PRIVACY AND SECURITY ASSESSMENT

ENSURING SECURITY AND DATA PRIVACY FROM THE VERY START

CONTENTS

SECURITY AND DATA PRIVACY AT DEUTSCHE TELEKOM AG

FOREWORD

Dear Readers,

This brochure is designed to explain the Privacy and Security Assessment process (PSA process) – a core element in safeguarding security and data privacy at Deutsche Telekom.

One of the main objectives of the Deutsche Telekom AG is to ensure a suitable level of security and data privacy, along with ensuring compliance in data privacy and security. Against this backdrop, the central data privacy and security departments (Group Privacy, GPR) and Deutsche Telekom Security GmbH (DT Security GmbH) developed the PSA process, with the common goal of integrating the fulfillment of technical security and data privacy requirements from an early stage in the relevant Deutsche Telekom development processes.

The standardized process implements security and data privacy requirements as part of product and system development, ensuring greater transparency, improved project support, and a suitable level of protection for our products, services, platforms, and IT applications through compliance with requirements for data privacy and security.

The PSA process has enabled us to put in place the foundation for uniform support in relation to security and data privacy issues. All development projects and system releases that create or change IT or NT systems are categorized, taking into account the data being processed, attack vulnerability from the public Internet (hereinafter referred to as criticality), and complexity.

Security and data privacy experts provide ongoing consulting and review functions for highly critical and complex projects and system releases. Before such projects go live, they need to be expressly approved. Standardized requirements are provided for less complex and less critical projects and system releases. These requirements enable the responsible employees themselves to achieve a suitable level of security and data privacy. This is confirmed by a Statement of Compliance (SoC), which is archived for documentation purposes.

The PSA process is integrated into all key product and system development processes in Germany, on a cross-functional Group level, and in all European subsidiaries. Approximately 3,700 projects and systems go through the PSA process every year.

The PSA process is widely accepted throughout the group. It makes a fundamental contribution to our internationally recognized ISO 27001 certificate and forms an essential component of our certified data protection management system according to the PS 980 standard. In addition, it also serves as a role model outside of the company. The PSA process represents a cornerstone for compliance with the EU General Data Protection Regulation (EU GDPR).

The complete PSA process, including all workflows and requirements for security and data privacy, is mapped in a web application in the PSA Portal, where it can be conducted online by all stakeholders.

Yours,

Dr. Stefan Pütz Dorothee Schrief

SECURITY AND DATA PRIVACY AT DEUTSCHE TELEKOM AG

PSA PROCESS OWNERS

PSA process owners for security and data privacy

Dr. Stefan Pütz

Stefan Pütz has been head of the Network and IT Security department at Telekom Security GmbH since 2019. Together with Dorothee Schrief, he is responsible for the PSA process and controls its further development from a safety perspective (since 2009).

Stefan Pütz started out at Deutsche Telekom in 1997 and has since been in charge of various technical security areas. He studied electrical engineering, specializing in communications engineering, at the University of Siegen and completed a doctorate in the security of modern mobile communications systems.

Dorothee Schrief

Dorothee Schrief has been head of Privacy Audits & Standards since 2017. She is responsible for national and international data privacy inspections. Together with Stefan Pütz, she is also responsible for the PSA process and manages its further development from a security perspective.

Dorothee Schrief began working for Deutsche Telekom AG in 1998 in the International Regulation department. In 2003, she took on the role of deputy Group Data Privacy Officer and from 2007 she headed the Group's strategic and international data privacy departments.

PRIVACY AND SECURITY ASSESSMENT

SCOPE OF VALIDITY

The PSA process standardizes key activities in the area of security and data privacy and governs the creation of security and data privacy concepts for IT or NT systems. The process is also used to provide support and advice from DT Security GmbH and GPR experts, as well as to ensure approval and control of systems from a security and data privacy law perspective.

The PSA process is used in product or system development when new systems are created or existing systems undergo technical updates or changes to the type of data processing. Typically, new systems are created or systems are updated in the form of new releases. This process ensures that the specific changes caused by the new version are adapted in the data privacy and security concept from the very start.

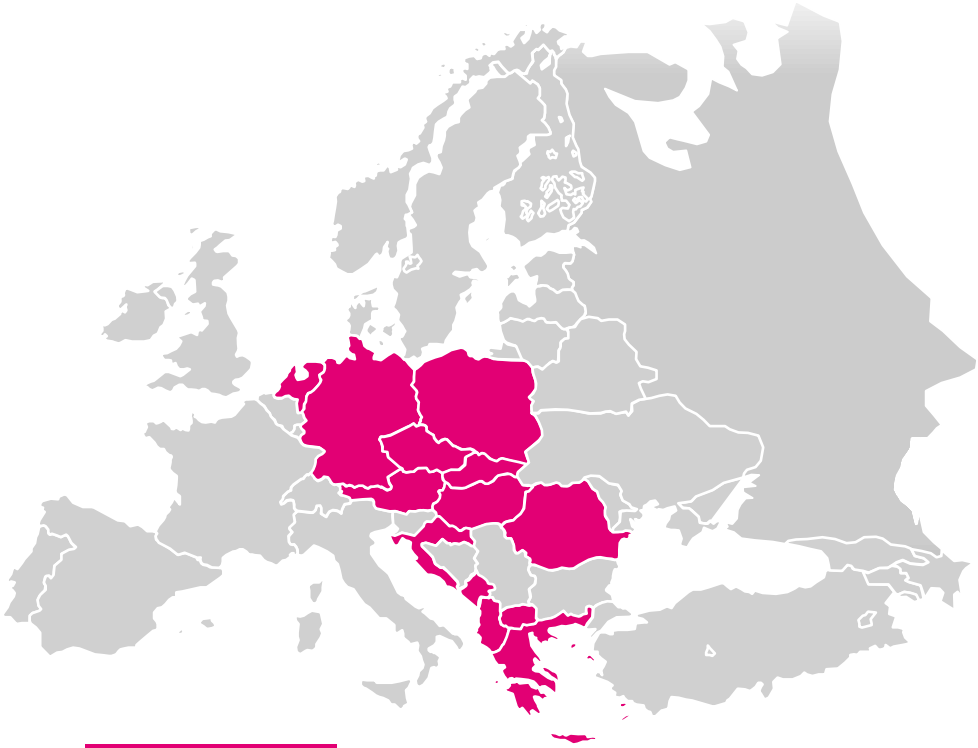
The PSA process can be used for all IT or NT systems, regardless of their size and complexity.

The use of the PSA process is mandatory for all European companies, as well as for all planned international projects of Deutsche Telekom.

SUMMARY – THE PSA PROCESS

- Integration of security and data privacy in product and system development.
- Consulting, documentation and approval regarding technical security and data privacy.
- PSA mandatory in European companies.

International rollout of the PSA process

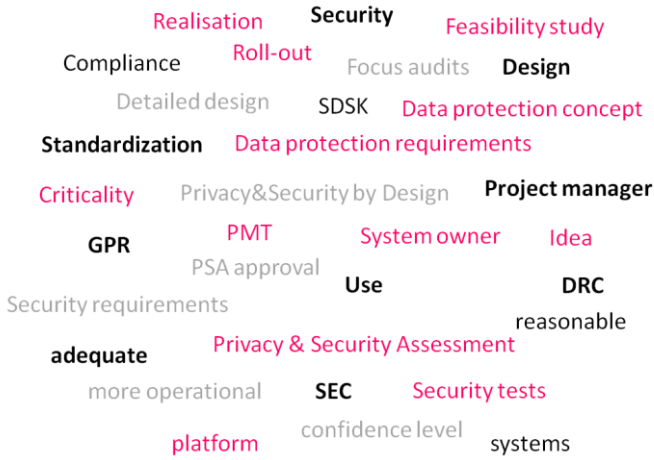


PSA implemented

PRIVACY AND SECURITY ASSESSMENT

OBJECTIVES

T-SEC and GPR establish important fundamentals within Deutsche Telekom for reliable products that also satisfy strict requirements for security and data privacy.
The PSA process guarantees that all development projects within the Group can meet the technical security and data privacy requirements.



Telekom Security (T-SEC, Internal Security)

T-SEC bears responsibility for internal security within Deutsche Telekom, among other things. To fulfill this task, a suitable level of security needs to be defined and implemented using appropriate measures.

Group Privacy (GPR)

GPR determines the Group's strategic alignment in terms of data privacy and defines the requirements from a legal, technical and organizational perspective. It also represents the Group in all data privacy matters, both internally and externally.

SUMMARY– THE AIMS OF THE PSA PROCESS

- Safeguarding a uniform, suitable level of security and data privacy.
- Integrated process for technical security and data privacy.
- Support level adapted to project/system release complexity and criticality.

The process has the following aims:

- An adequate level of security and data privacy in all products, systems and platforms that are updated or created from scratch, as well as compliance with requirements.
- An integrated process for technical security and data privacy as a component of the product and system development processes.
- A support level adapted to project and system release complexity and criticality through categorization at the start of each development project.

Deutsche Telekom operates several thousand different IT systems and network platforms. This implies a huge challenge for integrating security and data privacy requirements in a single process. These IT systems and network platforms are designed, implemented and constantly developed further via a host of different processes as well as through the involvement of functional and technical stakeholders. It is therefore an extremely complex, but achievable, intention to operate a single procedure to ensure both technical security and data privacy throughout the entire system landscape that is functionally integrated into the existing development processes.

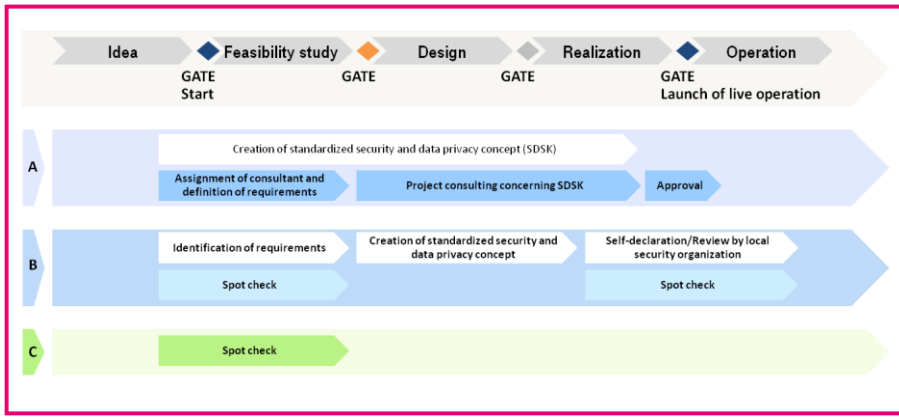
PRIVACY AND SECURITY ASSESSMENT

CONSULTING APPROACH

The following describes the PSA process methodology along a generic development process for system releases or projects.

It then explains the integration in the development process as well as the differences that result depending on the particular project categorization.

The PSA process at a glance



Integration in the development processes

The PSA process is integrated into Deutsche Telekom's key development processes. These basically follow the generic model of a development process presented here (initial idea – feasibility study – design – realization – operation).

At the decision gates between the process steps, a decision is made whether the next process step can be taken. This requires an explicit gate decision by the responsible management. This decision may only be made if the necessary PSA process steps have been completed.

SUMMARY– INTEGRATION OF THE PSA PROCESS

- Integration in the product and system development processes.
- Categorization in terms of security and data privacy relevance.
- Approval prior to live operation.

The PSA process is always linked to the decision gates at the start of development and at the launch of live operation. At the start development, the project is given a PSA category by the project manager for projects or the system owner for system releases in terms of its security and data privacy relevance.

At the end of the realization phase, i.e., before the launch of live operation, the PSA process must have been completed successfully. As such, all necessary approvals must be in place. If conditions for effective operation have been granted, the implementation of the resulting measures will be tracked until the project is completed.

If T-SEC and GPR are not directly involved in project management, the effectiveness of the process is tested on a spot check basis. Selected projects and systems are additionally controlled by GPR and T-SEC for compliance with particularly critical requirements directly on the system.

Agile system development

The established PSA process was adapted for agile system development.

The roles of Privacy Champion and Security Champion are filled in the agile team. They ensure that data protection and security are permanently in focus during agile development and answer basic questions immediately. Data protection and security experts or local supervisors support the champions with their expertise in more complex questions and issue their approvals before they go live or in the event of minor changes after 6 months at the latest.

"Agile" in the sense of the PSA procedure is a system release, if

- there are frequent start-ups of new or changed features (at least 4 per year)
- there are short development cycles (2 - 4 weeks)
- an agile method is used for development, e.g. Scrum or Kanban

Project and system release categorization

Before the decision gate for the start of the project, a project manager/system owner categorizes their project/system release using a tool-supported questionnaire. The categorization (A, B, C) defines the level of detail with which the project or the system release is supported and approved. In agile development there is also a relevance assessment per sprint.

The categorization is based on characteristics such as the processing of particularly sensitive data, the complexity of the platforms or systems considered, their accessibility from the Internet, or the strategic and financial significance of the products.

For category B and C projects/system releases, compulsory random samples are taken by GPR and/or T-SEC in order to check the categorization by subject.

Relevance and level of support for projects and systems

Category	Relevance/level of support/approval	Year	Systems	Projects
A	▪ High relevance, as projects and systems are complex and/or critical. ▪ The project or system is supported, advised and approved directly by security and/or data ▪ privacy experts from DT SEC and GPR.	2020: 2019: 2018:	57,1% 59,4% 52,9%	38,8% 37,1% 36,4%
B	▪ Relevant, but projects or systems are less complex with less sensitive data. ▪ Standard requirements are implemented by the project teams themselves, with support from local security organizations if necessary. ▪ Approval is given through a self-declaration by the project manager/systems owner and, if appropriate, is reviewed by local security organizations; DT SEC and GPR review these approvals on a spot check basis.	2020: 2019: 2018:	36,0% 32,6% 39,7%	33,2% 26,0% 23,4%
C	▪ No changes or generally irrelevant. ▪ The projects/systems do not result in any changes relevant for security and/or data privacy. ▪ No approval is required; SEC and GPR review the project categorizations on a spot check basis.	2020: 2019: 2018:	6,9% 8,0% 7,4%	27,9% 37,0% 40,2%

Source: AGIS, KPI-Report, date: 2021-04-01

PRIVACY AND SECURITY ASSESSMENT

CONTEXT BETWEEN PROJECT AND SYSTEM LEVEL

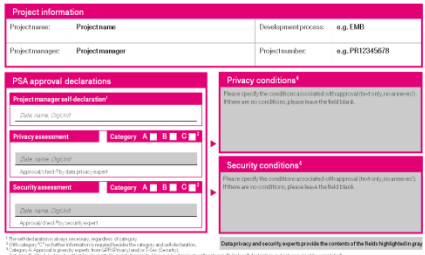
Alongside categorization, the PSA process is based on two other central elements: the PSA release document and the standardized data privacy and security concept (SDSK).

PSA release document

The PSA release document is the form used to document the project categorization and approval. It is prepared by the project manager/responsible person at project level.

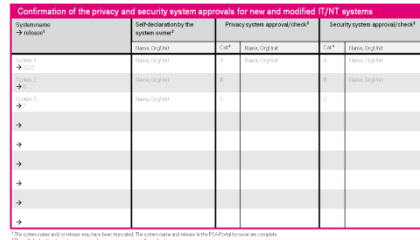
Project approval is generally only given and documented in the PSA release document once all system releases affected by the project have been approved. This means that the approval of all systems in the PSA release document is the prerequisite for project approval for live operation.

PSA APPROVAL DOCUMENT
DOCUMENTATION OF PROJECT CATEGORIZATION AND APPROVAL



- Documentation of project categorization and approval and any requirements by the project manager and the security and data privacy experts.

PSA APPROVAL DOCUMENT
OVERVIEW OF SYSTEM APPROVALS



- List of newly created or modified IT or NT system releases affected, including approval status.

SUMMARY – PROJECT LEVEL VS. SYSTEM LEVEL IN THE PSA PROCESS

- Documentation of project categorization, approval and any requirements in the PSA release document.
- Documentation of project categorization, approval and any requirements, and implementation of the security and data privacy requirements for system releases in the SDSK.
- Approval prior to live operation.

Standardized data privacy and security concept (SDSK)

The SDSK is created and updated for each system by the system owner within the system releases. The system owner is responsible for ensuring that the respective system releases meet the requirements for technical security and data privacy. He documents the implementation of security and data privacy requirements at IT or NT system level, as well as their approval or self-declaration in the SDSK.

The role and area of responsibility of the system owner are not dependent on specific projects and generally apply for the entire life cycle of a system.

The PSA portal – Helping you to execute the PSA process

The PSA portal is a web application for the tool-based execution of the PSA process. The project or system to be processed is provided with end-to-end online support, from initial categorization to approval. Stakeholders have a current view of the status of their projects at all times.

The PSA portal also manages all requirement catalogs and documents.

STANDARDIZED DATA PRIVACY & SECURITY CONCEPT

System information

System name:	*Short text*	System owner, Org. unit:	*Name, Org.*
System release:	*Current release*	Phone no.:	*+49 (xxx) xxxxxxxx*
System code:	*e.g. app-ID, ICTO-ID*	SDSK version:	*No.*

❶ **SDSK documentation** — SDSK-Documentation: Template

SDSK documentation takes place within a ZIP archive with the following components:

1. System description
2. Authorization concept
3. Data privacy information
4. Requirements catalogs / SoC
5. Action plan
6. Release categorization
7. Privacy frame conditions/assessment report (only for privacy category A)
8. if available: Test results
9. if available: Approval mail

ZIP archive

ZIP archive, please insert here.

Date: MMM DD, YYYY

❷ **SDSK approval statement**

SDSK Version	System Release[1]	Self-declaration by system owner[2]		Privacy system approval/check[3]		Security system approval/check[3]	
		Date	Name, Org/Unit	Cat.[4]	Name, Org/Unit	Cat.[4]	Name, Org/Unit
1.0.2	1.0	May 31, 2005	Name, Org/Unit	A	Name, Org/Unit	A	Name, Org/Unit
1.1.4	1.1	Oct. 10, 2006	Name, Org/Unit	C	n/a	A	Name, Org/Unit

[1] The description of the system release may have been truncated. The corresponding description in the PSA-Portal however is complete.
[2] The self-declaration by system owner is always necessary, regardless of category.
[3] Category A: Approval is given by experts from GPR (Privacy) and/or T-Sec (Security).
Category B: Check is done by other/local experts for assisted system releases. Unsupervised system releases with category B: Only self-declaration and category must be completed.
[4] Category of the system release

Explanations on the SDSK

❶ The SDSK consists of:

- System description
- Authorization concept
- Data privacy information
- Requirement catalogs/Statements of Compliance (SOC)
- Action plan
- System categorization
- Data privacy framework approval

❷ Since the SDSK is maintained over the entire lifecycle of a system, it includes the update of the particular releases, including the release status.

PRIVACY AND SECURITY ASSESSMENT

BENEFITS OF THE PROCESS

The Privacy and Security Assessment (PSA process) gives structure and transparency to Deutsche Telekom's security and data privacy work and maps the requirements of the GDPR.

The process gives projects and systems a uniform and suitable level of security and data privacy for each new or further development, ensuring efficient, standardized documentation and control. Expert support for technical security and data privacy is provided based on a uniform procedure model.

This process model ensures that all security and data privacy requirements are known at an early stage.

The early integration has the advantage of preventing costly reworking and unnecessary compromises.

The integration takes place for critical and complex projects/system releases (category A) usually immediately after the start of the project/system release; and ensures that the necessary subsequent steps and measures are identified, developed and documented for the relevant A categorizations.

It also prevents projects and system releases from having to be stopped due to late integration, possibly before going live.

The categorization system for the level of data privacy and technical security support required allows data privacy and security departments to focus effectively on the main topics and to provide ongoing support for project work and system development and, if necessary, to control these in the system before live operation begins.

SUMMARY– BENEFITS OF THE PSA PROCESS

- Structure and transparency of security and data privacy work.
- Suitable level of security and data privacy thanks to standardized procedural model.
- Efficiency thanks to early integration.

The benefits of the PSA process at a glance

- The PSA process maps the requirements of the GDPR.
- Data privacy and security are combined into one process, which optimizes resources.
- Projects and system releases can be processed using a tool-based approach in the PSA process.
- Data privacy and security requirements are harmonized, aligned with one another and standardized. They are therefore comprehensible and form a reliable basis.
- Technical security and data privacy are reviewed and evaluated based on uniform and recognized requirements and criteria.
- Redundant documentation is minimized as a result of uniform, standardized templates.
- Integration into development processes ensures technical security and data privacy are incorporated into the relevant topics at an early stage.
- Project/system release prioritization ensures that critical, complex projects/system releases are supported by security and data privacy experts.
- The modular, requirement-based approach allows maximum flexibility when implementing the necessary measures for projects and system releases.

ANNEX
GLOSSARY

Requirements catalogs /
Statements of Compliance (SoC)
Documentation of the requirements from technical security and data protection and their degree of fulfillment

Authorization concept
Description of roles and functions

Data privacy adviser (DPA)
Adviser for a project or system release in terms of data privacy, including review and approval

Data privacy information
Description of the purpose of processing personal data or data that can be traced back to a given individual in the IT/NT system concerned

GDPR
General Data Protection Regulation

GPR
Group Privacy

IT or NT system
Systems that process or transmit information in electronic form. These generally consist of a number of applications, computer systems or network elements with the same or similar purpose, e.g. servers, IT or NT networks, and platforms

Action plan

Privacy Champion (PC)
Is a multiplier for data protection in an agile team, considers all activities in an agile team from a data protection perspective. The PC identifies topics relevant to data protection in user stories and notifies the agile team. With data protection-relevant topics, he recognizes whether these are covered by the previous framework agreements from the initial consultation.

Project Security Manager (PSM)
Adviser for a project or system release in terms of data privacy, including review and approval

PSA
Privacy and Security Assessment: The PSA process is intended to ensure an appropriate level of data privacy and security

Requirements catalogs/
Statements of Compliance (SoC)
Documentation of the degree of compliance with technical security and data privacy requirements

SDSK
Standardized data privacy and security concept

Security Champion (SC)
Is a multiplier for security in an agile team and considers all activities in an agile team from a security perspective. The SC

Documentation of measures through which the requirements can be met in future

identifies security-relevant topics in user stories, notifies the agile team and supports the implementation. He recognizes security-relevant topics that cannot be solved with standard specifications or his own know-how and contacts the security experts.

System description
Documentation of the responsibilities, along with functional and technical system description

DT Security GmbH
Deutsche Telekom Security GmbH (Internal Security)

Contact

Deutsche Telekom Security (Internal Security):
sicherheit@telekom.de

Group Privacy:
datenschutz@telekom.de

Publication details
Deutsche Telekom AG
Deutsche Telekom Security GmbH (Internal Security) / Group Privacy
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
Design: PSA Office
Last revised: May 2022