# BINDING INTERPRETATIONS

# GENERAL DATA PROTECTION REGULATION (GDPR)

Group Privacy

Version: 1.0

Last revised: 2016-11-18

Status: Final Version

## Table of Contents



Last updated: November 2016

Last updated: November 2016

**DISCLAIMER:**

The content of these Binding Interpretations is based on the final text of the GENERAL DATA PROTECTION REGULATION (GDPR) - (April, 2016). As of yet there are no official interpretations of certain items (by supervisory authorities, etc.).

The Binding Interpretations cannot replace an individual assessment of the applicability of the GDPR to the processing in your unit/ business unit/ department by your own.

Deutsche Telekom AG
Group Headquarters
Group Privacy
Contact: GDPR@telekom.de


| Publisher<br>Deutsche Telekom AG, Group Privacy | | |
|---|---|---|
| File Name<br>GDPR Binding Interpretations | Document Number<br>1 | Document name<br>GDPR Binding Interpretitions |
| Version<br>1.0 | Last Review<br>2016-11-18 | Status<br>Final |
| Short Description<br>Binding Interpretations of the General Data Protection Regulation | | |

# 1. INTRODUCTION

THE BINDING INTERPRETATIONS OF THE

GENERAL DATA PROTECTION REGULATION

(Regulation (EU) 2016/679)

BY GROUP PRIVACY

PREAMBLE

The digitization of our society continues apace. Millions of machines are networked with each other and huge quantities of data are being processed. All of which gives rise to questions about our data protection standards, which traditionally tend to be higher in Europe than the rest of the World. How can we transfer these standards to a digital age? Is it enough to comply with laws or do we need rules which go beyond these in order to gain people's trust? Digital responsibility lies at the heart of all these issues. A responsibility which Deutsche Telekom also assumes, especially when it comes to data protection.

Deutsche Telekom assumes responsibility for consistently fostering people's trust in data processing. This is the only way that digital business and processing models can be successfully further developed for the good of society and the individual.

The individual's digital autonomy takes center stage. This autonomy is guaranteed through a high degree of transparency, decision-making freedom and the development of data protection-friendly solutions. To this end, data protection experts need to be involved from the start in the development of new products and services that process personal data.

Recognising our aim to ensure data protection throughout the DT Group the new GENERAL DATA PROTECTION REGULATION (GDPR) will provide the legal and harmonized basis for all EU member states and it will apply to any entity offering goods or services to (regardless of payment being taken) and any entity monitoring the behaviours of citizens within the EU. Undertakings and enterprisesare now directly responsible for data protection compliance with the GDPR wherever they are based, as long as they are processing EU citizens' personal data.

This also means that in case of an infringement of the GDPR caused by an individual group undertaking the applicable basis of assessment for a fine could be the worldwide annual turnover of the Telekom Group.

## NATURE OF THESE BINDING INTERPRETATIONS AND HOW TO USE THEM

In providing these BINDING INTERPRETATIONS (BI) the DEUTSCHE TELEKOM Group Privacy Officer is delivering a standardized approach to the implementation needs regarding the GDPR. On a best effort basis it delivers interpretations of the legal aspects, assists with recommendations and best practises, and provides an initial set of compliance check questions.

A full and consequent adoption of the solutions mentioned in this document (e.g. interpretations, best practices, recommendations) will help to fulfil the implementation needs regarding the GDPR.

The BI are the combined result of requirements and interpretations regarding the successful EU-wide implementation of the GDPR. They shall be binding with regard to the processing of personal data for all DEUTSCHE TELEKOM Group undertakings within the European Union. In this context they are also relevant on international level when processing EU data of DEUTSCHE TELEKOM GROUP undertakings.

However, due to the transition period until the effectiveness of the GDPR on 25th May 2018 and in the light of other frame conditions not yet defined like the announced guidelines of the Article 29 Working Party, these BI reflect the current state of interpretation. It will be adopted in line with the further evolving of official statements and interpretations. Therefore it is a living document. Updates to this document will be made available communicated via myDMS and TELEKOM SOCIAL NETWORK / YOU AND ME.

## STRUCTURE OF THE BINDING INTERPRETATION

The BI deliver a set of legal notices and remarks, recommendations and implementation suggestions of relevant articles. The document includes the relevant articles of the GDPR – each with a general description, a short content summary, the BI itself, a preliminary compliance questionnaire, information on sanctions and finally best practises and templates.

- A GENERAL DESCRIPTION provides you an overview of the corresponding article including cross references and recitals. This shall help you to keep the overview among all articles.
- The short CONTENT SUMMARY shall give you an overview of the corresponding GDPR article. In case of questions please refer to the full GDPR article in the regulation itself.

- The BINDING INTERPRETATIONS (BI) contain short interpretations of relevant legal content of the GDPR. These interpretations are key components for your successful and compliant implementation of the relevant GDPR requirements.
- The COMPLIANCE QUESTIONAIRE (CQ) contains preliminary questions to check whether the implementation requirements are achieved or not. A comprehensive compliance approval concept will be developed and communicated via TELEKOM SOCIAL NETWORK / YOU AND ME.
- The SANCTIONS PART part shows you the possible fines if our undertaking won't be compliant with the corresponding GDPR article.
- Finally, the BEST PRACTICES and TEMPLATES section provides you a set of helpful hints or prepared templates for an EU wide usage.

## CONTACT AND QUESTIONS

In case of any questions e.g. regarding interpretation, implementation issues, the relation to other legal provisions, in case of any deviation of the Binding Interpretations or if you like to provide ideas or best practices please contact the GDPR team (gdpr@telekom.de), your contact person at Group Privacy your local Data Protection Officer (DPO). Information on the GDPR is provided via myDMS and TELEKOM SOCIAL NETWORK / YOU AND ME.

# 2. GENERAL DATA PROTECTION CONTENT (GDPR) CONTENT

## CHAPTER I - GENERAL PROVISIONS

Articles 1-4

The Regulation aims at balancing the protection of personal data and the free movement of such data. This chapter determines what kind of data processing is regulated by the GDPR and also lists which data processing activities fall outside the scope of the GDPR.

The chapter sets out the territorial scope for the application of the GDPR and gives the most important definitions for terms used throughout the Regulation.

## ARTICLE 3 TERRITORIAL SCOPE

### I.3.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 3 Territorial scope (Chapter I General provisions) |
| GDPR recitals | 22-25 |
| Cross references | Art. 2; 40 (3); 42 (2); 45 (3) |
| Relating documents | Working Party 29: Working Paper 203 on purpose limitation and further processing |
| BCRP references | None |

### I.3.2 Content Summary

The Article defines the territorial scope of the GDPR. The Regulation applies to all controllers and processors established in the European Union (EU) and under certain circumstances also if based outside the EU.

### I.3.3 Binding Interpretations

UNDERTAKINGS ESTABLISHED WITHIN THE EU:

- **definition of establishment**: effective and real exercise of activity through stable arrangements, Rec. 22
  → even a minimal exercise of activity (CJEU C-230/14; e.g. single representative)

→ the Legal personality is not the determining factor

- **data processing within the EU affecting data subjects outside the EU:** the GDPR is applicable to companies established in the EU and processing personal data of data subjects based outside the EU.

COMPANIES ESTABLISHED OUTSIDE THE EU:

- GDPR compliance is mandatory if they are targeting data subjects in the EU with their goods and services – irrespective of payment – or are monitoring their behavior in the EU.

### I.3.4 Compliance Questionnaire

- When processing personal data within the EU of data subjects based outside the EU are the requirements of the GDPR met? [Yes] / [No]
- Are undertakings compliant with the GDPR, which are targeting data subjects in the EU with their services or monitoring their behavior? [Yes] / [No]

### I.3.5 Sanctions

None

### I.3.6 Best practice and templates

None

# ARTICLE 4 DEFINITIONS

## I.4.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 4 Definitions (Chapter I General provisions) |
| GDPR recitals | 26-37 |
| Cross references | The Article defines the terms that are used in all Articles. |
| Relating documents | Working Party 29: Working Paper 203 on purpose limitation and further processing |
| BCRP references | §8 Principle<br>§9 Admissibility of personal data use<br>§10 Consent by the data subject<br>§11 Automated individual decisions<br>§13 Special categories of personal data<br>§15 Prohibition of tying-in<br>§18 Commissioned data processing<br>§20 Data security – technical and organizational measures<br>§27 Responsibility for data processing<br>Part Seven Definitions and Terms |

## I.4.2 Content Summary

The key terms such as “personal data”, “processing”, “controller”, “processor” and “consent”, which are used throughout the text of GDPR are defined in this Article.

## I.4.3 Binding Interpretations

CONSENT:

- consent from the data subject must be obtained in writing e.g. email, or a clear affirmative act - opt-in mechanism.

RESTRICTION OF PROCESSING:

- ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future; restriction of processing gives more possibilities than the blocking of data, it does not necessarily require the complete blocking of the processing of data.

OTHER DEFINITIONS:

- are defined and explained in the context of the Articles in this document where they become relevant.

### I.4.4 Compliance Questionnaire

None

### I.4.5 Sanctions

None

### I.4.6 Best practice and templates

None

# CHAPTER II - PRINCIPLES

Articles 5-11

This chapter sets out the data protection principles as the main responsibilities for organisations. The processing is only lawful if certain conditions listed in this chapter are met.There are conditions relating to consent as the legal basis for processing including special conditions applicable to a child's consent.

The conditions for the processing of special categories of personal data, e.g. racial background, political opinions, biometric data, are specified. Special rules apply to the processing of personal data relating to criminal convictions and offences and processing which does not require identification.

## ARTICLE 5 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

### II.5.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 5 Principles relating to processing of personal data (Chapter II Principles) |
| GDPR recitals | 39 |
| Cross references | Art. 23 (1); 25; 47 (2) d); 89 (1) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 203 "Opinion 03/2013 on purpose limitation and further processing" |
| BCRP references | §14 Data minimization, data avoidance, anonymization and aliasing<br>§19 Data quality<br>§22 Right of protest, right to have data erased or blocked, and right to correction |

### II.5.2 Content Summary

The Article contains the data protection principles on 'lawfulness, fairness and transparency'; 'purpose limitation'; 'data minimization'; 'accuracy'; 'storage limitation'; 'integrity and confidentiality' and 'accountability'.

### II.5.3 Binding Interpretations

ACCOUNTABILITY:

- the principle on accountability requires to be compliant with the GDPR principles and also to be able to demonstrate compliance
- where specific GDPR articles regulate in which form compliance must be demonstrated, the undertaking is responsible to set up any missing processes that ensure that the necessary documentation is kept by the undertaking/enterprise

DOCUMENTATION REQUIRED UNDER THE ACCOUNTABILITY PRINCIPLE:

must:

- be in written or electronic form
- be findable at any time
- be the result of a clear documentation process including clear assignment of responsibility for the documentation
- define the actual situation and circumstances clearly
- refer to the legal basis
- show author and editing history

DT GROUP SPECIFIC DOCUMENTATION THAT FULFILS THE ACCOUNTABILITY REQUIREMENTS:

e.g.:

- Privacy and Security Assessment (PSA)
- Standardized Data Privacy & Security Concept (SDSK)
- Commissioned Data Processing Agreement (CDPA)
- collective agreements
- records of processing activities (e.g. CAPE[1] for Controller)

### II.5.4 Compliance Questionnaire

- See specific articles

### II.5.5 Sanctions

Art. 83 (5) a): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### II.5.6 Best practice and templates

- https://drc.telekom.de/en/sec/privacy-security-assessment
- https://drc.telekom.de/en/privacy/privacy

[1] The software CAPE is part of the certification, according to the „Assurance-Standard 980" of the Privacy-Compliance-Management-System of DT Group.

# ARTICLE 6 LAWFULNESS OF PROCESSING

## II.6.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 6 Lawfulness of processing (Chapter II Principles) |
| GDPR recitals | 32, 40 – 50, 55, 56 |
| Cross references | Art. 8; 10; 13 (1) d), (2) c); 14 (2) d); 17 (1) b); 20 (1) a); 21 (1); 55 (2) |
| Relating documents | Working Paper 203 - Opinion 03/2013 on purpose limitation<br>Working Paper 216 on Anonymisation Techniques<br>Working Paper 217 - Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC |
| BCRP references | §8 Principle<br>§9 Admissibility of personal data use<br>§10 Consent by the data subject<br>§28 Data Privacy Officer |

## II.6.2 Content Summary

The Article stipulates the general conditions for lawful processing of personal data including consent, legitimate interest and conditions for further processing for a purpose other than the original purpose of data collection whereas the new purpose must be compatible with the original purpose. The Article lists inter alia pseudonymisation as a safeguard measure to ascertain the compatibility.

## II.6.3 Binding Interpretations

### LEGAL GROUNDS FOR THE PROCESSING OF ELECTRONIC COMMUNICATION DATA AND OTHER EXEPTIONS:

- the processing of electronic communication data is subject to the ePrivacy Directive (ePD) and its national implementations. For the relationship between the ePD and the GDPR please refer to Art. 95 (section XI.95.3).
- the processing of electronic communication data on the basis of legitimate interests, Art. 6 (1) f), or further processing, Art. 6 (4), is therefore not lawful

- regarding special categories of data the requirements of Art. 9 prevail
- in the employment context Art. 6 is applicable if not national law or other specifics (e.g. Art. 9) prevail (see "legal grounds based on legitmate interest")

LEGAL GROUNDS BASED ON LEGITIMATE INTERESTS, ART. 6 (1) f):

- if data is processed for the purposes of the controller's legitimate interests a balance test and a case by case assessment is necessary. In the following cases there is a refutable presumption for a legitimate interest of the controller:
  - **fraud, direct marketing**: e.g. processing of personal data for the **purpose of preventing fraud**, or for **direct marketing** purposes, see Rec. 47
  - **network and information security**: e.g. preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems, see Rec. 49
  - **intra group processing** and **balance of interest**: group undertakings may have a legitimate interest in transmitting personal data from clients or employees within the group of undertakings for **internal administrative** purposes, see Rec. 48. The requirements for international data transfer remain relevant.
    - → e.g. internal administrative purposes including the prosessing of client's and employee's data, Rec 48, e.g. such as commission of data for internal audit purposes; administrative puroses do not include processing of customer or employee data for marketing and sales purposes.
  - if **processing of personal data is already covered by a legal permission or by consent,** a following data processing within DT Group can be regarded as an assessed balance of interest: That means a Commissioned Data Protection Agreement (CDPA) **is not required.** However a service agreement will be necessary and the collaborating undertakings have to adhere to the Binding Corporate Rules Privacy (BCRP). Not to forget the information of the data subject.
- transparency: information to the data subject must include details regarding the controller's legitimate interest, see Art. 13 (1) d), 14 (2) b)

LEGITIMATE GROUNDS BASED ON FURTHER PROCESSING FOR ANOTHER BUT COMPATIBLE PURPOSE, ART. 6 (4):

- unless further processing is allowed by Member State law or based on consent further processing based on another compatible purpose is subject to comprehensive weighing of all relevant aspects necessary. Art. 6 (4) contains some relevant criteria. Legitimate processing based on a compatible purpose could be lawful if inter alia:
  - there is a strong link between the original purposes and the purpose of the intended further processing (e.g. own service of the controller in context with the prior purpose) or if the further processing is in close context to the prior purpose, in particular regarding the relationship between data subjects and the controller (e.g. list of contracts of previous contractors) and
  - the existence of appropriate safeguards, which may include encryption or pseudonymisation (pseudonymisation of data is a measure to fulfil the requirement of carrying out a compatibility

assessment before further processing of data can take place, Art. 6 (4e), see II.6.6). The DPO has to be informed in any case of pseudonymisation at an early stage according to § 28 (7) BCRP .

It is unlikely to be lawful,

- in particular if special categories of personal data are processed, pursuant to Art. 9 and the processing might have negative consequences of the intended further processing for data subjects (e.g. possible negative effects on financial or legal issues)

### II.6.4 Compliance Questionnaire

- Are direct marketing activities based on adequate legal grounds of the GDPR or are specific regulations relevant? [Yes] / [No]

### II.6.5 Sanctions

Art. 83 (5) a): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### II.6.6 Best practice and templates

- EXAMPLE: Privacy Requirement Anonymization and Pseudonymization: https://mydms.telekom.de:443/mydms/Start.do?spx=LTDAT5641363444951669545605 45

# ARTICLE 7 CONDITIONS FOR CONSENT

## II.7.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 7 Conditions for consent (Chapter II Principles) |
| GDPR recitals | 32, 33, 42, 43 |
| Cross references | Art. 6 (4); 8; 9 (2) a), c), d); 83 (5) a) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §10 Consent by the data subject<br>§15 Prohibition of tying-in |

## II.7.2 Content Summary

Article 7 stipulates requirements for consent (special requirements regarding children's consent, see. Art. 8) such as the need to be able to demonstrate the data subject given consent, form of the request, right to withdraw the consent and the preconditions for a freely given consent.

## II.7.3 Binding Interpretations

FORM OF CONSENT:

- consent, definition see Art. 4 (11), can be obtained **verbally, in writing and electronically**. It has to be given by a clear an affirmative action (opt-in):
  - valid e.g. ticking a box when visiting an internet website, "double opt-in" in case of email
  - not valid e.g.: silence, pre-ticked boxes, inactivity, consent in general contract conditions, simple opt-in in case of email
- request for consent: the request has to be presented in a manner which is clearly distinguishable from other matters, easy (group of customers addressed) to understand and access. Otherwise the consent is invalid.
  - EXAMPLE: advertising consent of DT Group-wide consent clause, Germany, see II.7.6
  - EXAMPLE: "Online Privacy Statement – DT One Pager": DT current online privacy statement
- informed consent: minimal requirements for an informed consent are identity of the controller and purposes of the processing and specific requirements in the following Articles 13, 14.
  - EXAMPLE "informed consent", see II.7.6
- Voluntary nature: consent has to be given freely.

- It is not freely given if:
  - the data subject has no genuine or free choice, is unable to refuse or withdraw consent without detriment
  - the performance of a contract, including the provision of a service, is dependent on the consent despite such data not being necessary for such performance. The prohibition of tying-in does not apply where consent is obtained e.g. for advertising purposes in the context of promotional contest
  - there is a clear imbalance between the data subject and the controller and it is therefore unlikely that consent was freely given (e.g. employment context)
  - it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case

WITHDRAW OF CONSENT:

- form of withdrawal: the withdrawal of consent has to be as easy as giving the consent at least being able to use the "same channel" (e.g. consent was given electronically, withdraw by using electronic means) or offering an easier way for the data subject
  - e.g. giving consent by ticking a box – unticking a box in the same form and place (e.g. privacy cockpit)
  - information of withdrawal: data subject must be informed about the right to withdraw the consent prior to giving the consent.

EVIDENCE OF CONSENT:

- where processing of personal data is based on consent, an appropriate evidence and documentation process must be implemented to demonstrate that consent has been given.

  - EXAMPLE: advertising consent process of the DT Group-wide consent clause Germany (KEK). The consent can be obtained **verbally, in writing and electronically**. Consent obtained verbally can be demonstrated by voice file and written confirmation; consent obtained electronically can be demonstrated by technical verification mechanisms.
  - given consent prior to the application of the GDPR: is the consent process in line with the requirements of the GDPR it can be demonstrated by showing the general consent process. The relevant consent based on this process should be flagged. The supervisory authority should be addressed.

### II.7.4 Compliance Questionnaire

- Is there a process in place to document the declarations of consent obtained from the data subject? [Yes] / [No]
- Is there a process in place to ensure that the requirements to obtain consent are taken into account in the respective case when consent is being obtained? [Yes] / [No]
- Are there procedural requirements in place for the withdrawal process? [Yes] / [No]

### II.7.5 Sanctions

Art. 83 (5) a): 20.000.000,- €, or up to 4% of the total worldwide annual turnover

### II.7.6 Best practice and templates

- EXAMPLE: “demonstration of consent”: current practice of consent for advertising purposes:

KEK_Art.7.pdf

- EXAMPLE: One-Pager: ‘Privacy made simple’:

One_pager.pdf

# ARTICLE 8 CONDITIONS APPLICABLE TO CHILD'S CONSENT IN RELATION TO INFORMATION SOCIETY SERVICES

## II.8.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 8 Conditions applicable to child's consent in relation to information society services (Chapter II Principles) |
| GDPR recitals | 38 |
| Cross references | Art. 6 (1) a); 12 (1); 40 (2) g) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §10 Consent by the data subject<br>Child: no regulation |

## II.8.2 Content Summary

Consent as specified in Art. 6 (1) a) to process data in relation to information society services has to be given or be authorised by the holder of parental responsibility if the child is under 16 or – if foreseen by national law - up to a lower age not under 13.

## II.8.3 Binding Interpretations

### SCENARIOS WHERE THE SPECIAL CONDITIONS FOR CONSENT BY A CHILD APPLY:

- need for concent or authorisation by the holder of the parental control in the context of information society services (e.g. social networks) are in particular
  - → for marketing purposes, creating personality or user profiles, collecting data when using services offered directly to a child, see Rec. 38, where the child's consent constitutes the legal basis for processing its personal data

### GENERAL CONTRACT LAW:

- the requirements of the general contract law e.g. rules on the validity, formation or effect of a contract in relation to a child (e.g. electronically by distant selling) remain valid

### AGE VERIFICATION TOOLS:

- the controller has to verify the consent given or authorised by the holder of parental responsibility

### II.8.4 Compliance Questionary

- Are appropriate measures implemented in your undertaking to verify the age of customers if necessary? [Yes] / [No]
- Are there adequate technical means in place to ensure that consent is given or authorized by the holder of parental responsibility over the child in cases where the child does not have the required age to give consent if necessary? [Yes] / [No]

### II.8.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### II.8.6 Best practice and templates

None

# ARTICLE 9 PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

## II.9.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 9 Processing of special categories of personal data (Chapter II Principles) |
| GDPR recitals | 51-56 |
| Cross references | Art.6 (4) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §13 Special categories of personal data |

## II.9.2 Content Summary

Processing of special categories of personal data (racial or ethical origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, data concerning a natural person's sex life and orientation) shall be generally prohibited unless the exemptions that are explicitly listed in the Article apply.

## II.9.3 Binding Interpretations

CONDITIONS FOR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA:

- **Art. 9 has its own catalogue of conditions** for lawful processing of these special categories. Art. 6 is – as far as Art. 9 is applicable not relevant to the processing of special categories of data:
  - → e.g. the undertaking cannot rely on the pursuance of its legitimate interests to process sensitive personal data

EXPLICIT CONSENT:

- **consent has to be explicit**: the general rules regarding consent according to Art. 4 (11) apply plus the explicit naming of the respective category of special categories of personal data that is to be processed.

BIOMETRIC AND GENETIC DATA:

- **biometric and genetic data** are now expressly included in the special categories of personal data. Any DT Group undertaking that has been or will be processing biometric or genetic data needs to assess the lawfulness of this processing by using the PSA process.

### II.9.4 Compliance Questionnaire

- Does your undertaking process special categories of personal data and in case of consent do you comply with the requirement of the GDPR? [Yes] / [No]
- Do you have technical and organizational measures (TOMs) in place that protect these data in a specific and secure way? [Yes] / [No]

### II.9.5 Sanctions

Art. 83 (5) a): 20.000.000,- €, or up to 4% of the total worldwide annual turnover

### II.9.6 Best practice and templates

None

# ARTICLE 10 PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES

## II.10.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 10 Processing of personal data relating to criminal convictions and offences (Chapter II Principles) |
| GDPR recitals | None |
| Cross references | Art. 6 (1) |
| Relating documents | Working Party 29: Working Paper 203 on purpose limitation and further processing |
| BCRP references | None |

## II.10.2 Content Summary

The processing of personal data relating to criminal convictions and offences or security measures should only be carried out under the control of official authority or with special authorisation of the EU or Member States.

## II.10.3 Binding Interpretations

CERTIFICATES OF GOOD CONDUCT:

- the presentation of a candidate's or employee's certificate of good conduct as part of the recruitment process is only permitted when the processing is authorized by Union or Member State law

## II.10.4 Compliance Questionnaire

- In case the presentation of certificates of good conduct is part of the recruitment process in yourundertaking, is this authorized by Union or Member State law? [Yes] / [No]

## II.10.5 Sanctions

None

## II.10.6 Best practice and templates

None

# ARTICLE 11 PROCESSING WHICH DOES NOT REQUIRE IDENTIFICATION

## II.11.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 11 Processing which does not require identification (Chapter II Principles) |
| GDPR recitals | 57 |
| Cross references | Art. 12 (2); 15-20 |
| Relating documents | None |
| BCRP references | Section 4 Data quality and data security<br>§ 19 Data quality |

## II.11.2 Content Summary

The controller is not obliged to keep information to identify the data subject for the sole purpose of complying with the GDPR. If the controller is not able to identify the data subject he needs to inform the data subject accordingly.

## II.11.3 Binding Interpretations

- telecommunication provider are required to identify the person with whom a telecommunication contract is concluded. Thus Art. 11 doesn't apply in terms of a non-identification
- the controller is obliged to identify the person **but not be required to collect additional information**. This could be the case if the data subject has the right to be informed but the controller has only pseudonomised data in data centers without the chance to reidentify the data subject (the key was deleted)
- Art 11 sec. 2 only restricts the rights of the data subjects e.g. in terms of the right of access by the data subject, but not in terms of the **obligation to transparency** of the controller. Therefore, the controller is also obliged to transparency if personal data are processessed in a pseudonyms way.

## II.11.4 Compliance Questionnaire

None

## II.11.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

## II.11.6 Best practice and templates

None

# CHAPTER III - RIGHTS OF THE DATA SUBJECT

Articles 12-23

The Regulation affords a wide range of rights to the data subjects, e.g. right to information and access to personal data, right to rectification, right to be forgotten, right to data portability and the right to object.

This chapter specifies for each right how and when the controller must give effect to them. Also, Art. 22 lays down the rights and restrictions concerning profiling.

## ARTICLE 12 TRANSPARENT INFORMATION, COMMUNICATION AND MODALITIES FOR THE EXERCISE OF THE RIGHTS OF THE DATA SUBJECT

### III.12.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject (Chapter III Principles) |
| GDPR recitals | 58, 59 |
| Cross references | Art. 11 (2); 13; 22; 34; 83 |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §5 Duty to inform<br>§11 Automated individual decisions<br>§12 The use of personal data for direct marketing purposes<br>§ 22 Right of protest, right to have data erased or blocked, and right to correction |

### III.12.2 Content Summary

Art. 12 contains detailed requirements regarding the controller's obligation to provide transparent information and communication to the data subject and regarding the modalities for the exercise of the rights of the data subject.

### III.12.3 Binding Interpretations

GENERAL REQUIREMENTS:

- form: information has to be in writing, electronic means or if requested orally, if the identity of the data subject is proven
- no action taken: the controller informs the data subject without delay and within one month at the latest when not taking action to answer. He informs on the possibility to address the supervisory authority and seeking judicial remedy.

SPECIFIC REQUIREMENTS IN ART. 12:

- are further discussed in the Art. 13 – 22 and 34 if it is relevant for the Binding Interpretations of these Articles.

### III.12.4 Compliance Questionary

- Do you have a process to check that transparency requirements are met? [Yes] / [No]

### III.12.5 Sanctions

Article 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.12.6 Best practice and templates

- One-Pager: 'Privacy made simple':


One_pager.pdf

# ARTICLE 13 INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED FROM THE DATA SUBJECT

# ARTICLE 14 INFORMATION TO BE PROVIDED WHERE PERSONAL DATA HAVE NOT BEEN OBTAINED FROM THE DATA SUBJECT

## III.13;14.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 13 Information to be provided where personal data are collected from the data subject (Chapter III Rights of the data subject)<br><br>Article 14 Information to be provided where personal data have not been obtained from the data subject (Chapter III Rights of the data subject) |
| GDPR recitals | 60-62 |
| Cross references | Art. 6 (1) f); 9 (2) a); 12; 22 (1), (4); 26 (1); 46; 47 (2) g); 49 (1); 79; 89 (1) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §5 Duty to inform<br><br>§11 Automated individual decisions |

## III.13;14.2 Content Summary

The Articles list the type of information that must be provided to the data subject where the data are collected directly from the data subject or have been obtained from another source.

## III.13;14.3 Binding Interpretations

TIME OF INFORMATION – WHERE DATA HAS BEEN OBTAINED DIRECTLY FROM THE DATA SUBJECT:

- at the time when personal data are obtained directly from the data subject

TIME OF INFORMATION – WHERE DATA HAS NOT BEEN OBTAINED FROM THE DATA SUBJECT:

- within a reasonable period after obtaining the data, at the latest within one month

- if data are used for communication with the data subject: at the latest at time of first communication
- if a disclosure to another recipient is envisaged: at the latest when data are first disclosed
- where controller wants to process data to a different/new purpose: information to data subject prior to that further processing

HOW TO PROVIDE THE INFORMATION TO THE DATA SUBJECT:

- clear language, any form, free of charge, use of icons after adoption of a delegated act by the EU-Commission
- it depends on the context under which data is collected from the data subject written e.g. privacy statement on website (see III.13.6 – 14.6 "DT one-pager"), send by email, orally communicated on the phone if requested by the data subject and the identity of the data subject is proven.
- information on intended transfer of personal data to third countries must be provided without the need to identify each specific third country.
- the data subject must be informed about the information listed in Art. 13 and 14 by the time the GDPR becomes effective.

FORM OF INFORMATION WHERE PROCESSING IS ADDRESSED TO A CHILD:

- to achieve specific protection of children, the information and communication must be in such clear and plain language that the child can easily understand.

### III.13;14.4 Compliance Questionnaire

- Did you check the existing process and content of providing information to the data subject, especially regarding form and time of information? [Yes] / [No]
- Did you check the existing privacy policy/privacy statement to ensure it contains all information as required under the GDPR? [Yes] / [No]

### III.13;14.5 Sanctions

Article 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.13;14.6 Best practice and templates

- EXAMPLE: "Online Privacy Statement – DT One Pager": DT current online privacy statement
  http://agb.telekom.de/doku/engldatei/43963.pdf
  http://agb.telekom.de/doku/engldatei/43968.pdf
- EXAMPLE: "Privacy statement": DT current privacy statement (telecommunication data in German):


Data privacy
information for the Te

# ARTICLE 15 RIGHT OF ACCESS BY THE DATA SUBJECT

## III.1.15 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 15 Right of access by the data subject (Chapter III Rights of the data subject) |
| GDPR recitals | 63, 64 |
| Cross references | Art. 11(2); 22 (1), (4); 46; 89 (2), (3) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 187 "Opinion 15/2011 on the definition of consent" |
| BCRP references | §5 Duty to inform<br>§11 Automated individual decisions |

## III.15.2 Content Summary

The Article sets out the right of the data subject to obtain access to the personal data which is processed by the controller and defines the content of the information (e.g. purpose, categories, recipients, storage, authorities to complain, right to request rectification or erasure, source of collected data, existence of automated decision making incl. profiling, information on appropriate safeguards when transferring data to third countries).

## III.15.3 Binding Interpretations

RIGHT OF ACCESS:

- information: the data subject has the right of access to the personal data and detailed information, see III.15.2. Information on transfer of personal data to third countries do not need to specify the countries but describe the appropriate safeguards used (e.g. BCRP, standard contractual clauses).
- form and costs: controller must provide information/copy free of charge unless repetitive, manifestly unfounded or excessive request, further copies allow a reasonable fee based on administrative costs. If access is requested by electronic means the answer has to be provided in an electronic form unless otherwise requested. To meet the request the controller can also provide remote access for the data subject to the personal data (e.g. via the section "personal data" in the online customer account).
- time: the information should be given one month after the request was received by the controller at the latest, see Art. 13 (3)
- confirmation of identity: the controller may request additional information to confirm the identity of the data subject who requested access

### III.15.4 Compliance Questionnaire

- Do you have a process in place for the handling of requests from the data subject to obtain access to their data and the process is compliant with the GDPR? [Yes] / [No]

### III.15.5 Sanctions

Art. 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.15.6 Best practice and templates

- Overview Content Art. 15 :


Informationselement e_art._15.pdf

# ARTICLE 16 RIGHT TO RECTIFICATION

## III.16.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 16 Right to rectification (Chapter III Rights of the data subject) |
| GDPR recitals | 65 |
| Cross references | Art. 5 (1) (d); 12; 14 (2) c); 15 (1) e); 58 (2) g) |
| Relating documents | None |
| BCRP references | §5 Duty to inform<br>§22 Right of protest, right to have data erased or blocked, and right to correction |

## III.16.2 Content Summary

The Article stipulates the data subject's right to obtain the rectification of inaccurate or incomplete personal data.

## III.16.3 Binding Interpretations

EXISTING PROCEDURES:

- no changes regarding the existing procedures needed if the processes are already in line with the national implementation of the General Data Protection Directive, 95/46/EC
- the data subject has the right to complete incomplete data also by a supplementary statement

REQUEST TO RECTIFY IS DENIED:

- if the data subject's request will not be followed, the reasons for that decision have to be documented and made transparent in the communication to the data subject

## III.16.4 Compliance Questionnaire

- Are the existing processes regarding the right of rectification in line with Art. 16? [Yes] / [No]

## III.16.5 Sanctions

Art. 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

## III.16.6 Best practice and templates

None

# ARTICLE 17 RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')

## III.17.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 17 Right to erasure ('right to be forgotten') (Chapter III rights of the data subject) |
| GDPR recitals | 65, 66 |
| Cross references | Art. 12; 13 (2) b); 14 (2) c); 15 (1) e); 18 (1) b); 58 (2) g); 70 (1) d); |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 225 "Guidelines on the implementation of the court of justice of the European union judgment on "Google Spain and inc v. agencia española de protección de datos (aepd) and mario costeja gonzález" c131/12 |
| BCRP references | §5 Duty to inform<br>§22 Right of protest, right to have data erased or blocked, and right to correction |

## III.17.2 Content Summary

Controllers must erase personal data "without undue delay" upon the data subject's request if the data is no longer needed, the data subject objects to the processing, the processing was unlawful or another ground as listed in the Article applies.

## III.17.3 Binding Interpretations

PROCEDURE TO DELETE DATA:

Art. 17 in principle does not include new requirements on how data must be deleted. Specific aspects are:

- objection to the processing: personal data has to be deleted, if the data subject objects to the processing in the following cases, see Art. 17 (1) (c), Art. 21 (1), (2):
  - the data subject objects to the processing based on Art. 6 (1) e) "public interest" or Art. 6 (1) f) "legitimate interest" including profiling and there are no overriding legitimate grounds for further processing or
  - the data subject objects against processing for direct marketing purposes. This includes profiling which is related to these purposes.

- withdrawal of consent: respective data has to be deleted if the data subject withdraws consent which is based on Art. 6 (1) a) "consent" or Article 9 (2) "consent regarding special categories of data" and there is no other legal ground for the processing, Art. 17 (1) b)
- copies and replicas: the deletion process must include the deletion of copies and replicas
- blocking: blocking of data is permitted based on the purposes listed in Art. 17 (3)
- processing software which do not include a delete function may not be implemented, if erasure is required by the GDPR.

SEARCH ENGINES:

- the obligations set out in Art. 17 (2) are mainly targeting the operators of search engines, e.g. Google, Bing, Yahoo. The standards set by the European Court of Justice in the so called "Google Ruling" (C-131/12) remain relevant.

### III.17.4 Compliance Questionnaire

- Are the processes in your undertaking in line with Art. 17 GDPR? [Yes] / [No]

### III.17.5 Sanctions

Art. 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.17.6 Best practice and templates

None

# ARTICLE 18 RIGHT TO RESTRICTION OF PROCESSING

## III.18.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 18 Right to restriction of processing (Chapter III Rights of the data subject) |
| GDPR recitals | 67 |
| Cross references | Art.4(3); 12; 19; 21 (1); 58 (2) g); |
| Relating documents | None |
| BCRP references | §5 Duty to inform |

## III.18.2 Content Summary

The data subject has the right to request from the controller to restrict the processing.

## III.18.3 Binding Interpretations

RESTRICTION OF FURTHER PROCESSING:

- right to restriction is a new right for the data subjects. It differs from the former right to request the blocking of data in so far as it still allows the processing for the purposes as set out in Art. 18 (2). If the processing of data has to be restricted the controller is only permitted to store the data and use it in the defined cases
  → e.g. with the consent of the data subject for the establishment, exercise or defence of legal claims
- the right to require restriction of processing is only available to the data subject.

TECHNICAL ABILITY TO RESTRICT THE PROCESSING:

- the undertaking needs to implement processes including technical and organisational aspects that give effect to the data subject's right to restrict the processing of their data

## III.18.4 Compliance Questionnaire

- Are the existing processes regarding the right of restriction of processing in line with Art. 18? [Yes] / [No]?
- Did you technically implement the possibility of data restriction? [Yes] / [No]?
- Did you implement a process regarding the information of the data subject before the restriction is lifted? [Yes] / [No]?

### .III.18.5 Sanctions

Article 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.18.6 Best practice and templates

None

# ARTICLE 20 RIGHT TO DATA PORTABILITY

## III.20.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 20 Right to data portability (Chapter III Rights of the data subject) |
| GDPR recitals | 68 |
| Cross references | Art. 6 (1) a), b); 14 (2) c); 17 |
| Relating documents | Working Paper 236 |
| BCRP references | §5 Duty to inform |

## III.20.2 Content Summary

Upon request the controller submits the data which the data subject provided to the data subject or directly to another controller in a commonly used and machine readable format.

## III.20.3 Binding Interpretations

DATA TO BE PROVIDED BY THE CONTROLLER:

- according to the wording "data provided to a controller":
  → only the data, which the data subject controls and accesses on its own (e.g. photos, emails)
  → not usage data and necessary contract data
- this means especially for **email services, cloud services and telecommunication services**:
  → the controller is obliged to provide data which has been *given to him* at any time up to the time of requesting. This might be mainly the **social media data of the data subject** (photos, contacts or any data, which has been stored by the data subject).
  → the controller is not obliged to provide data, which has been given by the data subject to fulfill the contract. The controller is not obliged to provide any data, which has been generated by the data subject in the meantime by using the service.
- article 20 is also applicable in the employment context, eg. YAM-data (according to the right of access).
- the DPO has to be contacted in any case of legal uncertainty about the application of this Article.

FORMAT OF TRANSMISSION:

- possibility of direct transmission from one controller to another:
  → interoperable formats already in place can be used

- transmission to the data subject:
  → commonly used formats should be used, e.g CSV

### III.20.4 Compliance Questionary

- Do you have a process in place to respond to a data subject's request to receive the data in a structured, commonly used and machine-readable format and to transmit it to another controller? [Yes] / [No]
- Do you have a process in place to inform the data subject at the latest within one month of the reasons for not taking action if there are reasons for not taking action on the data subject's request? [Yes] / [No]

### III.20.5 Sanctions

Article 83 (5) b): 20,000,000 € or 4% of the total worldwide annual turnover

### III.20.6 Best practice and templates

None

# ARTICLE 21 RIGHT TO OBJECT

## III.21.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 21 Right to object (Chapter III Rights of the data subject) |
| GDPR recitals | 69, 70 |
| Cross references | Art. 6 (1); 13 (2) b); 14 (2) c); 15 (1) e); 17 (1) c); 18 (1) d); 89 (1) |
| Relating documents | None |
| BCRP references | §5 Duty to inform<br>§11 Automated individual decisions<br>§12 The use of personal data for direct marketing purposes<br>§22 Right of protest, right to have data erased or blocked, and right to correction |

## III.21.2 Content Summary

Data subjects have the right to object to data processing if it is based either on the grounds of public interest or the controller's legitimate interests with the result that the processing has to stop unless the controller's interests outweigh the data subject's interests. The data subject can also object to the processing of the data for direct marketing purposes.

## III.21.3 Binding Interpretations

RIGHT TO OBJECT TO THE PROCESSING ON THE BASIS OF LEGITIMATE INTEREST:

- **the objection has to be declared on grounds** relating to the personal/specific situation and does not lead directly to the elimination of the legal basis for processing, rather to **verification of the balance of interests determined**. The controller must demonstrate that his compelling legitimate grounds-override the interests, rights and freedoms of the data subject. If he cannot demonstrate this, the processing must stop.

RIGHT TO OBJECT TO THE PROCESSING FOR DIRECT MARKETING:

- the objection has an absolute impact on direct marketing on the basis of profiling. Means that the controller shall have the obligation to erase the personal data without undue delay, see Art. 17 (1) c)

- direct marketing means targeted advertising by using such as e-mail, post address, phone number

INFORMATION TO THE DATA SUBJECT ABOUT THE RIGHT TO OBJECT:

- controller must inform the data subject about the different rights to object as listed in Art. 21. at the latest at the time of the first communication:
  → e.g. when the first newsletter is sent to the recipient
  → see information regarding the rights to object in "DT one-pager", see III.15.1.6

HOW TO EXERCISE THE RIGHT TO OBJECT:

- A process must be set up that ensures that the controller can observe and process a right to object exercised by the data subject by automated means using technical specifications.

### III.21.4 Compliance Questionnaire

- Have you implemented a process, which in relation to processing of personal data on the basis of the controller's legitimate interests (Art. 6 (1) f)) documents the legitimate prevailing interests of the controller? [Yes] / [No]
- Can you verify the controller's legitimate interest in the case of an objection? [Yes] / [No]
- Are individuals informed clearly and separately at the point of 'first communication about their right to object (e.g. notices and policies)? [Yes] / [No]
- Is a process implemented that ensures that the processing of the data can be stopped immediately once the data subject objects to direct marketing and direct marketing based on profiling? [Yes] / [No]
- Do you have the processes in place so it is possible for the data subject to object by automated procedures on the basis of technical specifications? [Yes] / [No]

### III.21.5 Sanctions

None

### III.21.6 Best practice and templates

- see III.15.6

# ARTICLE 22 AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

## III.22.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 22 Automated individual decision-making, including profiling (Chapter III Rights of the data subject) |
| GDPR recitals | 69, 70, 71, 72 |
| Cross references | Art. 4 (4); 12 - 15; 21; 35 |
| Relating documents | None |
| BCRP references | §11 Automated individual decisions |

## III.22.2 Content Summary

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects for them or otherwise significantly affects them. Some exemptions apply, e.g. a decision based on profiling, if necessary to enter into a contract with the data subject.

## III.22.3 Binding Interpretations

SCOPE:

- decisions based solely on automated processing, which are based on evaluating *personal aspects* relating to the data subject, §11 a) BCRP:
  → e.g. automatic refusal of an online credit application/e-recruiting practices without any human intervention
- profiling is one example of an automated decision making that is explicitly mentioned in Art. 22
  → analyse or predict aspects relating to performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, see Art. 4 (4)
  → scoring with credit agencies if it is executed only by automated means without human intervention

INFORMATION ABOUT THE AUTOMATED DECISION MAKING:

- give specific information and explanation of the decision: the main reasons for the decision need to be explained not only on request, so that the data subject is able to express its point of view
- providing meaningful information about the logic involved, as well as the significance and the envisaged consequences:
  → in privacy policy or in response to data subject's request to access his/her data

- if there is an objective need to make automated decisions, the data subject must be informed without delay and must be given an opportunity to object, §11 b) BCRP

SPECIAL REQUIREMENTS FOR PROFILING:

- When processing personal data for profiling purposes, it must be ensured that appropriate safeguards are in place.
  → e.g. right to obtain human intervention, possibility to contest the decision
- use appropriate mathematical or statistical procedures for the profiling
- implement appropriate TOMs to enable inaccuracies to be corrected and minimise the risk of errors.
  → e.g. plausibility check
- secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

APPLICATION OF THE PSA PROCESS BEFORE AUTOMATED INDIVIDUAL DECISION-MAKING:

- an impact assessment is necessary where a systematic and extensive evaluation of personal aspects relating to natural persons which is based on profiling is intended, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual. The PSA process meets this requirement (category A of PSA)
- right to object see Art. 21(3)

### III.22.4 Compliance Questionary

- If there are use cases of automated individual decision-making, including profiling:
  - Is it excluded that a child is concerned by an automated decision? [Yes] / [No]
  - Is there a legal basis (necessary for contract or authorized by Union or Member State law or data subject´s explicit consent)? [Yes] / [No]
  - If special categories of personal data are processed, is there a legal basis (data subject´s explicit consent to the processing of those personal data for one or more specific purposes – except where Union or Member state law provide that the prohibition to process those data may not be lifted by the data subject)? [Yes] / [No]
  - Are there appropriate mathematical or statistical procedures used for the profiling? [Yes] / [No]
  - Are there suitable measures in place to safeguard data subject´s rights, which include:
    - Specific information and explanation of the decision to the data subject? [Yes] / [No]
    - Right of the data subject to contest the decision, to express its point of view and to obtain human intervention on the part of the controller? [Yes] / [No]
    - TOMs appropriate to secure personal data and to ensure, that risk of error is minimized? [Yes] / [No]
    -

### III.22.5 Sanctions

Article 83 (5) b): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### III.22.6 Best practice and templates

None

# CHAPTER IV - CONTROLLER AND PROCESSOR

Articles 24- 43

This chapter is separated in five sections. Section 1 of chapter IV defines the general obligations of the controller and the processor. The GDPR introduces the requirement to keep records in relation to the processing activities and the categories of the processing activities. Data protection by design and by default is described as a main aspect for the processing of personal data.

Section 2 sets out the requirements regarding the security of personal data as well as the processes that have to be followed regarding the information to the supervisory authority and the information to the data subject in the event of a personal data breach.

Section 3 provides the rules when a data protection risk assessment needs to be carried out and also describes in which cases the controller needs to consult the supervisory authority prior to the processing of personal data.

In section 4, the role, tasks and responsibilities of the DPO are specified. The last section 5 is dedicated to the instruments Codes of Conduct and certification that can be used to demonstrate compliance with the GDPR.

## ARTICLE 24 RESPONSIBILITY OF THE CONTROLLER

### IV.24.1 General Information

| Topic | Reference |
|---|---|
| GDPR ARTICLE | Article 24 Responsibility of the controller (Chapter IV Controller and processor) |
| GDPR recitals | 74-77 |
| Cross references | Art. 40; 42 |
| Relating documents | None |
| BCRP references | §20 Data security – technical and organizational measures |

### IV.24.2 Content Summary

The controller shall implement appropriate TOMs including in most cases a data protection policy to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. To demonstrate

compliance with the controller's obligations adherence to codes of conduct or certification mechanism may be used.

### IV.24.3 Binding Interpretations

IMPLEMENTATION AND DOCUMENTATION OF TOMS:

- appropriate TOMs and data protection policies have to be implemented and documented. Within the DT Group the PSA process and the usage of the standard Commissioned Data Processing Agreements as provided by Group Privacy (GPR) are fulfilling those requirements.
- data protection policies set out the data protection requirements or rules. These are included:
  → in the PSA process
  → in other documentation, e.g. privacy rules in YAM, privacy rules in employment agreements
- adherence to the BCRP and the Binding Interpretation for the GDPR demonstrate compliance with the GDPR

CERTIFICATION MECHANISMS:

- certification mechanisms should be used where in place

PSA PROCESS:

- the PSA process is an EU-wide DT Group standard and has been certified as an information security management system which fulfils the ISO/IEC 27001: 2013 standard. The PSA process ensures that the requirements according to Art. 24 and §20 BCRP are fulfilled and the respective documentation is maintained.

### IV.24.4 Compliance Questionnaire

- Do you use PSA for all relevant projects and systems? [Yes] / [No]
- Do you have a process implemented which secures the conclusion of CDP. As including TOMs before you engage in processing activities with a third party? [Yes] / [No]
- Is there sufficient documentation to demonstrate compliance with the Regulation? [Yes] / [No]
- Do you have a process in place to check that you are compliant with the BCRPand the Binding Interpretations? [Yes] / [No]
- Do you have any certifications in place? [Yes] / [No]

### IV.24.5 Sanctions

None

### IV.24.6 Best practice and templates

None

# ARTICLE 25 DATA PROTECTION BY DESIGN AND BY DEFAULT

## IV.25.1 General Information

| Topic | Reference |
|---|---|
| GDPR ARTICLE | Article 25 Data protection by design and by default (Chapter IV controller and processor) |
| GDPR recitals | 78 |
| Cross references | Art. 4 (5); 47 (2) d) |
| Relating documents | Commission Recommendation Of 10 October 2014 On The Data Protection Impact Assessment Template For Smart Grid And Smart Metering Systems (2014/724/EU)<br><br>Article 29 Data Protection Working Party: Working Paper 223 "Opinion 8/2014 On Recent Developments On The Internet Of Things" |
| BCRP references | §20 Data security – technical and organizational measures |

## IV.25.2 Content Summary

Article 25 implements the principle of data protection by design and by default. The principle of data protection by design requires at the time of the determination of the means for processing and the time of the processing itself during the life circle of a service, product or any other processing activity the controller to ensure the implementation of adequate TOMs (e.g. pseudonymisation) in accordance with the data protection principles. Data protection by default obliges the controller to implement TOMs which guarantee that only data necessary for the purpose are processed.

## IV.25.3 Binding Interpretations

### MANDATORY IMPLEMENTATION OF TECHNICAL AND ORGANISATIONAL MEASURES:

- it is mandatory for each DT Group undertaking to implement the concept of "data protection by design and privacy by default"
- data protection must be taken into account not only at the final stages of the product or service configuration but from its very beginning and during the whole lifecycle process
- when deciding whether to impose an administrative fine and deciding on the amount of the fine the degree of implementation of TOMs according to Art. 25 will be considered by the supervisory authority, see Art. 83 (2) d)
- EXAMPLE: no pre-ticking of content boxes for privacy by default

PSA PROCESS:

- to ensure compliance with the GDPR at any time the PSA process shall be implemented in the currently applicable version provided by GPR (http://drc.telekom.de/en/sec/privacy-security-assessment) in every DT Group undertaking, see also IV.25.6.
- the requirements for data protection by design and default are covered especially by the "initial consultation guide" and the privacy requirements of the PSA process. It is not sufficient to implement the PSA version without the "initial consultation guide", framework demands and focus audits.

### IV.25.4 Compliance Questionnaire

- Is the PSA implemented in the currently applicable version provided by GPR? [Yes] / [No]

### IV.25.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.25.6 Best practice and templates

- GPR Privacy Requirements/Initial Consultation Guide (ICG 5):
  https://psa-portal.telekom.de

# ARTICLE 26 JOINT CONTROLLERS

## IV.26.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 26 Joint controllers (Chapter IV Controller and processor) |
| GDPR recitals | 79 |
| Cross references | Art. 4 (7); 36 (3) a) |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 169 "Opinion 1/2010 On The Concepts Of "Controller" And "Processor"" <br><br> Information Commissioner's Office „Data Controllers And Data Processors 20140506 Version: 1.0" <br><br> Arbeitsbericht Der Ad-Hoc-Arbeitsgruppe „Konzerninterner Datentransfer", 11.01.2005, Regierungspräsidium Darmstadt, Aufsichtsbehörde Für Den Datenschutz Im Nicht Öffentlichen Bereich (only available in German) |
| BCRP references | §27 Responsibility for data processing <br> Part Seven Definitions and Terms |

## IV.26.2 Content Summary

The Article describes the definition of joint controller and the conditions relevant for such joint activities.

## IV.26.3 Binding Interpretations

DEFINITION JOINT CONTROLLERS:

- where two or more controllers jointly determine the purposes and means of processing of personal data they shall be considered as joint controllers.

RESPONSIBILITIES OF JOINT CONTROLLERS:

- joint controllers have joint responsibility for the data processing activities
- failure to apportion the responsibility can result in higher administrative fines, Art. 83 (1) d)

AGREEMENT REGARDING THE RESPONSIBILITIES:

- responsibilities have to be clearly fixed in an agreement according to Art. 26
- recommendation of what to include in the agreement:
  - → clear description of duties and responsibilities especially regarding who will meet the requirements of providing clear and transparent information to data subjects, see Art. 13, 14
  - → coordination with DT Group undertakings's DPO is necessary in the case of a contract involving joint controllers
- the essence of the agreement must be made available to the data subject

### IV.26.4 Compliance Questionnaire

- If your undertaking as a controller cooperates with another controller in relation to the same processing activities do you have an agreement in place according to Art. 26 GDPR? [Yes] / [No]

### IV.26.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.26.6 Best practice and templates

None

# ARTICLE 28 PROCESSOR

# ARTICLE 29 PROCESSING UNDER THE AUTHORITY OF THE CONTROLLER OR PROCESSOR

## IV.28.;29.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 28 Processor (Chapter IV Controller and processor)<br><br>Article 29 Processing under the authority of the controller or processor (Chapter IV Controller and processor) |
| GDPR recitals | 81 |
| Cross references | Art. 4; 24; 26; 27; 30 (2); 31; 32 (;33 (2); 37-40; 42; 44-49; 58; 77; 79; 82; 83 |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 169 "Opinion 1/2010 On The Concepts Of "Controller" And "Processor" |
| BCRP references | §18 Commissioned data processing |

## IV.28.;29.2 Content Summary

Art. 28 is setting out the requirements where processing is to be carried out on behalf of a controller. Furthermore, the Article contains special provisions if the processor wants to appoint another processor.

Art. 29 states the processor's duty to comply with the controller's instructions unless required to do so by Union or Member State law.

## IV.28.;29.3 Binding Interpretations

FORM OF A DATA PROCESSING AGREEMENT:

- **data processing on behalf of the controller:** shall be governed by a written contract, Art. 28 (9), the data processing agreement (see IV.28;29.6). To comply with this requirement, electronically agreed contracts are sufficient and the contract does not require an individual signature. For reasons of an eventual burden of proof, digital signature solutions like DocuSign or pdf-signature are the preferred method.

- **code of conduct:** the adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller.
  → **to check:** until the date of application of the GDPR, every processing of personal data within DT Group must be brought into conformity with the regulation (see Art. 99). Therefore, it must be checked if the existing data processing agreements fulfill the requirements set out in Art. 28 (see IV.28;29.6).

CONTENT OF DATA PROCESSING AGREEMENT:

- **selection of the processor:** where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate TOMs:
  - TOMs shall uniformly meet high data privacy requirements. For internal DT systems, the PSA process has to be followed. The checks carried out as part of the PSA process have to be managed by the DT department who is actually processing the personal data. External systems processing data of DT undertakings shall meet the PSA-requirements..
  - compliance with the contractually agreed TOMs must be verified as soon *as* the contract is concluded *and also before* the processing begins. If reasonable and adequate, the processor shall state compliance by a "self-assessment" and confirm compliance vis-à-vis the undertaking of the DT group in a so-called SOC document (https://drc.telekom.de/de/privacy/service/adv-kontrollen--was-ist-das/112718). In all other cases, an audit has to be carried out.
- **sub-processors (engagement of another processor):** in case the processor intents to engage another processor he has to take into account the following provisions:
  - the processor needs either the prior specific approval by the controller or a general authorization in writing which includes electronic form. In the latter case, the processor informs the controller on intended changes regarding other processors so the controller can object. The controller must decide if a prior consent for the involvement of sub-processors is required or if a general authorization is granted according to the requirements set out in Art. 28. The processor as the processing unit must ask the controller for the authorisation to engage sub-processors. Respective clauses have to be implemented in the contract (see.28;29.6).
  - the processor shall contractually impose on the sub-processor the same data protection obligations as set out in the data processing agreement. If in certain cases – even after consultation of the responsible DPO – this is not possible standard contractual clauses, Art. 28 (7) or other mechanisms listed in Art. 28 (6) can be used.
- **liability:** personal data are only to be processed by any person acting on behalf of the controller or processor based on the controller's documented instructions.
  - if a processor acts against the controller's instructions by processing data for other purposes he will be considered to be a controller in respect of this processing and be held liable
  - where the sub-processor fails to fulfill the data protection obligations the initial processor remains fully liable

  → TEMPLATE: for further details regarding the requirements for the data processing agreement see template IV.28;29.6.

### IV.28.;29.4 Compliance Questionnaire

- Controller and processor: Do you check the existing commissioned data processing contract for their compliance with the GDPR? [Yes] / [No]
- Controller and processor: Is all data processing on behalf of the controller governed by a written contract, Art. 28 (9) (the data processing agreement)? [Yes] / [No]
- Controller: Is ensured that the processor provides sufficient guarantees to implement appropriate TOMs (e.g. certification)? [Yes] / [No]
- Controller: Do you check the compliance with the contractually agreed TOMs for the first time as soon as the contract has been signed and also before processing begins? [Yes] / [No]
- Controller and processor: Are the responsibilities of the parties and liability issues clearly defined in the contract? [Yes] / [No]
- Controller and processor: Are the necessary documentation measures met? [Yes] / [No]
- Processor: Do you have the written authorization of the controller for all engaged sub-processors? [Yes] / [No]
- If you have an individual or a general written authorization from the controller to engage sub-processors, do you inform the controller of any intended changes concerning the addition or replacement of sub-processors? [Yes] / [No]
- Processor: If you engage sub-processors with the prior written authorization of the controller, did you check compliance with the obligations on the part of the sub-processor, in particular compliance with the agreed TOMs, before data processing begins (and at regular intervals thereafter) and do you document the result of the checks? [Yes] / [No]
- Processor: Do you process the data exclusively under the terms of the contract and according to the controller's instructions, unless required to do otherwise by Union or Member State law? [Yes] / [No]

### IV.28.;29.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.28.;29.6 Best practice and templates

- Check list:


Check_list_art
_28_deutsch.pdf

# ARTICLE 30 RECORDS OF PROCESSING ACTIVITIES

## IV.30.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 30 Records of processing activities (Chapter IV Controller and processor) |
| GDPR recitals | 82 |
| Cross references | Art. 5 (2); 24; 28-33; 49 (6) |
| Relating documents | None |
| BCRP references | None |

## IV.30.2 Content Summary

Both controller and processor have to maintain records. The controller records the processing activities which, on request, have to be made available to supervisory authorities. The processor records the categories of processing. The requirements regarding the content of the records differ.

## IV.30.3 Binding Interpretations

### DUTY OF THE CONTROLLER TO MAINTAIN RECORDS:

- the controller maintains records of the processing activities under its responsibility including e.g. information on contact details, purpose of processing, transfer to third countries and as appropriate time limits for erasure and TOMs, see Art. 30 (1)
- the requirements of Art. 30 (1) are covered by using the software CAPE

### DUTY OF THE PROCESSOR TO MAINTAIN RECORDS:

- the processor maintains records of the categories of the processing carried out on behalf of the controller including e.g. contact details of the processor, where applicable transfer to third countries.

## IV.30.4 Compliance Questionnaire

- Controller & processor: do you have an overview of your processing activities? [Yes] / [No]
- Controller: do you register based on CAPE? [Yes] / [No]
    - If [No] Does your register have all the necessary information lines which are stipulated in Art. 30 (1)? [Yes] / [No]

- Have you considered using the tool “CAPE”, which as a tool is part of the Compliance Management System of the DT Group and as such is part of the PS 980 certification of the DT Group? [Yes] / [No]
- Processor: are you prepared to provide a register for your activities as a processor, Art. 30 (2)? [Yes] / [No]

### IV.30.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.30.6 Best practice and templates

None

# ARTICLE 32 SECURITY OF PROCESSING

## IV.32.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 32 Security of processing (Chapter IV Controller and processor) |
| GDPR recitals | 83 |
| Cross references | Art. 4 (5); 5 (1) f), (2); 24 (1); 25 (1), (2); 28 (1), (3) c); 30 (1) g), (2) d); 34 (3) a); 35 (7) d); 40 (2) h); 42; 44 |
| Relating documents | Article 29 Data Protection Working Party: Working Paper 216 "Opinion 05/2014 on Anonymisation Techniques" |
| BCRP references | §20 Data security – technical and organizational measures |

## IV.32.2 Content Summary

Controllers and processors, shall implement TOMs to ensure a level of security appropriate to the risk.

## IV.32.3 Binding Interpretations

### STANDARD TOMS AND PSA PROCESS WITHIN THE DT GROUP OF UNDERTAKINGS:

- main IT security objectives, such as confidentiality, integrity, availability and resilience, mentioned in the GDPR, are fully covered by the standard Telekom TOMs (§20 BCRP) and the corresponding security requirements in the PSA process.
- to be able to demonstrate accountability at any time risk evaluation, definition of protection level and documentation of risk mitigation measures are mandatory under the GDPR. The DT Group's PSA process fully covers these obligations.

To be able to ensure compliance with the GDPR and to meet all security requirements under the GDPR at any time the PSA shall be implemented in the currently applicable version provided by GPR (http://drc.telekom.de/en/sec/privacy-security-assessment) in every DT Group undertaking.

### SECURITY OBLIGATIONS FOR THE PROCESSOR:

- liability: where DT undertakings act as a processor (e.g. T-Systems), they are – notwithstanding the contractual obligations – likewise responsible for the security of processing and have to be compliant with the GDPR.

- external controller: where processing is to be carried out on behalf of an external controller not part of the DT Group, certification can be used to demonstrate compliance with the GDPR instead of using the PSA.

### IV.32.4 Compliance Questionnaire

- Is the PSA implemented in the currently applicable version provided by GPR? (Especially Categorization and Initial Consultation (ICG 5), as these PSA tools do provide the privacy risk evaluation.) [Yes] / ]No]
- Do you perform PSA checks on a random basis, in order to check if the documentation and categorisation in the PSA is done correctly? [Yes] / ]No]
- If your undertaking is also a processor for companies outside the group others: Are you able to edhere GDPR requirements and show compliance? [Yes] / ]No]

### IV.32.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.32.6 Best practice and templates

- PSA: https://drc.telekom.de/en/sec/privacy-security-assessment
- PSA-Portal: https://psa-portal.telekom.de/intranet-ui/

# ARTICLE 33 NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

# ARTICLE 34 COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

## IV.33;34.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 33 Notification of a personal data breach to the supervisory authority (Chapter IV Controller and processor)<br><br>Article 34 Communication of a personal data breach to the data subject (Chapter IV Controller and processor) |
| GDPR recitals | 85-88 |
| Cross references | Art. 4 (12); |
| Relating documents | Article 29 Data Protection Working Party: Working paper 213 "Opinion 03/2014 On Personal Data Breach Notification" |
| BCRP references | §23 Right to clarification, comments and remediation<br>§30 Duty to inform in case of infringements *just intragroup not towards supervisory authority* |

## IV.33;34.2 Content Summary

In the case of a personal data breach, the competent supervisory authority must be informed immediately. The controller must also communicate the personal data breach to the data subject where the breach results in a high risk to the data subject's rights and freedoms.

## IV.33;34.3 Binding Interpretations

PERSONAL DATA BREACH:

- **breach of security:** is defined in Art. 4 (12) as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **notification:** the processor shall notify the controller immediately after becoming aware of a personal data breach. The controller or processor becomes aware of a personal data breach if he knows the facts that constitute a personal data breach as defined above. A mere suspicion is not sufficient.

NECESSITY TO NOTIFY TO THE SUPERVISORY AUTHORITY:

- after having become aware of a data breach, the controller must assess if the data breach is likely to result **in a risk or high risk** to the rights and freedoms of data subjects, see Art. 33 (1), 34
  - indicators for a risk are:
    - → the data subject's loss of control over his or her data; processing of special categories of data; automated decisions including profiling; processing of data relating to vulnerable data subjects; large scale processing
  - indicators for a high risk are:
    - → systematic and extensive automated profiling; large-scale processing of special categories of data, large-scale and systematic monitoring of a publicly accessible area
  - the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons:
    - → the data is encrypted; the controller processes only "anonymous data" (not subject to the GDPR); a very minor data breach involving innocuous information about a small number of people only. In these cases the supervisory authority does not have to be notified, see Art. 33 (1).
- the notification is provided by the controller - by the DPO or under the DPO's involvement - to the competent supervisory authority. As the basic rule, the competent supervisory authority is the authority of the Member State where the controller is established (for exemptions see section IV.33.6 „Process Model Incident Management"). Regarding the content of the notification please refer to the template „GDPR Data breach notification", see IV.33.6.
- notification to the supervisory authority must be provided immediately and latest within 72 hours. If later, the notification must include the reasons for the delay.
- If the controller decides not to notify a data breach to the supervisory authority he must be able to demonstrate that the data breach is unlikely to result in a risk for the data subject.

NECESSITY TO INFORM THE DATA SUBJECT:

- a communication regarding the personal data breach to the data subject **is required** where the breach is likely to result in **a high risk** to the data subject's rights and freedoms (examples see above
- **communication** must be provided by the controller to the data subject without undue delay in close cooperation with the relevant authority and the DPO., see Art. 34 (2)
- under certain circumstances immediate actions in cooperation with the DPO have to be taken:
  - → e.g. credit card details or other sensitive information such as passwords for email-accounts are compromised
- the communication has to be provided in clear and plain language. The information has to be communicated at least on the corporate website and depending on the kind of data breach additionally in other ways:
  - → e.g. email, letter, hotline

INFORMATION OF GROUP PRIVACY:

- GPR must receive information from the DPO in these cases, §30 BCRP:
  - potential effect to the public
  - effects more than one undertaking

- potential loss over 500.000,- €.

and with regard to the GDPR if the local or leading authority is located in Germany (for details see "Process model incident management", IV.33.6).

DOCUMENTATION:

- the undertaking that is contacted by the supervisory authority in relation to the incident must document the incident, the processor supports the controller, Art. 28, 29. In addition, all incidents notified to GPR are also documented by GPR.
- the Process Model Incident Management Process and the Data Breach Notification Template must be followed by the undertaking as controller or processor to fulfill the obligation for the controller to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken", Art. 33 (5).

CONSIDERATIONS IN CASE OF A BREACH UNDER THE EPRIVACY DIRECTIVE:

- if the data breach is a breach of security of the electronic communication data respective requirements of the national implementation of the ePD prevail. The requirements for the notification to GPR remain applicable, §30 BCRP.

### IV.33;34.4 Compliance Questionary

- Has your undertaking implemented an incident management process? [Yes] / [No]
- Does your undertaking document any personal data breach in line with the requirements of the GDPR? [Yes] / [No]
- Has your undertaking implemented a data breach communication process? [Yes] / [No]

### IV.33;34.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.33;34.6 Best practice and templates

- Process model incident management:


Process model incident management

- Data breach notification template:

Data Breach Notification Process_f

## ARTICLE 35 DATA PROTECTION IMPACT ASSESSMENT

## ARTICLE 36 PRIOR CONSULTATION

## IV.35;36.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 35 Data protection impact assessment (Chapter IV controller and processor)<br>Article 36 Prior consultation (Chapter IV controller and processor) |
| GDPR recitals | 84, 89-96 |
| Cross references | Art. 39 (1) c) |
| Relating documents | The British Information Commissioner's Office published a Conducting privacy impact assessments code of practice |
| BCRP references | §11 Automated individual decisions<br>§13 Special categories of personal data<br>§31 Review of the level of data privacy<br>§33 Cooperation with supervisory authorities |

## IV.35;36.2 Content Summary

Art. 35 imposes on controllers the obligation to conduct Data Protection Impact Assessments (DPIA) in certain processing situations and defines its requirements. The DPIA is an assessment to identify and minimise noncompliance risks.

Art. 36 obliges the controller to consult the supervisory authorities prior to the processing if a DPIA identifies a high level of unmitigated risk.

## IV.35;36.3 Binding Interpretations

### DATA PROTECTION IMPACT ASSESSMENT:

- implementation of PSA: To be able to ensure compliance with GDPR and to meet all security requirements under the GDPR at any time the PSA shall be implemented in the currently applicable version provided by GPR in every Group undertaking

### FURTHER DETAILS

- DPO: the advice of the designated DPO has to be obtained. The PSA process ensures that all A-categorised processes/systems are assessed by the relevant privacy department.

- risk assessment: The assessment of necessity and proportionality of the processing operations and their risks is part of the first consultation with measures in the PSA process. Therefore, the use of the "GPR-Initial Consultation Guide" is obligatory for all DT Group undertakings.

- relevant processing: in the future a "black" and "white list ", see Art. 35 (4),(5), will be provided by the supervisory authority defining the minimum processing activities being part of the privacy impact assessment. Insofar necessary adoptions will be included in the PSA-portal through change-releases twice a year by the Security Demand Management (SDM).

- approved codes of conduct: approved codes of conduct will be implemented through the central data privacy requirements. Requirements are to be observed by all DT Group undertakings.

PRIOR CONSULTATION:

- consultation of supervisory authority and involvement of DPO: in case of absence of mitigation measures of risks in a high risk data processing, the controller shall inform the supervisory authority prior to the processing. The controller shall align with the DPO of his undertaking in advance in accordance to §28 (7) BCRP.

- involvement of Group Privacy Officer: The Group Privacy Officer shall – in addition – be consulted in case of high relevance for assets of more than one Group undertaking or damages higher than 500.000,- €. Additionally the Group Privacy Officer shall be informed if any changes are made to the laws applying to a undertaking that are significantly unfavorable to compliance with these BCRP, see §. 30 BCRP.

### IV.35;36.4 Compliance Questionnaire

- Is the PSA implemented in the currently applicable version provided by GPR? [Yes] / [No]
- Is the PSA mandatory in your organization with all relevant elements? [Yes] / [No]
- Is a strong linking between the product development processes and the PSA established, which ensures that every new system or product goes through the PSA? [Yes] / [No]

### IV.35;36.5 Sanctions

Article 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.35;36.6 Best practice and templates

- PSA: https://drc.telekom.de/en/sec/privacy-security-assessment

# ARTICLE 37 DESIGNATION OF THE DATA PROTECTION OFFICER

## IV.37.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 37 Designation of the data protection officer (Chapter IV Controller and processor) |
| GDPR recitals | 97 |
| Cross references | None |
| Relating documents | Working Paper 236: Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR). |
| BCRP references | §28 Data Privacy Officer<br>§29 Group Data Privacy Officer |

## IV.37.2 Content Summary

The Article stipulates the cases where a DPO has to be designated by the controller or processor and sets out the different options for such a designation.

## IV.37.3 Binding Interpretations

### GROUP DATA PRIVACY OFFICER AND LOCAL DATA PRIVACY OFFICER:

- the DT Group has appointed the head of GPR as a "Group Data Privacy Officer". Each undertaking of the DT Group shall appoint an independent DPO. Where the undertaking has currently appointed a DPO the existing appointment remains in place.
- the Group Data Privacy Officer can be contacted at datenschutz@telekom.de/privacy@telekom.de and by phone +49-228-181-82001, see Art. 37 (2), §29 BCRP. The contact details of the Group Data Privacy Officer and the undertaking's DPO shall be published by each company internally and externally and be communicated to the supervisory authority, see Art. 37 (1, 7), §28 BCRP.

### SKILLS AND PROFESSIONAL QUALITIES:

- the "International Governance Model Group Privacy Deutsche Telekom AG" (Module 1.1 Skill profile of the Data Privacy Officer, Module 2.1 Responsibilities of the company/management board) and §28 BCRP stipulate the details regarding the skills of the DPOs in the DT Group,see Art. 37 (5).

## VI.37.4 Compliance Questionary

- The Group Data Privacy Officer is designated ? [Yes] / [No]
- A DPO is designated by the undertaking? [Yes] / [No]
- The contact details of the Group Data Privacy Officer and the DPO are published and communicated to the supervisory authority? [Yes] / [No]
- The DPO fulfils the DT Group skill requirements? [Yes] / [No]

### VI.37.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### VI.37.6 Best practice and templates

- International governance model:


International Governance Model.pc

# ARTICLE 38 POSITION OF THE DATA PROTECTION OFFICER

## IV.38.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 38 Position of the data protection officer (Chapter IV Controller and processor) |
| GDPR recitals | None |
| Cross references | Art. 37; 39 |
| Relating documents | Working Paper 236: Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR) |
| BCRP references | §28 Data Privacy Officer<br>§29 Group Data Privacy Officer |

## IV.38.2 Content Summary

The Article stipulates the DPO's rights and the position within the organization of the controller and processor.

## IV.38.3 Binding Interpretations

POSITION AND INVOLVEMENT OF DATA PRIVACY OFFICER:

- the provisions in §§28, 24 BCRP and the „International Governance Model Group Privacy Deutsche Telekom AG" meet the GDPR requirements:

→ e.g. independent DPO, provision of financial and personnel resources necessary, direct reporting line, connected organizationally to the undertaking management, involvement in all data protection issues in a timely manner and the right of the data subject to contact the DPO

- the DPO shall not be dismissed or penalized by the undertaking for performing his task, *see* Art. 38 (3)

## IV.38.4 Compliance Questionary

- Does the DPO have adequate human and financial resources available for implementing national and Group-wide data protection requirements? [Yes] / [No]
  (The DPO should be able to support the business units in privacy related matters and ensure compliance with the privacy regulations within the undertaking.)
- Is there a direct reporting line of the DPO to the undertaking's board of management? [Yes] / [No]

- Are there adequate processes and procedures to ensure that the DPO is involved in a proper and timely manner, in all issues which relate to the protection of personal data? (e.g. PSA) [Yes] / [No]
- Is there a transparent and easy way to contact the DPO (e.g. contact details in the intranet/internet)? [Yes] / [No]
- Does the DPO fulfill other tasks besides DPO function? If yes, do these tasks result in a conflict of interest? [Yes] / [No]

### IV.38.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.38.6 Best practice and templates

- Functional DPO Mail Boxes for the local complaint procedure, e.g. privacy@telekom.de
- International Governance Model:


International Governance Model.pc

# ARTICLE 39 TASKS OF THE DATA PROTECTION OFFICER

## IV.39.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 39 Tasks of the data protection officer (Chapter IV Controller and processor) |
| GDPR recitals | None |
| Cross references | Art. 37; 38 |
| Relating documents | Working Paper 236: Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR). |
| BCRP references | §28 Data Privacy Officer<br>§29 Group Data Privacy Officer |

## IV.39.2 Content Summary

The Article stipulates the tasks and duties of the DPO.

## IV.39.3 Binding Interpretations

GENERAL TASKS OF THE DPO:

- the provisions in §§27, 28, 31, 32, 33 BCRP:

→ e.g. inform and advise on data protection issues and privacy impact assessment, monitoring, training and cooperation with the supervisory authority

and the „International Governance Model Group Privacy Deutsche Telekom AG" (see IV.39.6) together with the PSA process (see IV.35;36.6) meets the requirements regarding the tasks of the DPO, see Art. 39.

MONITOR COMPLIANCE WITH THE DATA PROTECTION REQUIREMENTS:

- every DPO must monitor the compliance with the GDPR and other statutory or internal undertaking/Group requirements for data protection, see Art. 39 (1b), §28 (1) BCRP. The monitoring duties are specified in §31 BCRP.
- the final responsibility and accountability to be compliant with the GDPR lies with the operational management of the undertaking and not with the DPO, see Art. 5 (2)

### IV.39.4 Compliance Questionary

- Do you have a training concept? [Yes] / [No]
- Is the international PSA process integrated into the product and system development processes? [Yes] / [No]
- Choose one of the alternatives:
  - No Implementation of PSA
  - PSA not fully implemented but core requirements
  - PSA fully implemented (Usage of PSA Portal – unchanged Version)
- Do you have implemented a concept to monitor the compliance with the GDPR? [Yes] / [No]
- Do you carry out regular inspections to monitor the compliance with the GDPR, other statutory or internal undertaking/Group requirements for data protection in your undertaking? [Yes] / [No]
- Do you document the regular inspections and is the undertaking's board of management informed about the outcome of the inspections? [Yes] / [No]

### IV.39.5 Sanctions

Art. 83 (4) a): 10.000.000,- € or up to 2% of the total worldwide annual turnover

### IV.39.6 Best practice and templates

- International Governance Model Group Privacy Deutsche Telekom Group:


International Governance Model.pc

- Communication concept and risk plan:


DKIfin_englisch.pdf

- National group policy Organization of data privacy/Assumption of responsibility for data processing:


160303_NGP_OrgPri v_v2_0_Englisch_Fina

# ARTICLE 42 CERTIFICATION

# ARTICLE 43 CERTIFICATION BODIES

## IV.42;43.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 42. Certification (Chapter IV Controller and processor) |
| GDPR recitals | 100 |
| Cross references | Art. 24 (3); 25 (3); 28 (5), (6); 32 (3); 46 (2) f); 83 (4) b) |
| Relating documents | None |
| BCRP references | None |

## IV.42;43.2 Content Summary

Art. 42 sets out the framework for data protection certification. Controller and processor can on this basis demonstrate compliance with the GDPR through approved certification mechanisms, data protection seals and marks.

Art. 43 describes the requirements to be followed when implementing a certification body.

The new concept of certifying data processing operations (see overview certification under IV.42;43.6) may support to realize a reliable and auditable framework for data processing operations. The framework will be developed by the supervisory authorities and the European Commission

## IV.42;43.3 Best practice and templates

- Overview certification


overview_certification.pdf

# CHAPTER V - TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERN. ORGANISATIONS

Articles 44-50

This chapter covers the topic of the transfer of personal data to third countries or international organisations and lists each instrument that can be used as a legal basis for such a cross border transfer. The instruments include the transfer on the basis of an adequacy decision, transfers subject to appropriate safeguards and binding corporate rules. Also covered are data transfers to third countries based on court judgements or decisions of administrative authorities of third countries.

## ARTICLE 44 GENERAL PRINCIPLE FOR TRANSFERS

## ARTICLE 45 TRANSFERS ON THE BASIS OF AN ADEQUACY DECISION

## ARTICLE 46 TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS

## ARTICLE 48 TRANSFERS OR DISCLOSURES NOT AUTHORIZED BY UNION LAW

## ARTICLE 49 DEROGATIONS FOR SPECIFIC SITUATIONS

### V.44-46;48-49.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 44 General principle for transfers (Chapter V Transfers of personal data to third countries or International organisations)<br><br>Article 45 Transfers on the basis of an adequacy decision (Chapter V Transfers of personal data to third countries or International organisations)<br><br>Article 46 Transfers subject to appropriate safeguards (Chapter V Transfers of personal data to third countries or International organisations) |

| | |
|---|---|
| | Article 48 Transfers or disclosures not authorized by union law (Chapter V Transfers of personal data to third countries or International organisations)<br><br>Article 49 Derogations for specific situations (Chapter V Transfers of personal data to third countries or International organisations) |
| GDPR recitals | 101-109, 111-115 |
| Cross references | Art. 4; 6; 40; 42; 47 |
| Relating documents | None |
| BCRP references | §17 Transmission of data |

## V.44-46; 48-49.2 Content Summary

Art. 44 to 49 of the GDPR stipulate the conditions for the international transfer of data to third countries.

The third countries (outside of the EU and EEA[2]) must provide an adequate level of data protection.

The GDPR contains different options how to achieve and assess an adequate level of data protection:

1. adequacy decision from the Commission: the European Commission can decide that a third country, a territory, a sector and international organisations ensure an adequate level of protection, Art. 45
2. appropriate safeguards: data can be transferred to a third country if appropriate safeguards exist, e.g. Binding Corporate Rules (BCR), standard data protection clauses and approved certification mechanisms. Art 46
3. A data transfer to a third country required by a court judgment or a decision by the administrative authorities is only permitted if based on an international agreement, Art. 48.
4. exemptions: in the absence of an adequacy decision or appropriate safeguards, a transfer to a third country is possible if certain conditions are met, e.g. the data subject has explicitly consented to the transfer, Art. 49

## V.44-46; 48-49.3 Binding Interpretations

TRANSFER TO DATA IN A THIRD COUNTRY:

- **permission:** the transfer of data to a third country, including accessing the data from a third country, is permitted if the data processing itself is lawful and an adequate level of protection is provided in the third country where the recipient of the data is established, see Art. 44-49. These rules also apply to the onward data transfer within the third country or to a different third country and regardless of whether

[2] European Economic Area.

the transfer takes place between controller/controller or controller/processor. The lawfulness of the data processing means, that in case of commissioned data processing, in addition to the adequate level of data protection a data processing agreement is required.

- **responsibility:** regardless whether the processor is located in the EU/EEA or not, both controller and processor are responsible for the lawful data transfer

SAFEGUARDS:

- when selecting the appropriate safeguard for the transfer of data to a third country, this procedure should be followed:
  - for a data transfer from a DT Group undertaking to a DT Group undertaking in a third country: The BCRP are signed by the Group undertaking transferring the data and by the Group undertaking receiving the data and provide adequate safeguards. This also applies to an onward transfer to another Group undertaking in a third country.
  - for a data transfer to external companies in third countries: the standard data protection clauses adopted by the Commission must be signed
  - special cases: alignment with GPR or the competent DPO. In principle, the exemptions listed in Art. 49 (1, sentence 2) cannot be used.

### V.44-46;48-49.4 Compliance Questionnaire

- Do you transfer personal data to third countries, or do you allow access to personal data from such countries? [Yes] /[ No]
- If yes, have you checked that a respective adequacy decision exists? [Yes] /[ No]
- If no such decision exists have you made sure that respective safeguards (e.g. BCRP, EU SCC) are in place? [Yes] /[ No]
- Are the necessary transparency (e.g. Art. 13 (1f), 14 (1) f) ) and documentation (Art. 30) requirements met? [Yes] /[ No]
- In case of commissioned data processing do you have a data processing agreement in place? [Yes] /[ No]

### V.44-46; 48-49.5 Sanctions

Article 83 (5) c): 20.000.000,- € or up to 4% of the total worldwide annual turnover

### V.44-46;48-49.6 Best practice and templates

None

# ARTICLE 47 BINDING CORPORATE RULES

## V.47.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 47 Binding corporate rules Article 44 General principle for transfers (Chapter V Transfers of personal data to third countries or International organisations) |
| GDPR recitals | 110 |
| Cross references | Art. 13; 14; 22; 37; 49; 63; 70 (1) c), i); 79 |
| Relating documents | Working Paper 74 Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers;<br>Working Paper 133 Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data<br>Working Paper 153 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules;<br>Working Paper 154 Working Document Setting up a framework for the structure of Binding Corporate Rules ";<br>Working Paper 155 rev04 Working Document on Frequently Asked Questionnaire (FAQs) related to Binding Corporate Rules |
| BCRP references | Binding corporate rules for the protection of personal rights in the handling of personal data within the Deutsche Telekom Group Version 2.7, Last revised Dec. 05, 2013, Status: *final* |

## V.47.2 Content Summary

Art. 47 contains a detailed list of requirements for Binding Corporate Rules (BCR). In accordance with Art. 46 (5), authorisations by a supervisory authority on the basis of Article 26 (2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority. Substantive amendments to the BCRP are to be coordinated with the supervisory authority.

## V.47.3 Binding Interpretations

VALIDITY OF EXISTING BCRP:

- the “Binding corporate rules for the protection of personal rights in the handling of personal data within the DT Group (Version 2.7, Last revised Dec. 05, 2013, Status final)” remain valid.
- the existing BCRP are supplemented by the GDPR Binding Interpretations.

### V.47.4 Compliance Questionary

- Is your local data protection organization fully compliant with Part Four “Data Privacy Organization” of the BCRP? [Yes] / [No]
- Has your undertaking implemented a procedure to report any legal requirements in your country which are likely to have a substantial adverse effect on the guarantees provided by the BCRP to the supervisory authority, Art. 47 (2) m), §33 BCRP? [Yes] / [No]
- Does your undertaking provide appropriate data protection training to personnel having permanent or regular access to personal data, Art. 47 (2) n), §32 BCRP? [Yes] / [No]
- Does your undertaking fulfill all the tasks laid down in the International Governance Model Group Privacy Deutsche Telekom AG? [Yes] / [No]
- Does your undertaking provide information regarding the structure and contact details of the group of undertakings and each of its members to the supervisory authority and the data subject, Art. 47 (2) a), §42 BCRP? Yes] / [No]
- Are there mechanisms in place for reporting and recording changes to the BCRP rules and reporting those changes to the supervisory authority, Art. 47 (2) k)? Yes] / [No]
- Are the measures referred to in Art 47 (2) l), j) documented, Art. 47 (2) l), j), §31 (2) BCRP? [Yes] / [No]

### V.47.5 Sanctions

Art. 83 (5) c): 20.000.000,- €, or up to 4% of the total worldwide annual turnover

### V.47.6 Best practice and templates

- International Governance Model Group Privacy Deutsche Telekom AG:

International Governance Model.pc

- Template Quarterly Reporting GPR International:

Quartely reporting template.pdf

# CHAPTER VIII - REMEDIES, LIABILITY AND PENALTIES

Articles 77-84

The chapter sets out the remedies that are available to the data subjects in the case of processing of their personal data that involves an alleged infringement of the GDPR: right to lodge a complaint with the supervisory authority, right to an effective judicial remedy, right to receive compensation from the controller or processor.

In the case of an infringement of the GDPR supervisory authorities can impose sanctions and administrative fines in a manner that is effective, proportionate and dissuasive. These infringements are subject to a substantially higher level of fines than before. Two different levels of fines are established:

- Up to 10.000.000 EUR or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year.
- Up to 20.000.000 Euro or, in case of an undertaking, up to 4 % of the total worldwide annual tournover of the preceding financial year.

The chapter clarifies under which infringements which level of fines is applicable.

The Member States have the right to implement rules on other penalties in particular for infringements that are not subject to administrative fines pursuant to Art. 83.

## ARTICLE 82 RIGHT TO COMPENSATION AND LIABILITY

### VIII.82.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 82 Right to compensation and liability |
| GDPR recitals | 146, 147 |
| Cross references | Art. 26; 28; 47 (2) e); 62 (5); 80 |
| Relating documents | None |
| BCRP references | None |

### VIII.82.2 Content Summary

Art. 82 specifies the data subject's right to receive compensation from the controller and processor in the case of material and non-material damage suffered as a result of an infringement of the GDPR and looks at the question of the apportionment of liability between controllers and processors. To avoid liability, the

controller or processor must be able to prove that it is not responsible for the event giving rise to the harm. The Article clarifies the rules where more than one controller or processor or both a controller and processor are involved.

### VIII.82.3 Binding Interpretations

GENERAL:

- according to the GDPR the processor has either an independent liability or a several and joint liability towards the data subject. Therefore, it has to be ensured that the fulfillment of the obligations under the contract and the GDPR is granted and sufficiently documented. The proof of the proper fulfillment of these obligations is a precondition to be exempt from liability, see Art. 82 (3).

JOINT AND SEVERAL LIABILITY:

- **to mitigate the risk of liability** in the form of joint and several liability, a clear description of the mutual responsibilities and documented instructions from the controller are crucial. The law requires that the processor shall process the personal data only on the controller's documented instructions in written or electronically, e.g. e-mail, see Art. 28 (3) a), 29. This principle applies accordingly to sub-processors engaged by the processor.
- **to control the remaining** risk of liability in case DT undertaking is deemed to be a joint controller (Art. 82 (4)), the potential contract partner's liquidity must be assessed beforehand. If not in place already, adequate processes must be established.
- **claim back part of compensation:** if part of the damage claimed by the data subject is caused by a DT undertaking and this undertaking is held liable for the entire damage, it has to be ensured that the undertaking claims back that part of the compensation corresponding to their part of responsibility from the other companies involved, see Art. 82 (4, 5)
- **contract clauses will have to be reviewed** insofar as to ensure that they do not contain clauses that allow the contract partners to exclude rights to compensation etc.

### VIII.82.4 Compliance Questionnaire

- Do you conduct an internal risk assessment? [Yes] / [No]
- Does the DTAG/affiliate-undertaking evaluate whether the service, the product or other influences (e.g. partner, sub-processor, or company as a joint controller) is acceptable or nonacceptable in consideration of the possibility of liability and indemnification for damages and an unquantifiable amount of loss? [Yes] / [No]
- Do you evaluate the undertaking internal approval processes ? [Yes] / [No]
- The potential risk must be considered to be jointly and severally be liable for any damage (used with adhesion ratio of the subcontractor or partner (also "joint controller" )? [Yes] / [No]
- Do you agree on contractual clauses regarding compensation and liability? [Yes] / [No]
- Do you restrict compensation and liability (to the extent legally possible – direction to contractual partner)? [Yes] / [No]
- Do you use clauses to claim back compensation from contractual partners ? [Yes] / [No]

- Do you check if it is possible to use exculpation-clauses for cases where you can define your responsibility for the event giving rise to the damage and your area of responsibility is clearly defined? [Yes] / [No]
- Did you document the review of the contractual service/product for being compliant with the GDPR? [Yes] / [No]

### VIII.82.5 Sanctions

None

### VIII.82.6 Best practice and templates

None

# ARTICLE 83 GENERAL CONDITIONS FOR IMPOSING ADMINISTRATIVE FINES

## VIII.83.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 83 General conditions for imposing administrative fines (Chapter VIII Remedies, liability and penalties) |
| GDPR recitals | 148, 150-151 |
| Cross references | Art. 58; 78; 79; 82; 84 |
| Relating documents | None |
| BCRP references | §5 Duty to inform<br>§22 Right of protest, right to have data erased or blocked, and right to correction |

## VIII.83.2 Content Summary

The supervisory authorities are empowered to impose significant administrative fines in addition to, or instead of, measures of the supervisory authority according to Art. 58 (2). Fines can be imposed up to 10.000.000,- € or 2 % of the total worldwide annual turnover of the preceding financial year (e.g. obligations of the controller and the processor such as data protection by design, privacy impact assessment, maintenance of registers) or up to 20,000,000,- € or 4 % of the total worldwide annual turnover of the preceding financial year (e.g. conditions for consent, data subjects rights, international data transfer, non compliance with supervisory authorities), depending on the type of infringement.

## VIII.83.3 Binding Interpretations

FACTORS DETERMINING THE LEVEL OF FINE:

- to mitigate the risk to be fined measures to ensure compliance with the GDPR like BCRP and approved certification mechanisms are of importance in every individual case, because the supervisory authorities will take them into account when deciding on the amount of the administrative fine, see Art. 83 (2) GDPR
- where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.
- when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine the supervisory authority may give regard to the following :

- if an infringement of the GDPR is caused by an individual Group undertaking, due to its own operational setting, the amount of the fine shall be subject to the turnover of the undertaking concerned
- if the infringement has its source in the governance of the Group then the fine shall be subject to the turnover of the Group

- besides the fines in Art. 83 there are still other penalties – including personal responsibility of employees under civil and criminal law – possible.

### VIII.83.4 Compliance Questionnaire

- Have you considered where approved certification mechanisms in your organization do make sense in the light of the Regulation, esp. Art 83 GDPR? (e.g. key processes with most crucial data.) If yes, are you prepared for further certifications? Do you have the necessary documentations? (Best Practice: SDSK of the PSA) [Yes] / [No]
- Have you updated your risk registers, regarding the increased fines? [Yes] / [No]

### VIII.83.5 Sanctions

None

### VIII.83.6 Best practice and templates

- BCRP: https://drc.telekom.de/en/privacy/themen/binding-corporate-rules-privacy/171386

# CHAPTER IX - PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Articles 85-91

The chapter introduces provisions relating to specific processing situations, e.g. processing in the context of employment, processing and public access to official documents, processing for archiving purposes in the public interest, processing by a controller or processor that is subject to obligations of secrecy. In the context of processing in these situations, the GDPR leaves it to the Member States to adopt their own national rules.

## ARTICLE 88 PROCESSING IN THE CONTEXT OF EMPLOYMENT

### IX.88.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 88 Processing in the context of employment (Chapter IX provisions relating to specific processing situations) |
| GDPR recitals | 155 |
| Cross references | Art. 4 (18), (19) |
| Relating documents | None |
| BCRP references | None |

### IX.88.2 Content Summary

Member State law or collective agreements (including works agreements) can provide more specific rules and procedures for data processing in the employment context.

### IX.88.3 Binding Interpretations

EXISTING COLLECTIVE AND WORK AGREEMENTS:

- have to be aligned with the GDPR and respective Menber State law until May 2018

TRANSFER OF EMPLOYEE DATA:

- Art. 88 (2) GDPR explicitly provides for the possibility to stipulate the transfer of employee data within the group of undertakings, in collective and work agreements

### IX.88.4 Compliance Questionnaire

- Are the collective and work agreements that are in place in your company aligned with the GDPR and respective Member State law? [Yes] / [No]

### IX.88.5 Sanctions

None

### IX.88.6 Best practice and templates

None

# CHAPTER XI - FINAL PROVISIONS

Articles 94-99

The last chapter contains the final provisions, e.g. repeal of Directive 95/46/EC, relationship with the ePD as well as entry into force and application.

## ARTICLE 94 REPEAL OF DIRECTIVE 95/46/EC

## ARTICLE 99 ENTRY INTO FORCE AND APPLICATIONS

### XI.94., 99.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 94 Repeal of Directive 95/46/EC (Chapter XI Final provisions)<br><br>Article 99 Entry into force and applications (Chapter XI Final provisions) |
| GDPR recitals | 171 |
| Cross references | Art. 7 |
| Relating documents | None |
| BCRP references | None |

### X.94;99.2 Content Summary

The GDPR entered into force on 24th May 2016. It must be applied from 25th May 2018. Directive 95/46/EC is repealed with effect from 25th May 2018.

### X.94;99.3 Binding Interpretations

GDPR IMPLEMENTATION AND CONFORMITY:

- during the period of two years when the GDPR entered into force and the date of application every processing of personal data in DT Group must be brought into conformity with the GDPR
- the Binding Interpretation for selected GDPR Articles contained in this document must be followed

EXISTING CONSENT:

- where processing is based on consent, it is not necessary to renew the data subject's consent after the date of application of the GDPR if two conditions are met:
  - the existing consent has been given pursuant to Directive 95/46/EC and
  - the manner in which the existing consent has been given is in line with the conditions of the GDPR, Art. 6 (1) a), 7, 8, 9 (2) a)
- due to the binding character of the GDPR, these requirements apply Group wide without exemptions. There is no room for national deviations.
- the same applies to consent given in ePrivacy related matters. According to Art. 2 (f) of the ePD, consent by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC without imposing additional requirements regarding the form of consent, see Art. 88

APPLICATION OF THE GDPR:

- the GDPR or parts of the GDPR may not be applied before 25th May 2018

### X.94;99.4 Compliance Questionary

- Is the data subject's existing consent to your undertaking in line with the conditions of the GDPR? [Yes] / [No]
- Has your company applied the Binding Interpretation for GDPR Articles contained in this document? [Ye]s / [No]

### X.94;99.5 Sanctions

None

### X.94;99.6 Best practice and templates

None

# ARTICLE 95 RELATIONSHIPS WITH DIRECTIVE 2002/58/EC

## XI.95.1 General Information

| Topic | Reference |
|---|---|
| GDPR article | Article 95 Relationships with Directive 2002/58/EC (Chapter XI Final provisions) |
| GDPR recitals | 173 |
| Cross references | None |
| Relating documents | None |
| BCRP references | None |

## X.95.2 Content Summary

The GDPR applies to all matters concerning the protection of fundamental rights and freedoms *vis-à- vis* the processing of personal data which are not subject to specific obligations with the same objective set out in the ePD. The ePD contains specific rules for the processing of personal data in the telecommunication and electronic communication sector.

## X.95.3 Binding Interpretations

RELATIONSHIP EPD AND GDPR:

- if the processing of personal data is subject to both GDPR and ePD, the provisions of the national laws based on the ePD prevail
- the ePD sets out the rules for processing of personal data in the telecommunication and electronic communication sector and special provisions relate to e.g. incident reporting, direct marketing, processing of location and traffic data
- the GDPR does not impose additional obligations on a group undertaking in relation to the ePD

REVIEW OF THE EPD:

- is in progress in order to ensure consistency with the GDPR

## X.95.4 Compliance Questionary

- Does your undertaking process telecommunication and/or electronic communication data? [Yes] / [No]
- If the answer was "Yes" to the previous question: Does your company have an incident reporting process in place to report incidents that fall under the scope of the ePD? [Yes] / [No]

### X.95.5 Sanctions

None

### X.95.6 Best practice and templates

- Template for incident reporting on the basis of the ePD and process:


Process model
incident management

# 3. ENCLOSURES

## DEFINITIONS

| Term | Definition |
|---|---|
| 'biometric data' | Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; |
| 'binding corporate rules' | Means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity; |
| 'CAPE' | See: https://mywiki.telekom.de/pages/viewpage.action?pageId=10485770 |
| 'consent' | of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; |
| 'controller' | Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are de- termined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; |
| 'cross-border processing' | Means either:<br><br>(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or<br><br>(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. |

| | |
|---|---|
| 'data concerning health' | Means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status; |
| 'Deutsche Telekom Group' | Shall mean Deutsche Telekom AG and all undertakings in which Deutsche Telekom AG directly or indirectly holds more than a 50% share, or which are fully consolidated. See also Part Seven BCRP 'Definitions and Terms' |
| 'direct marketing' | Means targeted advertising by using such as e-mail, post address, phone number. |
| 'electronic communication data' is part of the 'electronic communication service' | Means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks; |
| 'enterprise' | Means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity; |
| 'filing system' | Means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis; |
| 'genetic data' | Means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question; |
| 'group of undertakings' | Art. 4 (19) Means a controlling undertaking and its controlled undertakings |
| 'information society service' | Means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council1; |
| 'international organisation' | Means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. |
| 'main establishment' | Means:<br><br>(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the |

| | |
|---|---|
| | power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;<br><br>(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation; |
| 'personal data' | Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; |
| 'personal data breach' | Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; |
| 'processing' | Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |
| 'processor' | Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; |
| 'profiling' | Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; |
| 'recipient' | Means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing; |

| | |
|---|---|
| 'relevant and reasoned objection' | Means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the funda- mental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union; |
| 'representative' | Means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation; |
| 'restriction of processing' | Means the marking of stored personal data with the aim of limiting their processing in the future; |
| 'supervisory authority' | Means an independent public authority which is established by a Member State pursuant to Article 51; |
| 'supervisory authority concerned' | Means a supervisory authority which is concerned by the processing of personal data because:<br><br>(a) the controller or processor is established on the territory of the Member State of that supervisory authority;<br><br>(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or<br><br>(c) a complaint has been lodged with that supervisory authority; |
| 'third party' | Means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data; |
| 'pseudonymisation' | Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; |
| 'undertaking' | No definition in the GDPR. The term is used in a variety of contexts in the GDPR, most often to refer to a legal entity that is engaged in economic activities in a group of undertakings.<br>In the context of this document the term 'undertaking' stands for e.g. NATCO, LBU or fully consolidated Deutsche Telekom Group subsidiary. |

## ABBRIVIATIONS

| Term | Abbreviation |
|---|---|
| Art. | Article |
| BCR | Binding Corporate Rules |
| BCRP | Binding Corporate Rules Privacy |
| BDSG | Federal Data Protection Act |
| CAPE | The software CAPE is part of the certification, according to the „Assurance-Standard 980" of the Privacy-Compliance-Management-System of DT Group.) |
| CDPA | Commissioned Data Processing Agreement |
| CSV | Computer system validation |
| DPA | Data Protection Agreement |
| DPIA | Data protection impact assessments |
| DPO | Data protection officer |
| DT | Deutsche Telekom |
| EEA | European Economic Area |
| E.g. | For example |
| ePD | ePrivacy Directive |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| GPR | Group Privacy |
| KEK | Consent clause across the group |
| LBU | Local Business Unit |
| NatCo | National Company |
| PSA | Privacy and Security Assessment |
| Rec. | Recital |
| SDM | Security Demand Management |
| SDSK | Standardized Data Privacy & Security Concept |
| Tbd. | To be defined |
| TOMs | Technical and organizational measures |

# 4. ANNEX

GDPR - Text.docx


BCRP.pdf


Arbeitsbericht_der_a
d-hoc-Arbeitsgruppe_


Commission_Recomm
endation_of_10.10.2


ICO_privacy_impact
_assessement


Information_Commis
sioner's_Office_„Data


Working_Paper_74


Working_Paper_133


Working_Paper_153


Working_Paper_154


Working_Paper_155


Working_Paper_169


Working_Paper_187


Working_Paper_203


Working_Paper_213


Working_Paper_216


Working_Paper_217


Working_Paper_223


Working_Paper_225


Working_Paper_236