# GUIDELINE

## FOR THE DESIGN OF AI-SUPPORTED BUSINESS MODELS, SERVICES AND PRODUCTS AT DEUTSCHE TELEKOM IN COMPLIANCE WITH DATA PRIVACY REGULATIONS

Group Headquaters, Group Privacy

Version 1.0
Stand 07.12.2018
Status *final*

LIFE IS FOR SHARING.

# CONTENTS

# 1 PRELIMINARY NOTES

In order to provide a starting point for the development of practicable data privacy specifications for AI systems at Deutsche Telekom, the broad public discussion on artificial intelligence was focused on the current data protection requirements of Deutsche Telekom.

This guideline is intended for product and business model managers, developers, Privacy and Security Assessment (PSA) requesters of systems and projects with an AI component and data privacy experts.

According to the General Data Protection Regulation (GDPR), a distinction can be made between AI systems which, as assistance systems, support people in their decisions and systems which make decisions independently (automated individual decisions). The GDPR applies to AI-supported assistance systems. Article 22 GDPR contains special regulations for so-called ADM systems (Algorithmic Decision Making).

Irrespective of this legal differentiation between different AI solutions, Deutsche Telekom applies uniform governance to AI projects that covers both AI assistance systems and ADM systems.

This guideline is intended to provide the necessary orientation and security of action for the operationally responsible body in the phase between the business or product idea and the PSA procedure.

# 2 GENERAL QUESTIONS

## 2.1 What is artificial intelligence?

Current AI systems represent a combination of analysis systems based on formalized expert knowledge (Data Warehouse, Business Intelligence) and machine learning as well as the targeted application of what has been learned. In the algorithmic decision-making process, which is regularly used as the basis for an AI, an assessment is made on the basis of information, which leads to a decision, forecast or recommendation for action. Thus, not only the data processing itself, but in particular the decision as a consequence of the processing bears a potential risk for the data subject.

The classical IT with its elements "input" - "processing" - "output" is extended by the abilities "perceiving" - "understanding" - "acting" - "learning"[1]. These characteristics, which until now have only been assigned to humans, can now also be performed by machines to an increasingly greater extent. The term "understanding" is new territory in connection with computers and must be critically accompanied with regard to traceability and adherence to ethical values. Machine learning refers to a series of optimization methods in artificial neural networks, among others. AI systems can have very complex structures between the input and output layers. By mapping several hierarchical processing layers, machine learning can become considerably more efficient (Deep Learning). However, this inevitably results in a loss of traceability in AI decisions. Due to the complexity of the algorithms and the multitude of arithmetic operations performed by the machine, the deeper processing layers (hidden layers) elude transparency in the decision criteria and their weighting. Although the disclosure of the algorithms on which the AI is based is a core demand in the current debate about more transparency in AI systems, the concrete verification of the decision logic of highly complex AI systems on the basis of disclosed algorithms is likely to be difficult in practice. "Explainable AI systems" is an approach that is currently being intensively researched. In future, it would be desirable for AI systems to provide information regarding the decision criteria and their weighting in decisions beside the factual results of an AI based data processing.

[1] see also: Bitkom position paper: https://www.bitkom.org/sites/default/files/file/import/FirstSpirit-1496912702488Bitkom-DFKI-Positionspapier-Digital-Gipfel-AI-und-Entscheidungen-13062017-2.pdf

**It is more practical at this stage to monitor the decision-making processes of AI systems from "outside", where the decisions taken by the AI are reviewed against a pre-determined purpose of the system and ethics governance.**

AI decisions that are outside the expected range can be identified and intervention can be taken. Tools developed specifically for the analysis of AI decisions can help. However, the principle applies, that monitoring machines exclusively by machines is paradoxical. Human judgements must always dominate AI monitoring processes.

In addition to the efficiency of the learning mechanisms, successful machine learning depends not least on the quantity and quality of the available data. The "Big Data" trend in IT and the mass availability of data are currently significantly accelerating the development of AI systems.

**Transparency of data sources used and the lawfulness of their processing in AI systems are therefore key data privacy requirements.**

The very complex psychological and emotional processes of human knowledge and decisions are likely to remain hidden from the machines for some time to come. When evaluating and weighing up data privacy law, it must therefore be borne in mind that machine decisions are based on different principles and mechanisms than those applied to human decisions.

In order to achieve the necessary security in dealing with AI systems, comprehensive ethical and legal governance for AI decisions must be effectively implemented.

All ethical rules of conduct agreed in the Group and all compliance requirements that are binding for organizational units and every employee must also form the basis for decisions on AI systems.

## 2.2 Which specific data privacy legal questions need to be clarified within the case of AI-projects?

In the Group, we design data privacy-compliant Big Data, BI, Data Warehouse and Data Analytics systems on a daily basis and have sufficient experience and specifications in dealing with data protection issues relating to these IT processes. With AI systems and AI-supported business models, of course, all these existing data protection requirements must be applied and complied with. This applies in particular to the question of the permissibility of the processing of personal data.

In addition, the following specific questions essentially arise in the evaluation of AI systems under data protection law:

**1. How are transparency and action rights of the user / data subject guaranteed?**

Contracts and customer processes must be designed in such a way that the type and scope of the share of AI-supported decisions is transparent. It must therefore be clear whether an AI system is being used and how big the part of the decisions making process of the AI actually is.
The legally required objection and complaint possibilities must be implemented processually in the business model and should be useable in a simple way.

**2. How is (internal) transparency regarding AI decisions ensured and how do we control and monitor AI systems?**

As part of a balancing process, an appropriate control method and monitoring intensity must be established for the decisions of an AI system. It must be checked whether decisions made / recommended by the AI system are in line with the previously defined purpose of the AI system, the needs of the data subject and the ethical principles of our company. Ethical principles are all rules of conduct that we have established in our company for dealing with each other and with our customers. These include, in particular, the respectful handling of personal rights, fairness, non-discrimination, social participation and pluralism.

In our opinion, AI systems are compliant to data privacy regulations if,

- the lawfulness of the processing of all data (sources) is guaranteed,
- the use of Artificial intelligence is sufficiently transparent to all participants,
- There are possibilities for regulation in the case of allegedly existing wrong decisions,
- the decision-making processes of AI systems are regularly monitored and
- it can be ensured that any decision taken by the AI is always in line with the Group's Digital Ethics Guidelines.

In order to comply with the transparency requirements of the GDPR for AI systems, the user must be able to rely on the fact that the ethical principles for AI decisions are transparent, observed and effectively monitored. The specialist´s project responsibility also includes the mapping and implementation of the transparency and control processes required for this

# 3 CONCRETE DATA PRIVACY REQUIREMENTS OF THE GROUP DURING THE DESIGN OF AI PROJECTS

Deutsche Telekom has committed itself to a transparent and people-centric approach to AI systems under the aspect of "digital responsibility" in nine guidelines.

https://www.telekom.com/en/company/digital-responsibility

In the following, Group Privacy specifies the data protection requirements that apply to the individual guidelines:

**We are responsible.**

- The purpose of the AI system used must be finally determined and documented;
- The responsibilities for the business model / product are clearly defined. The responsibility for purchasing, development and proper operation of the AI elements is also clearly assigned;
- The legality of the use of all used data sources as well as the data is proved and documented.

**We care.**

- In order to control the decisions of the AI system, an appropriate and effective monitoring process has to be implemented by the responsible technical unit. The monitoring process must at least meet the following requirements:
  - Data subjects affected by the AI decision may address a complaint. The AI's decision that gave reason to the complaint must be reviewed with regard to the compliance with the agreed business purpose and for compliance with Group governance. The decision must be made comprehensible to the complainant and, in case of doubt, corrected.
  - All employees entrusted with the operation of the AI system are particularly sensitized with regard to the range of expected decisions of the AI system within the scope of the intended purpose and the relevant governance requirements. If the employees have indications for a deviation of the AI decisions from the specified decision range, immediate intervention must be possible ("emergency stop button"). The causes of the detected deviations must be identified and documented. If necessary, corrective measures must be implemented before the AI system is resumed.
  - Depending on the criticality of the processed data or the scope of the decisions made by the AI system, the responsible professional unit shall review the AI system at regular intervals. The decisions of the AI system are to be checked for compliance with the governance requirements. The result must be documented. The type and scope of the checks to be carried out are agreed between the technical responsible unit and GPR within the framework of the PSA process and are mapped processually in regular operation.
- For each AI project, a data privacy impact assessment must be carried out as part of the PSA procedure. Risks have to be analyzed and measures for risk reduction have to be defined and implemented in the project.

**We put our customers first.**

- The highest benchmark for the design of AI-based business models is the integrity of the personal rights of the affected customers or employees. If personality rights are impaired, trust is lost. Without trust, there is no business success and the reputation of the Group is damaged. AI solutions are therefore conceived and developed by the customer’s/employee’s point of view.

**We are transparent.**

- It must be transparent to Customers and employees at all times as to whether they communicate with an AI system and what part the AI system plays in decisions making process.
- It must be transparent to Customers and employees as to which of their data is processed in an AI system and for what purpose.
- It must be possible to question AI decisions by the data subject and to explain the decision in a comprehensible way

**We are secure.**

- In addition to the requirements specifically mentioned here, all data privacy and data security requirements established in the Group also apply when designing AI-supported business models and products.
- The Privacy and Security Assessment (PSA) procedure is mandatory for all AI-based business models and products.

**We set the grounds.**

- The development of our own AI systems must take the ethical and legal requirements for our Group into account at the development stage (Privacy by Design, Ethic by Design, Transparency by Design).
- Purchased AI systems must be able to comply with our ethical and legal requirements in practical operation. If this is not guaranteed, the product cannot be used. This must be evaluated and documented before using external AI systems.

**We keep control.**

- Irrespective of the monitoring processes mentioned above, AI systems and their operating processes must be designed in such a way that immediate intervention to prevent or reduce damage is guaranteed.

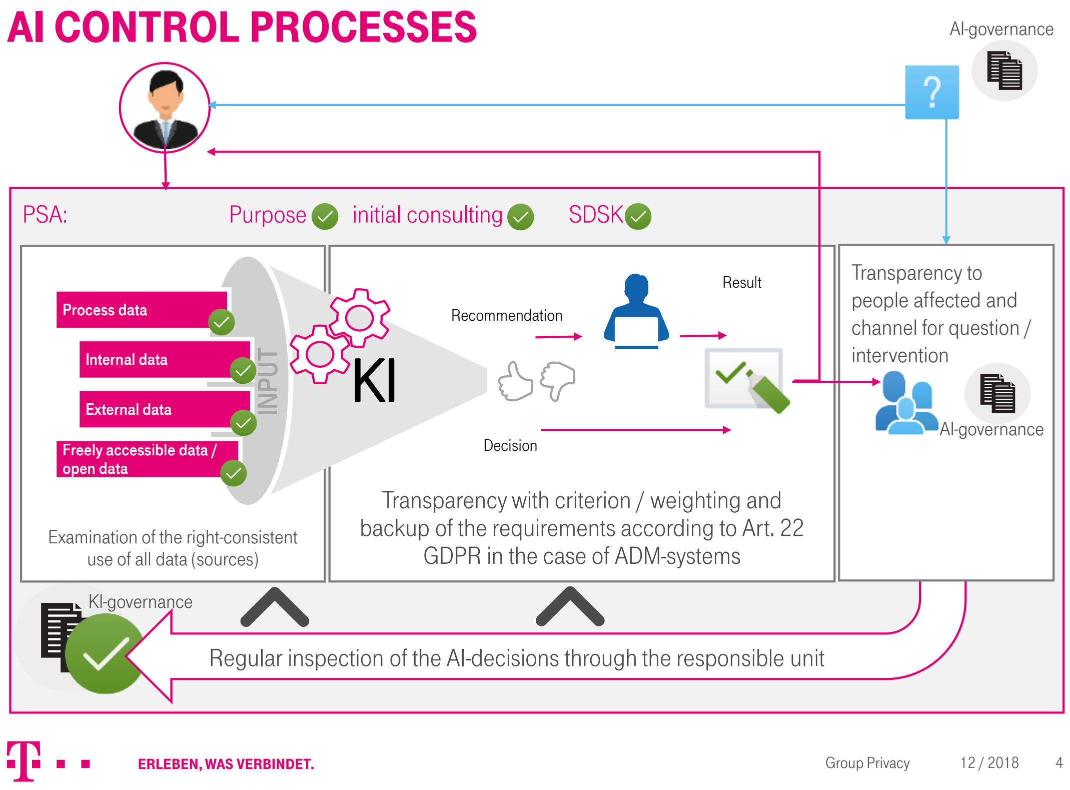
**We foster the cooperative model.**

- To regard humans and their personal rights as a benchmark for the design of AI systems does not exclude far-reaching cooperation between humans and machines. Through innovative ideas and the consideration of human interests already in the planning and development of AI business models and products, we are able to establish standards that ensure lasting trust in Deutsche Telekom's products and enable fruitful cooperation between human and machine.

**We share and enlighten.**

- We share our ideas for a privacy-compliant design of AI business models and products with others and thus promote our high standards.

# 4 THE CONTROL PROCESSES



AI CONTROL PROCESSES

Examination of the right-consistent use of all data (sources)

Transparency with criterion / weighting and backup of the requirements according to Art. 22 GDPR in the case of ADM-systems

Transparency to people affected and channel for question / intervention

Regular inspection of the AI-decisions through the responsible unit

ERLEBEN, WAS VERBINDET.

Group Privacy 12 / 2018 4

The following process-related requirements must be mapped by the responsible operational departments:

- Ensure and monitor transparency regarding the AI component in the business model and the established control processes vis-à-vis the data subject.
- Ensure and monitor impact and complaint processes for all parties involved in data processing.
- Monitoring of AI decisions for compliance with the defined purpose of the system and AI governance.

# 5 PRIVACY ASSESSMENT AI

Due to the limited scope of application of data privacy standards, the data privacy framework is always only a sub-area that must be considered within the framework of an AI and the underlying processes and which standardizes the relevant requirements. Procedures that are based from the outset or due to corresponding measures (anonymization) on information that has no personal reference fall outside the scope of data privacy regulations (e.g. GDPR). In addition, data privacy standards primarily aim at the protection of individual rights of the individual. Group- or company-related goals, such as non-discrimination and participation, are regularly not safeguarded. However, in the area to which the provisions of the GDPR apply, there are already sufficient regulations and requirements concerning AI and the underlying algorithmic decision-making procedures. There are both specific standards dealing with these procedures and general principles and requirements of data privacy to be observed due to the processing of personal data in the context of AI.
There are roughly two types of algorithmic systems. Art. 22 GDPR contains specific provisions on systems that evaluate people and make algorithmic decisions (Algorithmic Decision-Making Systems, or ADM systems for short).

This must be distinguished from decision support systems, which "only" support the decision maker in the human decision and only serve to prepare human decisions (Decision Support Systems, or DS systems for short). The latter can be used to any extent within the framework of the general requirements of the GDPR.

From the data privacy point of view, it is therefore initially decisive whether the scope of data privacy law has been opened up.

*Definition: Personal data and/or personal related data*

Then - as with any data processing - the general requirements of the GDPR must be observed. Here, reference can be made to already existing guidelines, e.g. on Big Data. The specific requirements of Art. 22 GDPR on automated individual decision-making (including profiling) apply only in the event that an ADM system is also used within the framework of the AI, i.e. algorithm-based decisions are made automatically and not merely prepared.

## 5.1 Basic principle: Prohibition of an automated individual decision-making

Pursuant to Art. 22 GDPR, individuals have the right not to be subject to a decision based exclusively on automated processing - including profiling - which has legal effect on them or significantly affects them in a similar manner. Profiling is defined in Art. 4 para. 4 GDPR and forms a subset of the automated individual case decision.

### 5.1.1 Exclusively automated processing

Art. 22 GDPR therefore only covers systems in which the decision is based "exclusively on automated processing" without any human influence. However, the possibility of influencing or involving humans must not be merely a formal act but must offer scope for co-responsibility in terms of content, i.e. humans must also be able to decide against the recommendation without fear of disadvantages.

### 5.1.2 Legal effect or considerable detraction

Furthermore, the decision must have a legal effect vis-à-vis the data subject or significantly affect him or her. A "legal effect" can always be said to exist if the decision changes the legal position of the data subject. A "considerable impairment" can always be assumed if the economic or personal development of the data subject is significantly disturbed.

### 5.1.3 Exceptions

According to Art. 22 para.2 GDPR, systems of automated decisions are "exceptionally" permissible if (a) the decision is necessary for the conclusion or performance of the contract between the data subject and the data controller, (b) the ADM decision has been declared admissible by a statutory provision in the data subject's country, or (c) the decision is made with the data subject's express consent.

### 5.1.4 Special categories of personal data

Art. 22 para. 4 GDPR provides a special limit for the admissibility of ADM systems: The use of special categories of personal data within the meaning of Art. 9 para.1 GDPR may not be used for automated decision-making - unless the data subject has consented or EU or national legislation permits this for reasons of substantial public interest.

### 5.1.5 Adequate protective measures

If an automated individual decision is finally exceptionally permissible under Art. 22 para. 2 or para. 4 GDPR, Art. 22 para. 3 GDPR lays down specific requirements with regard to accompanying appropriate measures "in order to safeguard the rights and freedoms as well as the legitimate interests of the data subject" Art. 22 para. 2 b, para. 3 and para. 4 GDPR. Article 22 para. 3 and recital 71 of the GDPR provide guidance on these measures. These are procedural measures and technical measures.

Procedural measures:

- Right to request the intervention of a person
- Right to express one's own point of view
- Right to appeal against a decision

Contrary to the wording, it will probably be assumed that these rights must not be granted unconditionally, but for legitimate reasons in individual cases.

Examples of technical measures:

- Appropriate mathematical or statistical methods
- Technical and organizational measures to avoid incorrect personal data
- Regular review of the data records and the procedure (audit algorithms if necessary)
- Test routines during development and operation

Further details can also be derived from the opinion of the Article 29 Working Party (October 2017).[2]

## 5.2 Basic principles of the processing

Both with regard to the processing of personal data within the framework of ADM systems and with regard to systems such as DS systems which do not fall under the special requirements of Art. 22 GDPR, the principles of processing personal data within the meaning of Art. 5 GDPR must be observed. These principles are in turn substantiated by a number of individual provisions in the GDPR.

These include legality, transparency, purpose limitation, accuracy, integrity and confidentiality of the processing and accountability.

## 5.3 Transparency

The transparency obligations include the obligation to inform the data subject about the data processing (Art. 13 and 14 GDPR). The information duties are intended to ensure that the data subject learns about the data processing and its scope so that he or she can effectively exercise his or her rights.

In the case of automated decision-making pursuant to Art. 22 para.1 and para.4 GDPR, the data subject must be informed that an ADM system is being used. In addition, "meaningful information on the logic involved and the scope and desired effects of such processing for the data subject" is required (Art. 13 para. 2 lit. f and Art. 14 para. 2 lit. g GDPR).

Since the right of the data subject to obtain meaningful information is regularly opposed in this case to the legitimate interest of the responsible party in the protection of his business secrets (also recital 63 GDPR), this does not automatically mean that the algorithm of the procedure must be communicated. However, the purpose and criteria to be taken into account in decision-making should be disclosed (see also Article 29 Working Party).

The principle of proportionality will also have to be applied. The transparency obligations also include the right to information pursuant to Art. 15 GDPR, according to which the data subject has the right to demand information from the person responsible about the purpose and scope of the data processing. The right to information is intended in particular to enable the data subject to check whether the data are being processed lawfully. In the case of automated decision-making pursuant to Art. 22 para.1 and para.4 GDPR, the information must also contain "meaningful information on the logic involved as well as the scope and intended effects of such processing on the data subject" (Art. 15 (1) lit. h GDPR).

It should be noted that the legal wording allows considerable scope for interpretation, so that it can be assumed, that just abstract information about the system functionality is required and not the disclosure of the algorithm.

However, if a Decision Support System (DS-System) is used which merely supports or recommends decisions, the special transparency obligations of Art. 13 para. 2 lit. f or Art. 14 para. 2 lit. g GDPR are not applicable.

A special legal framework applies to automated individual decision-making in the field of public administration, where statutory provisions already provide for an obligation to state reasons with regard to the comprehensibility of a decision.

[2] „Guidelines to automatized decisions on an individual basis including profiling for the purposes of the regulation2016/679“, WP251 rev01 - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

### 5.4 Data privacy impact assessment

If data processing is likely to pose a high risk to the rights and freedoms of data subjects, the data controller must first carry out a data privacy impact assessment (Art. 35 para. 1 GDPR). The data privacy impact assessment is thus an important instrument for fulfilling the obligation under Art. 5 para.2 GDPR to demonstrate compliance with the GDPR ("accountability"). In addition, the data privacy impact assessment has the function of an early warning system and a risk analysis which can prevent a potential violation of personal rights. Within this framework, a certain degree of documentation of the underlying algorithms will be required - especially in order to be able to carry out a sufficient risk assessment.

In the case of automated decision making (ADM system), the data privacy impact assessment is generally mandatory under Art. 35 para. 3 lit. a GDPR - but in the view of the Article 29 Data Protection Working Party, constellations are also covered in which the algorithm is only used in preparation for decision support (DS systems). The Data Protection Conference (body of the German data protection supervisory authorities) has published a list of processing operations for which a data privacy impact assessment must always be carried out in accordance with the provisions of Article 29 of the Data Protection Working Party[3]. If it emerges from the data privacy impact assessment that the processing would result in a high risk for the rights and freedoms of the data subjects, provided that the data controller does not take measures to contain the risk, there is finally an obligation to consult the supervisory authority pursuant to Art. 36 (1) GDPR.

The necessary data protection impact assessment is part of the Privacy and Security Assessment (PSA) procedure.

# 6 EXISTING REQUIREMENTS TO BE OBSERVED WHEN VALUATING AI PROJECTS

### 6.1 General specifications

The Privacy and Security Assessment (PSA) must be completed for all IT/NT systems in the Group and for all Telekom products.

### 6.2 BigData

Whitepaper Group Privacy on data privacy compliant design of data-driven business models.

OnePager for data privacy compliant design of data-driven business models.

Guiding principles of Deutsche Telekom for BigData:
https://www.telekom.com/resource/blob/323582/dcd78db4c7aef740430249974179e703/dl-guiding-principles-big-data-data.pdf

[3] https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

# 7 OVERVIEW OF ALL DATA PRIVACY LEGAL REQUIREMENTS

All specific requirements from this guide in the overview:

## 7.1 Before realization of the Privacy and Security Assessment (PSA)

- The purpose of the AI system is conclusively determined.
- The responsibilities for the business model / product / IV processes are clearly defined.
- The planned use of the AI solution is conceived and developed by the customer's/employee's point of view.
- Purchased AI systems must be able to comply with our ethical and legal requirements in practical operation. If this is not guaranteed, the product cannot be used. This must also be evaluated and documented before using external AI systems.

## 7.2 During the Privacy and Security Assessment

- The lawfulness of the processing of all data (sources) is guaranteed.
- An appropriate and effective monitoring process has been implemented to monitor the decisions of the AI system.
- A data privacy impact assessment was carried out for the project.
- The development of our own AI systems must take the ethical and legal requirements of our Group into account at the development stage (Privacy by Design, Ethic by Design, Transparency by Design).
- AI systems and their operational processes must be designed in such a way as to ensure immediate intervention to prevent or reduce damage is possible.

## 7.3 On completion of the Privacy and Security Assessment

- It must be transparent at all times to Customers and employees as to whether they communicate with an AI system and what part the AI system plays in decisions made.
- Customers and employees must be transparent as to which of their data is processed in an AI system and for what purpose.
- AI decisions must be questioned by the data subject and the decision must be explained in a comprehensible way.
- Continuous monitoring of AI decisions for compliance with the defined purpose of the system and AI governance.