίας δεδομένων έχουν πρόσβαση αποκλειστικά και μόνο στα δεδομένα για τα οποία έχουν εξουσιοδοτηθεί και ότι τα προσωπικά δεδομένα δεν μπορούν, κατά τη διάρκεια της επεξεργασίας ή της χρήσης ή μετά από την καταγραφή τους, να διαβαστούν, να αντιγραφούν, να αλλαχθούν ή να διαγραφούν από μη εξουσιοδοτημένα πρόσωπα (έλεγχος πρόσβασης στα δεδομένα).
- d) μέτρα που εξασφαλίζουν ότι, κατά τη διάρκεια της ηλεκτρονικής διαβίβασης ή κατά τη διάρκεια της μεταφοράς ή της καταγραφής των δεδομένων, τα προσωπικά δεδομένα δεν μπορούν να διαβαστούν, αντιγραφούν, αλλαχθούν ή αφαιρεθούν από μη εξουσιοδοτημένα πρόσωπα, και ότι είναι δυνατό να ελεγχθούν και να εξακριβωθούν οι εκτελούντες την επεξεργασία, στους οποίους έχουν μεταβιβαστεί προσωπικά δεδομένα μέσω εξοπλισμού μετάδοσης δεδομένων (έλεγχος διαβίβασης δεδομένων).
- e) μέτρα που διασφαλίζουν ότι είναι δυνατό αναδρομικά να εξεταστεί και να εξακριβωθεί εάν και από ποιόν εισήχθησαν, τροποποιήθηκαν ή διαγράφηκαν προσωπικά δεδομένα στα συστήματα επεξεργασίας δεδομένων (έλεγχος εισόδου δεδομένων).
- f) μέτρα που διασφαλίζουν ότι τα προσωπικά δεδομένα που επεξεργάζονται τρίτα μέρη/ανάδοχοι τυγχάνουν επεξεργασίας μόνο σύμφωνα με τις οδηγίες του πελάτη (έλεγχος αναδόχου).
- g) μέτρα που διασφαλίζουν ότι τα προσωπικά δεδομένα προστατεύονται από τυχαία καταστροφή ή απώλεια (έλεγχος διαθεσιμότητας).
- h) μέτρα που διασφαλίζουν ότι τα δεδομένα που έχουν συλλεχθεί για διαφορετικούς σκοπούς μπορούν να υποβληθούν σε επεξεργασία ξεχωριστά (κανόνας διαχωρισμού).

ΜΕΡΟΣ ΤΡΙΤΟ- ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

21) Δικαίωμα Ενημέρωσης

(1) Τα υποκείμενα των δεδομένων έχουν δικαίωμα να επικοινωνούν οποιαδήποτε στιγμή με οποιαδήποτε εταιρία επεξεργάζεται τα δεδομένα τους και να ζητούν τις παρακάτω πληροφορίες:

- a) ποια προσωπικά του δεδομένα διατηρεί η εν λόγω εταιρεία καθώς και την προέλευση και τους αποδέκτες αυτών
- b) το σκοπό χρήσης
- c) τα πρόσωπα και τους υπεύθυνους επεξεργασίας, στους οποίους τα δεδομένα διαβιβάζονται τακτικά, ιδίως εάν τα δεδομένα διαβιβάζονται στο εξωτερικό
- d) τις διατάξεις των παρόντων BCRP

(2) Οι σχετικές πληροφορίες θα πρέπει να καθίστανται διαθέσιμες στον αιτούντα σε κατανοητή μορφή και εντός εύλογου χρονικού διαστήματος. Αυτό επιτυγχάνεται εν γένει με έντυπη ή ηλεκτρονική επικοινωνία. Η παροχή αντιγράφου των BCRP στον αιτούντα θεωρείται επαρκής ενημέρωση σχετικά με τις απαιτήσεις που προβλέπονται από το κείμενο αυτό.

Εάν αυτό επιτρέπεται από την εθνική νομοθεσία, η εταιρεία μπορεί να χρεώνει ένα ποσό για την παροχή των σχετικών πληροφοριών.

22) Δικαίωμα Αντίρρησης, Δικαίωμα Διαγραφής ή Αποκλεισμού των Δεδομένων/ Δικαίωμα Διόρθωσης

- (1) Το υποκείμενο των δεδομένων έχει δικαίωμα να προβάλλει οποτεδήποτε αντιρρήσεις για την χρήση των προσωπικών του δεδομένων, αν τα δεδομένα αυτά χρησιμοποιούνται για σκοπούς που δεν επιβάλλονται από την νομοθεσία.
- (2) Το δικαίωμα αντίρρησης ισχύει ακόμα και αν το υποκείμενο παρείχε σε προηγούμενη περίπτωση τη συγκατάθεσή του για την χρήση των δεδομένων του.
- (3) Νόμιμα αιτήματα διαγραφής ή αποκλεισμού χρήσης των προσωπικών δεδομένων πρέπει να ικανοποιούνται άμεσα. Ως νόμιμα θεωρούνται ιδίως τα αιτήματα, που αφορούν στην διαγραφή των δεδομένων, εάν η νομική βάση της επεξεργασίας των προσωπικών δεδομένων έπαυσε να ισχύει. Εάν το υποκείμενο των δεδομένων έχει το δικαίωμα να διαγραφούν τα δεδομένα του, αλλά η διαγραφή τους δεν είναι δυνατή, τότε τα δεδομένα πρέπει να προστατεύονται από μη επιτρεπόμενη χρήση αποκλείοντας την πρόσβαση. Οι περίοδοι διατήρησης των προσωπικών δεδομένων, που προβλέπονται από την εθνική νομοθεσία κάθε εταιρίας, πρέπει να τηρούνται.
- (4) Τα υποκείμενα των δεδομένων μπορούν να ζητήσουν από την εταιρεία να διορθώσει τα προσωπικά δεδομένα που διατηρεί ανά πάσα στιγμή, εφόσον τα δεδομένα αυτά είναι ελλιπή ή / και ανακριβή.
- (5) Το υποκείμενο των δεδομένων ενημερώνεται σε περίπτωση που η ανάκληση της συναίνεσής του ή η διαγραφή των προσωπικών του δεδομένων οδηγεί σε μη εκπλήρωση συμβατικών υποχρεώσεων.

23) Δικαίωμα Υποβολής Αιτήματος για Παροχή Διευκρινίσεων, Παρατηρήσεων και Αποκατάστασης Σχολιασμού

- (1) Εάν το υποκείμενο των δεδομένων ισχυρίζεται ότι τα δικαιώματά του έχουν παραβιαστεί λόγω παράνομης χρήσης των δεδομένων του, ιδίως με την παροχή αποδεικτικών στοιχείων που επαληθεύουν την παραβίαση των BCRP, οι αρμόδιες εταιρίες πρέπει να αποσαφηνίζουν τα

πραγματικά περιστατικά χωρίς υπαίτια καθυστέρηση. Για τα δεδομένα που μεταφέρονται σε επιχειρήσεις εκτός της Ευρωπαϊκής Ένωσης, η εταιρεία με έδρα στην Ευρωπαϊκή Ένωση πρέπει να διευκρινίζει τα γεγονότα και να παρέχει στοιχεία, που να αποδεικνύουν ότι ο αποδέκτης των δεδομένων δεν έχει παραβιάσει τις απαιτήσεις των BCRP, διαφορετικά είναι υπεύθυνη για κάθε ζημία που έχει προκληθεί. Οι εταιρείες πρέπει να συνεργάζονται στενά για να αποσαφηνίσουν τα πραγματικά περιστατικά και να παρέχουν αμοιβαία πρόσβαση σε όλες τις πληροφορίες που απαιτούνται για την εξακρίβωση των πραγματικών περιστατικών της υπόθεσης.

- (2) Το υποκείμενο των δεδομένων μπορεί οποτεδήποτε να υποβάλει καταγγελία κατά της Deutsche Telekom Group Holding, αν υποψιάζεται ότι μια εταιρεία του Ομίλου Deutsche Telekom δεν επεξεργάζεται τα προσωπικά του δεδομένα σύμφωνα με την νομοθεσία ή τις διατάξεις των εν λόγω BCRP. Οι τεκμηριωμένες καταγγελίες θα εξετάζονται εντός εύλογου χρονικού διαστήματος και το υποκείμενο των δεδομένων θα ενημερώνεται σχετικά.
- (3) Αν η καταγγελία αφορά περισσότερες από μια εταιρείες του Ομίλου, ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων της Εταιρείας, που σχετίζεται περισσότερο με το θέμα, συντονίζει όλη τη σχετική επικοινωνία με το υποκείμενο των δεδομένων. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου δικαιούται να ασκήσει τις εξουσίες υποκατάστασης και να προβεί σε ενέργειες ανά πάσα στιγμή.
- (4) Πρέπει να υπάρχουν κατάλληλα κανάλια επικοινωνίας για την αναφορά περιστατικών περί προστασίας προσωπικών δεδομένων (π.χ. ειδικός λογαριασμός ηλεκτρονικού ταχυδρομείου).
- (5) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων της Εταιρείας ενημερώνει τον Υπεύθυνο Προστασίας Δεδομένων του Ομίλου για κάθε περιστατικό παραβίασης προσωπικών δεδομένων χωρίς καθυστέρηση εφαρμόζοντας τις σχετικές διαδικασίες υποβολής αναφορών.
- (6) Τα υποκείμενα των δεδομένων μπορούν να υποβάλουν αίτηση σύμφωνα με το Κεφάλαιο 5 των παρόντων BCRP, αν έχουν παραβιαστεί τα δικαιώματά τους ή αν έχουν υποστεί ζημία.

24) Δικαίωμα Υποβολής Ερωτήσεων και Παραπόνου

Κάθε υποκείμενο των δεδομένων έχει το δικαίωμα ανά πάσα στιγμή να επικοινωνήσει με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων της εταιρείας, που χρησιμοποιεί τα προσωπικά του δεδομένα καταθέτοντας ερωτήσεις και παράπονα σχετικά με την εφαρμογή των BCRP. Η εταιρεία που σχετίζεται περισσότερο με την εκάστοτε συγκεκριμένη περίπτωση ή η εταιρεία που συνέλεξε τα δεδομένα του υποκειμένου των δεδομένων διασφαλίζει ότι τα δικαιώματα του υποκειμένου των δεδομένων προστατεύονται επαρκώς από τις άλλες εταιρείες.

25) Τρόπος Άσκησης των Δικαιωμάτων των Υποκειμένων

Τα υποκείμενα των προσωπικών δεδομένων δεν θα υφίστανται διακριτική μεταχείριση, εξαιτίας του γεγονότος ότι έκαναν χρήση των προαναφερομένων δικαιωμάτων. Ο τρόπος επικοινωνίας με το υποκείμενο των δεδομένων, π.χ. τηλεφωνικά, ηλεκτρονικά ή εγγράφως, πρέπει να επιλέγεται, όπου αυτό είναι εφικτό, ανάλογα με το αίτημα του υποκειμένου των δεδομένων.

26) Αντίγραφο των BCRP

Αντίγραφο των BCRP σε έντυπη μορφή παρέχεται σε οποιονδήποτε το αιτηθεί.

ΜΕΡΟΣ ΤΕΤΑΡΤΟ - ΔΙΟΙΚΗΤΙΚΗ ΟΡΓΑΝΩΣΗ

27) Αρμοδιότητα για την Επεξεργασία Δεδομένων

Οι εταιρείες υποχρεούνται να διασφαλίζουν τη συμμόρφωση με την νομοθεσία για την προστασία των δεδομένων και με τους παρόντες BCRP.

28) Υπεύθυνος Προστασίας Προσωπικών Δεδομένων

- (1) Κάθε εταιρεία ορίζει έναν ανεξάρτητο Υπεύθυνο Προστασίας Προσωπικών Δεδομένων, του οποίου καθήκον είναι να διασφαλίζει ότι όλες οι επιμέρους οργανωτικές μονάδες της εταιρείας ενημερώνονται για την ισχύουσα νομοθεσία και τις εσωτερικές απαιτήσεις του Ομίλου Deutsche Telekom αναφορικά με την διαχείριση των προσωπικών δεδομένων και ειδικότερα για τους BCRP. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων χρησιμοποιεί τα κατάλληλα μέτρα, όπως έκτακτους ελέγχους, προκειμένου να διαπιστώσει την συμμόρφωση με τους κανόνες της προστασίας των προσωπικών δεδομένων.
- (2) Η εταιρεία συμβουλευεται τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου Deutsche Telekom πριν τον διορισμό του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων της εταιρείας.
- (3) Η εταιρεία διασφαλίζει ότι ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων διαθέτει την κατάλληλη τεχνογνωσία για την αξιολόγηση των νομικών, τεχνικών και οργανωτικών θεμάτων που σχετίζονται με τα μέτρα προστασίας των προσωπικών δεδομένων.
- (4) Η εταιρεία οφείλει να παρέχει στον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων τους απαραίτητους οικονομικούς και ανθρώπινους πόρους που απαιτούνται για την εκτέλεση των καθηκόντων του.
- (5) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων αναφέρεται άμεσα στην διοίκηση της εταιρείας και συνδέεται οργανωτικά με αυτήν.
- (6) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων είναι υπεύθυνος για την υλοποίηση των απαιτήσεων του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων του Ομίλου Deutsche Telekom και της στρατηγικής περί προστασίας δεδομένων του Ομίλου Deutsche Telekom.
- (7) Όλες οι οργανωτικές μονάδες κάθε εταιρείας υποχρεούνται να ενημερώνουν τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων για τυχόν εξελίξεις στην υποδομή πληροφορικής, στην υποδομή δικτύου, τα επιχειρηματικά μοντέλα, τα προϊόντα, την επεξεργασία δεδομένων προσωπικού και τα αντίστοιχα στρατηγικά σχέδια. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων πρέπει να ενημερώνεται για τις νέες εξελίξεις σε αρχικό στάδιο, προκειμένου να διασφαλιστεί ότι τυχόν ζητήματα προστασίας των προσωπικών δεδομένων θα εξεταστούν και θα αξιολογηθούν.

29) Υπεύθυνος Προστασίας Προσωπικών Δεδομένων Ομίλου

- (1) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου συντονίζει τις διαδικασίες συνεργασίας και συμφωνιών σε όλα τα σημαντικά θέματα που αφορούν την προστασία των δεδομένων εντός του Ομίλου Deutsche Telekom. Επιπλέον ενημερώνει το Διευθύνοντα Σύμβουλο της Deutsche Telekom Group Holding για τις τρέχουσες εξελίξεις και συντάσσει συστάσεις όπου είναι αναγκαίο.
- (2) Η ανάπτυξη και εξέλιξη της πολιτικής του Ομίλου της Deutsche Telekom σχετικά με την προστασία των προσωπικών δεδομένων αποτελεί αρμοδιότητα του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων του Ομίλου, ο οποίος ενεργεί αφού συμβουλευθεί τους Υπευθύνους

Προστασίας Προσωπικών Δεδομένων των εταιρειών του Ομίλου, όπου είναι αναγκαίο. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων αναπτύσσει την πολιτική προστασίας προσωπικών δεδομένων για την εταιρία του λαμβάνοντας υπόψη την πολιτική του Ομίλου. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου και οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων των εταιρειών συναντιούνται σε ετήσια βάση στις Διεθνείς Συναντήσεις Υπευθύνων Προστασίας Προσωπικών Δεδομένων (International Privacy Leader Meetings) και ανταλλάσσουν πληροφορίες.

30) Καθήκον Ενημέρωσης σε Περίπτωση Παραβίασης

Η εταιρεία πρέπει να ενημερώνει άμεσα τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων για κάθε παραβίαση ή σαφή ένδειξη παραβίασης των κανονισμών προστασίας προσωπικών δεδομένων και κυρίως των παρόντων BCRP. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων ενημερώνει άμεσα τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου αν το περιστατικό ενδέχεται να έχει επιπτώσεις στο κοινό, επηρεάζει περισσότερες από μία εταιρεία του Ομίλου, ή συνεπάγεται οικονομική ζημία άνω των 500.000 ευρώ. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων ενημερώνει επίσης τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου εάν τυχόν έχουν γίνει τροποποιήσεις στην ισχύουσα νομοθεσία και η νέα ισχύουσα νομοθεσία έρχεται σε σύγκρουση με τους παρόντες BCRP.

31) Επιθεώρηση του Επιπέδου Προστασίας Δεδομένων

- (1) Επιθεώρηση του επιπέδου συμμόρφωσης με τις απαιτήσεις των BCRP και του επιπέδου της προστασίας των προσωπικών δεδομένων διενεργείται από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου ως μέρος του ετήσιου πλάνου ελέγχων, καθώς και μέσω άλλων μέτρων, όπως επιθεωρήσεις που διενεργούνται από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων των εταιριών και την υποβολή εκθέσεων.
- (2) Εσωτερικοί και εξωτερικοί ελεγκτές διενεργούν ελέγχους εκ μέρους του Υπευθύνου Προστασίας Προσωπικών Δεδομένων του Ομίλου. Περιοδικές αυτό-αξιολογήσεις πρέπει επίσης να διενεργούνται εντός του Ομίλου Deutsche Telekom και συντονίζονται από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου. Ο Διευθύνων Σύμβουλος του Ομίλου της Deutsche Telekom Group Holding πρέπει να ενημερώνεται για τα αποτελέσματα των βασικών ελέγχων και των συμφωνηθέντων μέτρων. Η αρμόδια εποπτική Αρχή λαμβάνει αντίγραφο των αποτελεσμάτων των ελέγχων κατόπιν υποβολής σχετικού αιτήματος. Η αρμόδια εποπτική Αρχή μπορεί επίσης να πραγματοποιήσει έλεγχο. Η εταιρεία οφείλει να συνεργάζεται κατά την διάρκεια των ελέγχων και να υλοποιεί τα μέτρα που προκύπτουν από αυτούς.
- (3) Η εταιρεία λαμβάνει τα κατάλληλα μέτρα για την αντιμετώπιση τυχόν αδυναμιών που εντοπίζονται κατά τη διάρκεια των ελέγχων, και ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου παρακολουθεί την υλοποίηση των μέτρων αυτών. Εάν η εταιρεία αδυνατεί να εφαρμόσει τα μέτρα, χωρίς επαρκή αιτιολογία, ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου αξιολογεί τις επιπτώσεις στην προστασία των προσωπικών δεδομένων και προβαίνει στις απαραίτητες ενέργειες, κλιμακώνοντας τα θέματα εφόσον είναι αναγκαίο.
- (4) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου ή άλλες οργανωτικές μονάδες στις οποίες έχει αυτό ανατεθεί, διενεργούν ελέγχους με βάση ένα καταγεγραμμένο πλάνο με σκοπό να διαπιστώνεται εάν η εταιρία συμμορφώνεται με τις απαιτήσεις προστασίας των δεδομένων.
- (5) Αν αυτό δεν απαγορεύεται από την ισχύουσα νομοθεσία, ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου και οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων επιτρέπεται να ελέγχουν σε όλες τις εταιρίες και στη δική τους εταιρία αντίστοιχα εάν τα προσωπικά δεδομένα χρησιμοποιούνται ορθώς. Οι εταιρείες πρέπει να χορηγούν στον

Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου και στους Υπεύθυνους Προστασίας Προσωπικών Δεδομένων πλήρη πρόσβαση στις πληροφορίες που απαιτούνται για την αξιολόγηση της κατάστασης. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου και οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων των εταιρειών έχουν το δικαίωμα να εκδίδουν σχετικές οδηγίες.

- (6) Ως μέρος των επιθεωρήσεων, οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων των εταιρειών πρέπει να χρησιμοποιούν τυποποιημένες διαδικασίες εγκεκριμένες για όλο τον Όμιλο, π.χ. κοινός έλεγχος για την προστασία των δεδομένων, όπου αυτό είναι δυνατό. Τις διαδικασίες αυτές μπορεί να υποδείξει ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου.

32) Δέσμευση και Εκπαίδευση Εργαζομένων

- (1) Οι εταιρείες υποχρεώνουν τους υπαλλήλους τους να τηρούν την εμπιστευτικότητα των προσωπικών δεδομένων και το απόρρητο των τηλεπικοινωνιών με την σύναψη της σύμβασης εργασίας. Οι εργαζόμενοι λαμβάνουν επαρκή εκπαίδευση σε θέματα προστασίας προσωπικών δεδομένων. Η εταιρεία πρέπει να διαθέτει σχετικές διαδικασίες και να παρέχει τους πόρους για το σκοπό αυτό.
- (2) Οι εργαζόμενοι λαμβάνουν εκπαίδευση αναφορικά με τις βασικές αρχές της προστασίας των προσωπικών δεδομένων τουλάχιστον ανά διετία. Η εταιρεία αναπτύσσει ειδικά προγράμματα εκπαίδευσης για τους εργαζομένους της. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων κάθε εταιρείας τηρεί αρχείο με τις εκπαιδεύσεις, που έχουν πραγματοποιηθεί και ενημερώνει τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου σε ετήσια βάση.
- (3) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου μπορεί να διαθέτει τους πόρους και τις διαδικασίες κεντρικά με σκοπό την εκπαίδευση των υπαλλήλων του Ομίλου.

33) Συνεργασία με τις Εποπτικές Αρχές

- (1) Οι εταιρείες οφείλουν να συνεργάζονται, με την εποπτική Αρχή στην οποία υπάγονται οι ίδιες ή με την αρμόδια Αρχή στην οποία υπάγεται η εταιρεία που διαβιβάζει τα δεδομένα και ιδίως οφείλει να απαντάει σε ερωτήματα και να ακολουθεί τις συστάσεις τους.
- (2) Σε περίπτωση τροποποίησης της νομοθεσίας, η οποία έχει επηρεάζει σημαντικά την εφαρμογή των BCRP, η αρμόδια εταιρεία ενημερώνει σχετικά την αρμόδια εποπτική Αρχή.

34) Υπεύθυνος Επικοινωνίας για Ερωτήματα

Οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων ή ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου είναι αρμόδιοι για το χειρισμό ερωτημάτων σχετικά με τα BCRP. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου ενημερώνει σχετικά με τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Προσωπικών Δεδομένων των εταιρειών, κατόπιν αιτήματος.

Η επικοινωνία με τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου γίνεται σε εργάσιμες ώρες με τους παρακάτω τρόπους:

datenschutz@telekom.de

privacy@telekom.de

+49-228-181-82001

ΜΕΡΟΣ ΠΕΜΠΤΟ – ΕΥΘΥΝΗ

35) Πεδίο Εφαρμογής των Διατάξεων Περι Ευθύνης

- (1) Το Πέμπτο Μέρος των BCRP εφαρμόζεται αποκλειστικά για την επεξεργασία των προσωπικών δεδομένων που συλλέγονται στην ΕΕ / ΕΟΧ και εμπίπτει στο πεδίο εφαρμογής της οδηγίας 95/46/ΕΚ της ΕΕ για την προστασία των δεδομένων.
- (2) Εντός της ΕΕ / ΕΟΧ, εφαρμόζονται οι διατάξεις περί νομικής ευθύνης της χώρας στην οποία έχει την έδρα της η εταιρεία. Για τα δεδομένα που δεν εμπίπτουν στο άρθρο 35 παρ. 1 των BCRP, ισχύουν οι διατάξεις περί ευθύνης της χώρας στην οποία έχει την έδρα της η εταιρεία που συνέλεξε τα δεδομένα, ή αν δεν υπάρχει σχετική νομική πρόβλεψη, εφαρμόζονται οι όροι και οι προϋποθέσεις της εταιρείας που συνέλεξε τα δεδομένα.
- (3) Η καταβολή αποζημίωσης, η οποία υπερβαίνει την ζημία που έχει προκληθεί στο υποκείμενο των δεδομένων, αποκλείεται ρητά.

36) Αποζημίωση

1. Κάθε άτομο, που έχει υποστεί ζημία ως αποτέλεσμα παραβίασης μίας ή περισσοτέρων ρυθμίσεων των BCRP από εταιρία του Ομίλου Deutsche Telekom ή από αποδέκτη δεδομένων στον οποίο εταιρία του Ομίλου έχει διαβιβάσει δεδομένα, δικαιούται να διεκδικήσει αποζημίωση από τις εταιρείες του Ομίλου Deutsche Telekom.
2. Το υποκείμενο των δεδομένων έχει επίσης το δικαίωμα να ζητήσει αποζημίωση από την εταιρία Deutsche Telekom Group holding. Σε περίπτωση που η Deutsche Telekom Group holding καταβάλλει αποζημίωση έχει το δικαίωμα να στραφεί αναγωγικά κατά της εταιρείας, που είναι υπεύθυνη για την ζημία ή που συνεργάστηκε με τον τρίτο, που την προκάλεσε.
3. Το υποκείμενο των δεδομένων δικαιούται να διεκδικήσει αποζημίωση αρχικά από την εταιρεία που διαβίβασε τα δεδομένα. Εάν αυτή εταιρία δεν ευθύνεται de jure ή de facto (με βάση την ισχύουσα νομοθεσία ή με βάση τα πραγματικά περιστατικά), το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει αποζημίωση από την εταιρεία που ήταν αποδέκτης των δεδομένων. Η εταιρεία -αποδέκτης των δεδομένων σε περίπτωση παραβίασης δεν δικαιούται να αντικρούσει την ευθύνη της επικαλούμενη την ευθύνη του αναδόχου.
4. Το υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία στην αρμόδια εποπτική Αρχή ή στην εποπτική Αρχή που είναι αρμόδια για την Deutsche Telekom Group holding ανά πάσα στιγμή.

37) Βάρος Απόδειξης

Το βάρος απόδειξης αναφορικά με την ορθή χρήση των δεδομένων του υποκειμένου εναπόκειται στην υπεύθυνη εταιρεία.

38) Ρήτρα Υπέρ Τρίτου

Εάν το υποκείμενο των δεδομένων δεν δικαιούται να διεκδικήσει άμεσα αποζημίωση, μπορεί ως τρίτος να στραφεί κατά των εταιρειών που έχουν παραβιάσει τις συμβατικές τους υποχρεώσεις με βάση τις διατάξεις των παρόντων BCRP.

39) Αρμοδιότητα Δικαστηρίων

Το υποκείμενο των δεδομένων μπορεί να επιλέξει να διεκδικήσει αποζημίωση στα αρμόδια δικαστήρια:

- a) της χώρας που σχετίζεται άμεσα με το ενδιαφερόμενο άτομο ή
- b) της χώρας απ' όπου προέρχονται τα διαβιβασθέντα δεδομένα, ή
- c) της χώρας, όπου βρίσκονται τα κεντρικά γραφεία του Ομίλου στην Ε.Ε ή της εταιρείας μέλους του Group εντός της Ε.Ε, στην οποία έχουν ανατεθεί ειδικές αρμοδιότητες περί προστασίας των προσωπικών δεδομένων.

40) Εξωδικαστική Διαιτησία

- (1) Τρίτα μέρη που θεωρούν ότι το δικαίωμά τους στην προστασία των προσωπικών τους δεδομένων έχει παραβιαστεί, ως αποτέλεσμα πραγματικής ή πιθανής μη ορθής χρήσης των προσωπικών τους δεδομένων, έχουν το δικαίωμα να ζητήσουν από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων να μεσολαβήσει για το θέμα. Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων δικαιούται να εξετάσει την καταγγελία και να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τα δικαιώματά του. Σε αυτή την περίπτωση, ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων υποχρεούται να τηρεί το απόρρητο τυχόν άλλων προσωπικών δεδομένων του καταγγέλλοντος, εκτός εάν ο καταγγέλλων απαλλάξει τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων από την υποχρέωση αυτή. Καταβάλλεται προσπάθεια για να υπάρξει μία συμφωνία σχετικά με την καταγγελία, με την συμμετοχή του υποκειμένου των δεδομένων και του Υπευθύνου Προστασίας Προσωπικών Δεδομένων. Μια τέτοια συμφωνία μπορεί να περιλαμβάνει πρόταση σχετικά με την επανόρθωση - αποζημίωση για τη ζημία που υπέστη το υποκείμενο των δεδομένων ως αποτέλεσμα παραβίασης των δικαιωμάτων του. Εάν η πρόταση αυτή γίνει αποδεκτή από τα μέρη τότε αποκτά δεσμευτική ισχύ στις εμπλεκόμενες με την υπόθεση εταιρείες.
- (2) Το δικαίωμα του υποκειμένου των δεδομένων να υποβάλει καταγγελία στην αρμόδια εποπτική Αρχή ή να προσφύγει στα αρμόδια δικαστήρια δεν επηρεάζεται από την ανωτέρω περιγραφόμενη διαδικασία.

ΜΕΡΟΣ ΕΚΤΟ-ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

41) Τροποποίηση

- (1) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου εξετάζει τα BCRP ανά τακτά χρονικά διαστήματα και τουλάχιστον μία φορά το χρόνο, με σκοπό την εναρμόνισή τους με την ισχύουσα νομοθεσία, και προβαίνει σε όλες τις αναγκαίες τροποποιήσεις.
- (2) Κάθε σημαντική τροποποίηση αυτών συμφωνείται με την αρμόδια εποπτική Αρχή. Οι τροποποιήσεις αυτές ισχύουν άμεσα σε όλες τις εταιρείες που έχουν υπογράψει τους BCRP, έπειτα από μια κατάλληλη μεταβατική περίοδο.
- (3) Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου ενημερώνει όλες τις εταιρείες που έχουν υιοθετήσει τα BCRP για τις τροποποιήσεις επί του περιεχομένου.
- (4) Οι Υπεύθυνοι Προστασίας Προσωπικών Δεδομένων των εταιριών είναι υποχρεωμένοι να εξετάσουν αν οι τροποποιήσεις των BCRP επηρεάζουν την υποχρέωση συμμόρφωσης με την ισχύουσα νομοθεσία ή αν έρχονται σε αντίθεση με τις εθνικές νομικές διατάξεις. Εάν η εταιρεία δεν είναι σε θέση να εφαρμόσει τις τροποποιήσεις αυτές για λόγους συμμόρφωσης προς την εθνική νομοθεσία, αυτή ενημερώνει άμεσα τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων του Ομίλου και την αρμόδια εποπτική Αρχή. Στην περίπτωση αυτή η ισχύς των BCRP αναστέλλεται προσωρινά.

42) Λίστα Επαφών και Εταιρειών

Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων του Ομίλου τηρεί κατάλογο των εταιρειών που έχουν υιοθετήσει τα BCRP και των προσώπων επικοινωνίας στις εταιρείες αυτές. Κρατάει ενημερωμένο αυτό τον κατάλογο κι ενημερώνει τα υποκείμενα των δεδομένων και την αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κατόπιν αιτήματος.

43) Δικονομικά Θέματα / Ρήτρα Διαχωρισμού (Severability Clause)

Σε περίπτωση διαφορών, τα BCRP υπόκεινται στο δίκαιο της Ομοσπονδιακής Δημοκρατίας της Γερμανίας.

Εάν μεμονωμένες διατάξεις των BCRP είναι ή καταστούν άκυρες, αυτές θεωρείται ότι έχουν αντικατασταθεί από άλλες διατάξεις, που προσεγγίζουν όσο το δυνατό περισσότερο το αληθινό πνεύμα των BCRP και των άκυρων διατάξεων. Σε περιπτώσεις αμφιβολιών ή ελλείψεως σχετικών διατάξεων εφαρμόζεται η ισχύουσα νομοθεσία περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης.

44) Δημοσίευση

Οι εταιρείες πρέπει να παρέχουν πληροφορίες, σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων και την ρήτρα υπέρ τρίτου. Οι πληροφορίες αυτές καθίστανται διαθέσιμες στο κοινό σε κατάλληλη μορφή (πχ σχετικές αναρτήσεις στο διαδίκτυο). Οι πληροφορίες αυτές δημοσιεύονται αμέσως μόλις τα BCRP τεθούν σε ισχύ.

Όροι – Συντομογραφίες

Όρος – Συντομογραφία	Επεξήγηση
Χρήση ψευδώνυμων δεδομένων (aliasing)	Η αντικατάσταση του ονόματος, άλλων στοιχείων ταυτοποίησης ή χαρακτηριστικών ενός ατόμου με άλλα στοιχεία - χαρακτηριστικά, προκειμένου να αποφευχθεί ή να είναι πολύ δύσκολο να ταυτοποιηθεί το υποκείμενο των δεδομένων.
Χρήση ανώνυμων δεδομένων (anonymization)	Η διαδικασία αλλαγής πληροφοριών με τέτοιο τρόπο ώστε τα προσωπικά δεδομένα και άλλα στοιχεία να μην μπορούν πλέον να αντιστοιχηθούν σε ένα φυσικό πρόσωπο ή να μπορούν να αντιστοιχηθούν με δυσανάλογη μεγάλη προσπάθεια από άποψη χρόνου και κόστους.
Αυτοματοποιημένη χρήση προσωπικών δεδομένων	Η χρήση προσωπικών δεδομένων που μπορεί να επιφέρει νομικές συνέπειες ή σημαντικό αρνητικό αντίκτυπο στο υποκείμενο και η οποία βασίζεται αποκλειστικά σε αυτοματοποιημένη χρήση αυτών των δεδομένων με σκοπό την αξιολόγηση ορισμένων πτυχών της προσωπικότητάς του υποκειμένου των δεδομένων, όπως απόδοσή στην εργασία, φερεγγυότητα, αξιοπιστία, διαγωγή, επαγγελματική καταλληλότητα, κατάσταση της υγείας, κ.λπ.
Εταιρεία	Ως εταιρεία ορίζεται οποιαδήποτε εταιρία υπόκειται στους παρόντες Δεσμευτικούς Εταιρικούς Κανόνες για την Προστασία των Προσωπικών Δεδομένων. Ένας ξεχωριστός κατάλογος των εταιρειών αυτών διατηρείται για λόγους αναφοράς και ενημερώνεται σε συνεχή βάση. Ο κατάλογος μπορεί να δοθεί σε οποιονδήποτε, ανά πάσα στιγμή.
Υπεύθυνος επεξεργασίας	Οποιοσδήποτε επεξεργάζεται προσωπικά δεδομένα, αλλά όχι απαραίτητα νομικό πρόσωπο.
Υποκείμενο Δεδομένων	Οποιοδήποτε φυσικό πρόσωπο του οποίου τα προσωπικά δεδομένα αποτελούν αντικείμενο επεξεργασίας εντός του Ομίλου Deutsche Telekom.
Όμιλος Deutsche Telekom	Η Deutsche Telecom AG και όλες οι εταιρίες στις οποίες η Deutsche Telecom AG κατέχει άμεσα ή έμμεσα ποσοστό μεγαλύτερο από 50% ή κάθε εταιρεία που έχει πλήρως συγχωνευθεί.
Ελέγχουσα (μητρική) Εταιρεία του Ομίλου (Group Holding)	Η ελέγχουσα (μητρική) εταιρεία του Ομίλου είναι σήμερα η Deutsche Telekom AG με έδρα στη Βόννη, Γερμανία (Friedrich-Ebert- Allee 140, 53113).
Προσωπικά δεδομένα	Κάθε πληροφορία που είναι σχετισμένη με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (υποκείμενο των δεδομένων). Ως ταυτοποιήσιμο θεωρείται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, κυρίως με ένα ή περισσότερα συγκεκριμένα στοιχεία που το χαρακτηρίζουν, όπως αριθμός ταυτότητας, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα.

Αποδέκτης των δεδομένων	Κάθε φυσικό ή νομικό πρόσωπο, δημόσια Αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται τα δεδομένα, ανεξαρτήτως εάν πρόκειται για τρίτο μέρος ή όχι. Ωστόσο, οι δημόσιες Αρχές που μπορεί να λάβουν δεδομένα στο πλαίσιο έρευνας δε θεωρούνται αποδέκτες.
Ειδικές κατηγορίες προσωπικών δεδομένων	Κάθε δεδομένο που αποκαλύπτει φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστικά όργανα ή που αφορά στην υγεία ή στην ερωτική ζωή.
Τρίτο μέρος	Κάθε πρόσωπο ή υπεύθυνος επεξεργασίας εκτός του μέρους που έχει την ευθύνη για την επεξεργασία των προσωπικών δεδομένων. Ως τρίτα μέρη δεν θεωρούνται το υποκείμενο των δεδομένων, τα πρόσωπα ή οι υπεύθυνοι επεξεργασίας στους οποίους έχει ανατεθεί η συλλογή, επεξεργασία ή χρήση των προσωπικών δεδομένων στην Γερμανία, σε άλλο κράτος - μέλος της Ευρωπαϊκής Ένωσης (ΕΕ) ή σε άλλο κράτος συμβαλλόμενο με τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ).
Χρήση	Επεξεργασία δεδομένων προσωπικού χαρακτήρα, ιδιαίτερα η συλλογή, επεξεργασία και χρήση, συμπεριλαμβανομένης της μεταφοράς, των εν λόγω δεδομένων.