New legal data protection requirements and implementation at Deutsche Telekom	
Accountability / documentation	Products, services and IT systems offered or used by Deutsche Telekom Group Companies for processing personal data must undergo the Privacy & Security Assessment (PSA procedure) in order to check data protection/GDPR compliance and to be able to prove them in a standardised data protection and security concept (SDSK). The Group company responsible for the product, service or IT system must start and complete the PSA process. https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/more-transparency - Measures for more data protection "Privacy and Security Assessment".
Processing on behalf of a controller / commissioned data processing	The existing contract templates and the Deutsche Telekom **Data Protection Requirement* Processing of Personal Data on Behalf of a Controller**, which already met the requirements of the GDPR, were standardized throughout Europe and the Group processes for concluding these contracts were updated. The new legal requirements set out in Art. 28 and 82 GDPR will be directly effective without later contractual agreement. The existing commissioned data processing agreements have not to be adjusted to the GDPR, if the templates provided by Group Privacy Deutsche Telekom were used in contracting or the contract was concluded on the basis of a verified customer contract template in accordance with DIRECTIVE 95/46/EC. The legal situation does not change for telecommunications products and services. As before, no commissioned data processing agreements need to be concluded for this purpose.
Data Protection Impact Assessment	The Privacy & Security Assessment (PSA procedure) as a key component of security and data protection at Deutsche Telekom meets the requirements of the data protection impact assessment statued in the GDPR.
Rights of the data subject / Data Privacy Information	The **Data Protection Requirement Data Privacy Information** (as of May 2018) of Deutsche Telekom Group Privacy provides the companies of Deutsche Telekom Group with explanations of the GDPR requirements and, as applicable, additional Member State law as to the creation and the use of data privacy Information. In addition templates for "data privacy information for web portal" and "data privacy information for apps" do exist.
Responsibilities	Since 2015 the National Group Policy **Organization of data privacy - Assumption of responsibility for data processing** engages the Group Companies located in Germany to designate concrete roles to the assumption of responsibility for data processing.

Erasure	With the **Data Protection Requirement Erasure of Personal Data** and **Data Protection and Security Requirement Erasing data carriers,** the requirements of the GDPR for the erasure of personal data are regulated uniformly and bindingly for the Group. The concrete implementation of the deletion requirements is secured and documented by the PSA procedure.
Transfers of personal data to third countries	Since 2014, the Binding Corporate Rules Privacy (BCRP) have been the Group-wide internal data protection regulation. They are the national and international central basis for the handling of personal data, in particular the transmission of customer and employee data within the Deutsche Telekom Group. The BCRP is a new version of the Privacy Code of Conduct, which has uniformly regulated and replaced the internal requirements for the handling of personal data worldwide since 2004. The Telekom BCRP are approved by the German Federal Commissioner for Data Protection and Freedom of Information. https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2014/06_BCRTelekom.html https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/laws-and-corporate-rules-443956
Records of Processing	Within the Deutsche Telekom Group the central documentation-system CAPE, merging all data protection structures and procedures, is used as records of processing.
Data portability	Customers can assert their right to data portability against Deutsche Telekom at any time. https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/your-data-at-dt/details/protected-by-yourself-511824.
Certifications	In order to reinforce data protection and data security in the Group, Deutsche Telekom regularly carries out relevant internal audits and certifications of corporate departments. To do so, the company uses a system of audits and certifications by external and internal experts. It plays a pioneering role here: In the telecommunications industry, certification of individual corporate departments is still the exception. Find out more about it here: https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/audits–certifications-and-training-courses-356010.

Data protection officer	The BCRP obligate each Group Company to appoint an independent Data Privacy Officer, whose task is to advise the company on the statutory and internal company/Group requirements for data privacy and, in particular, on the Binding Corporate Rules Privacy and also to monitor compliance with data protection regulations through suitable measures, in particular random inspections. https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/news/laws-and-corporate-rules-443956 .
Data protection by design and default	Eines der Hauptziele des PSA Verfahrens ist die Umsetzung von Privacy by Design und Default in den konkreten Systemen und Produkten der GmbH. So steuert das PSA Verfahren z.B. die Umsetzung der Datenschutzanforderung Anonymisierung und Pseudonymisierung. Diese stellt den Unternehmen des Konzerns detaillierte Erläuterungen zu den Anforderungen der DS-GVO und etwaiger ergänzender nationaler Gesetze an die Anonymisierung und Pseudonymisierung (Identifikationsschutzverfahren) von personenbezogenen Daten zur Verfügung. One of the main goals of the PSA procdure is the implementation of Privacy by Design and Default in the concrete Telekom systems and products. For example, the PSA procedure controls the implementation of data protection requirements such as anonymization and pseudonymization. This provides Group companies with detailed explanations of the requirements of the GDPR and any supplementary national laws on the anonymization and pseudonymization (identification protection procedures) of personal data.

* The data protection requirements of Deutsche Telekom will be published at a later date on www.telekom.com See also **data protection requirement "Technical-organizational measures".** https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/data-protection/more-transparency - Measures for more data protection.