PRIVACY AND SECURITY ASSESSMENT

SICHERHEIT UND DATENSCHUTZ VON VORNERHEIN BERÜCKSICHTIGEN

INHALT

SICHERHEIT UND DATENSCHUTZ BEI DER DEUTSCHEN TELEKOM AG

VORWORT

Liebe Leserinnen und Leser,

in der vorliegenden Broschüre möchten wir Ihnen das Privacy & Security Assessment (PSA-Verfahren) erläutern, einen zentralen Baustein zur Gewährleistung von Sicherheit und Datenschutz bei der Deutschen Telekom.

Eines der Hauptziele der Deutschen Telekom AG ist die Gewährleistung eines adäquaten Sicherheits- und Datenschutzniveaus sowie die Sicherstellung der Datenschutz- und Sicherheitscompliance. Vor diesem Hintergrund haben die zentralen Datenschutz- und Sicherheitsbereiche (Group Privacy (GPR) und Deutsche Telekom Security GmbH (DT Security GmbH)) das PSA-Verfahren mit dem gemeinsamen Ziel entwickelt, die Berücksichtigung von technischer Sicherheit und Datenschutz bereits frühzeitig in den relevanten Entwicklungsprozessen der Deutschen Telekom zu verankern.

Das standardisierte Verfahren integriert Sicherheits- und Datenschutzanforderungen in die Produkt- und Systementwicklung und gewährleistet auf diese Weise eine höhere Transparenz, verbesserte Projektunterstützung, sowie ein angemessenes Schutzniveau unserer Produkte, Services, Plattformen und IT-Anwendungen durch Compliance mit den Datenschutz- und Sicherheitsanforderungen.

Mit dem PSA-Verfahren haben wir die Grundlage für eine einheitliche Betreuung in Sicherheits- und Datenschutzfragen geschaffen. Projekte und Systemreleases (neue Version eines IT- oder NT-Systems), die zu Neuerungen oder Änderungen führen, werden unter Berücksichtigung der zu verarbeitenden Daten, der Angreifbarkeit aus dem öffentlichen Internet (im Weiteren Kritikalität genannt) sowie der Komplexität kategorisiert.

Besonders kritische und komplexe Projekte und Systemreleases werden von Sicherheits- und Datenschutzexperten begleitend beraten und geprüft. Vor Aufnahme des Wirkbetriebs müssen sie ausdrücklich freigegeben werden. Weniger komplexen und weniger kritischen Projekten und Systemreleases werden standardisierte Anforderungen zur Verfügung gestellt, mit denen die verantwortlichen Mitarbeiter selbst in die Lage versetzt werden, ein adäquates Sicherheits- und Datenschutzniveau zu erreichen. Dies bestätigen sie durch ein sogenanntes Statement of Compliance (SoC), das zu Dokumentationszwecken hinterlegt wird.

Das PSA-Verfahren ist in alle wichtigen Produkt- und Systementwicklungsprozesse in Deutschland, auf übergreifender Konzernebene sowie in den Europäischen Tochtergesellschaften integriert. Pro Jahr durchlaufen ca. 3.700 Projekte und Systeme das PSA-Verfahren.

Das PSA-Verfahren stößt im gesamten Konzern auf eine hohe Akzeptanz. Es liefert einen grundlegenden Beitrag zu unserem international anerkannten ISO 27001 Zertifikat und bildet einen wesentlichen Baustein unseres zertifizierten Datenschutzmanagementsystems nach dem Standard PS 980. Es hat zudem auch im externen Unternehmensumfeld Vorbildcharakter erlangt. Zudem bildet das PSA-Verfahren einen elementaren Grundstein für die Einhaltung der Europäischen Datenschutzgrundverordnung.

Das komplette PSA-Verfahren inkl. aller Workflows sowie Sicherheits- und Datenschutzanforderungen ist im PSA-Portal in einer Web-Anwendung abgebildet und kann von allen Beteiligten online durchgeführt werden.

Ihr Dr. Stefan Pütz

Ihre Dorothee Schrief

SICHERHEIT UND DATENSCHUTZ BEI DER DEUTSCHEN TELEKOM AG

VERANTWORTLICHE

Verantwortliche des PSA-Verfahrens seitens Sicherheit und Datenschutz

Dr. Stefan Pütz

Stefan Pütz leitet seit 2019 die Abteilung Network and IT Security der Deutschen Telekom Security GmbH. Gemeinsam mit Dorothee Schrief verantwortet er das PSA-Verfahren und steuert dessen Weiterentwicklung aus der Sicherheitsperspektive (bereits seit 2009).
Stefan Pütz begann seine Laufbahn 1997 bei der Deutschen Telekom und leitete seitdem verschiedene technische Sicherheitsbereiche. Er studierte an der Universität Siegen Elektrotechnik, Fachrichtung Nachrichtentechnik, und promovierte im Themengebiet Sicherheit moderner Mobilfunksysteme.

Dorothee Schrief

Dorothee Schrief leitet seit 2017 die Abteilung Privacy Audits & Standards. Sie ist verantwortlich für nationale und internationale Datenschutz-kontrollen. Gemeinsam mit Stefan Pütz verantwortet sie zudem das PSA-Verfahren und steuert dessen Weiterentwicklung aus der Datenschutzperspektive.
Dorothee Schrief begann ihre Konzern-laufbahn 1998 in der internationalen Regulierungsabteilung der DTAG, über-nahm 2003 die Funktion der stell-vertretenden Konzerndatenschutzbeauf-tragten der DTAG und leitete ab 2007 die strategische und internationale Abteilung im Datenschutz im Konzern.

PRIVACY AND SECURITY ASSESSMENT

ANWENDUNGSBEREICH

Das PSA-Verfahren vereinheitlicht zentrale Aktivitäten aus den Verantwortungsbereichen von Sicherheit und Datenschutz und regelt die Erstellung von Sicherheits- und Datenschutzkonzepten für IT- oder NT-Systeme. Das Verfahren dient zudem der Unterstützung und Beratung durch Experten aus der DT Security GmbH und GPR sowie der sicherheits- und datenschutzrechtlichen Freigabe und Kontrolle der Systeme.

Das PSA-Verfahren wird in der Produkt- oder Systementwicklung angewendet, wenn Systeme neu errichtet oder bestehende Systeme technisch oder in der Art der Datenverarbeitung angepasst werden. Neuentwicklungen oder Anpassungen von Systemen erfolgen typischerweise im Rahmen einer neuen Version (Release). Hierbei regelt das Verfahren, das von Anfang an genau die Änderungen, welche die neue Version ausmachen, inhaltlich betrachtet und im Sicherheits- und Datenschutzkonzept angepasst werden.

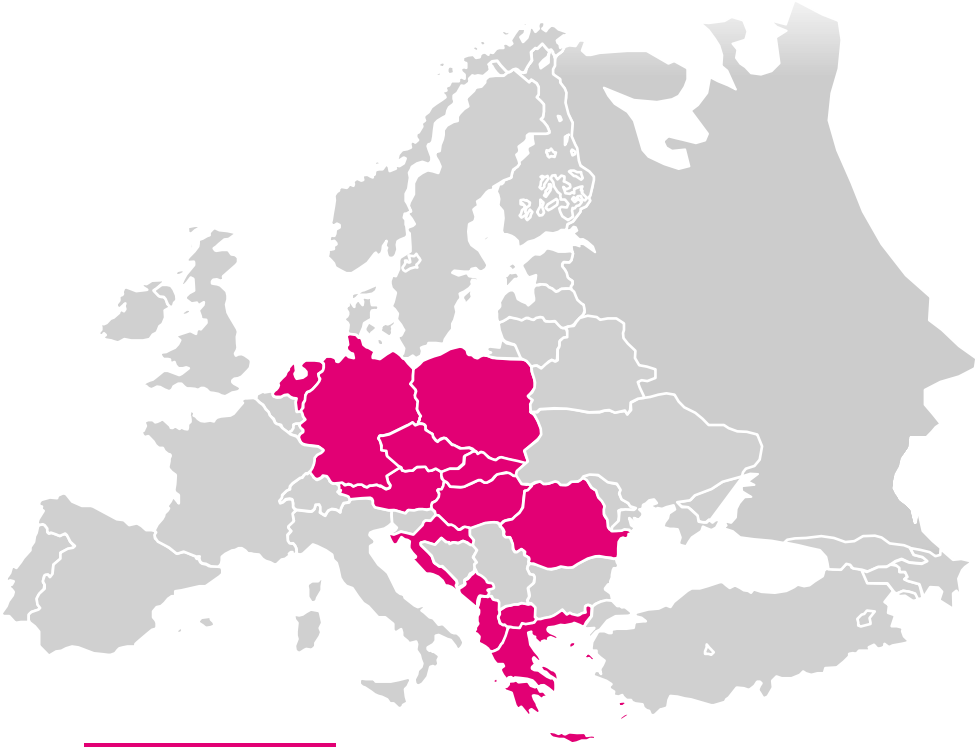
Das PSA-Verfahren kann auf alle IT- oder NT-Systeme, unabhängig von deren Größe und Komplexität, angewendet werden.

Die Anwendung des PSA-Verfahrens ist verbindlich für alle Europäischen Gesellschaften sowie für länderübergreifende Projektvorhaben der Deutschen Telekom.

IN KÜRZE – DAS PSA-VERFAHREN

- Integration von Sicherheit und Datenschutz in Produkt- und Systementwicklung.
- Beratung, Dokumentation und Freigabe zu technischer Sicherheit und Datenschutz.
- PSA verbindlich in Europäischen Gesellschaften.

Internationaler Rollout des PSA-Verfahrens



PSA Implementiert

PRIVACY AND SECURITY ASSESSMENT

ZIELE

Die DT Security GmbH und GPR leisten innerhalb der Deutschen Telekom wichtige Grundlagenarbeit für verlässliche Produkte, die zudem hohen Anforderungen an Sicherheit und Datenschutz genügen.

Über das PSA-Verfahren wird gewährleistet, dass alle Entwicklungsprojekte und Systemreleases innerhalb des Konzerns die Anforderungen für technische Sicherheit und Datenschutz erfüllen können.

Deutsche Telekom Security GmbH (DT-SEC GmbH, Interne Sicherheit)

DT-SEC trägt in der Deutschen Telekom unter anderem die Verantwortung für die interne Sicherheit. Um dieser Aufgabe Rechnung zu tragen, gilt es, ein angemessenes Sicherheitsniveau festzulegen und dieses mit geeigneten Maßnahmen umzusetzen.

Group Privacy (GPR, Datenschutz)

GPR bestimmt die strategische Ausrichtung des Konzerns in Fragen des Datenschutzes und definiert dabei die Anforderungen aus rechtlicher, technischer und organisatorischer Sicht. Zudem vertritt sie den Konzern in allen Angelegenheiten des Datenschutzes nach innen und nach außen.

IN KÜRZE – ZIELE DES PSA-VERFAHRENS

- Sicherstellung eines einheitlichen und adäquaten Sicherheits- und Datenschutzniveaus.
- Integriertes Verfahren für technische Sicherheit und Datenschutz.
- Betreuungsniveau angepasst an Projekt-/Systemreleasekomplexität und –kritikalität.

Das Verfahren adressiert die folgenden Ziele:

- Ein adäquates Sicherheits- und Datenschutzniveau in allen Produkten, Systemen und Plattformen, die aktualisiert oder neu erstellt werden, sowie Compliance gegenüber den Anforderungen.
- Ein integriertes Verfahren für technische Sicherheit und Datenschutz als Bestandteil der Produkt- und Systementwicklungsprozesse.
- Ein der Komplexität und Kritikalität der Projekte und Systemreleases angepasstes Betreuungsniveau auf Basis einer Kategorisierung zu Beginn jeder Entwicklung.

Die Herausforderung bei der Berücksichtigung von Sicherheits- und Datenschutzanforderungen in einem Verfahren ist, dass die Deutsche Telekom über mehrere tausend unterschiedliche IT-Systeme und Netzplattformen verfügt. Über viele verschiedene Prozesse sowie unter Einbeziehung von fachlichen und technischen Stakeholdern werden diese konzipiert, implementiert und stetig weiterentwickelt. Das Betreiben eines Verfahrens, das sowohl technische Sicherheit als auch Datenschutz in der gesamten Systemlandschaft gewährleistet und sich dabei funktional in die bestehenden Prozesse integriert, ist damit ein äußerst komplexes, aber realisierbares Vorhaben.

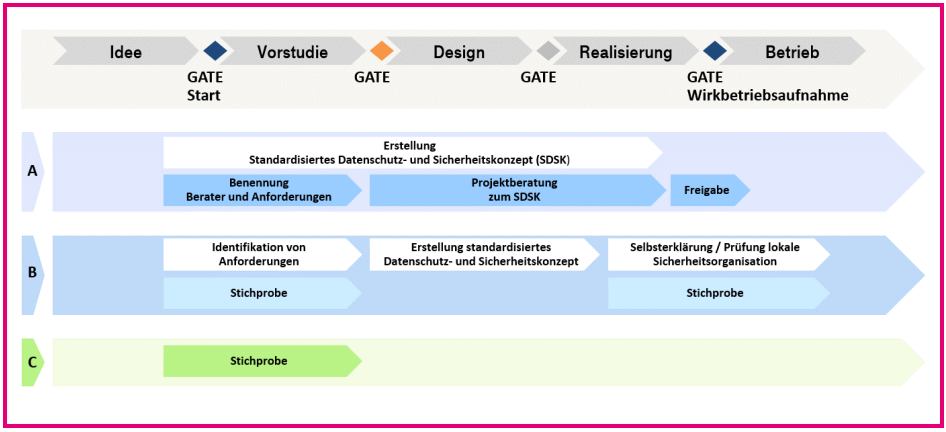
PRIVACY AND SECURITY ASSESSMENT

BERATUNGSANSATZ

Im Folgenden wird die Methodik des PSA-Verfahrens entlang eines generischen Entwicklungsprozesses für Projekte oder Systemreleases dargestellt.

Dabei werden nachfolgend die Integration in den Entwicklungsprozess sowie die Unterschiede, die sich abhängig von der jeweiligen Kategorisierung ergeben, erläutert.

Das PSA-Verfahren im Überblick



Integration in die Entwicklungsprozesse

Das PSA-Verfahren ist in wesentliche Entwicklungsprozesse der Deutschen Telekom integriert. Diese folgen grundsätzlich dem hier vorgestellten generischen Modell eines Entwicklungsprozesses (Idee-Vorstudie-Design-Realisierung-Betrieb).

An den Entscheidungspunkten (Gates) zwischen den einzelnen Prozessschritten wird entschieden, ob ein Übergang in den nächsten Prozessschritt erfolgt. Voraussetzung für den Übergang ist eine ausdrückliche Gate-Entscheidung durch das jeweils verantwortliche Management. Diese darf nur erfolgen, wenn die erforderlichen Prozessschritte im PSA-Verfahren durchlaufen wurden.

IN KÜRZE – PROZESSINTEGRATION DES PSA-VERFAHRENS

- Integration in die Produkt- und Systementwicklungsprozesse.
- Kategorisierung hinsichtlich Sicherheits- und Datenschutzrelevanz.
- Freigabe vor Aufnahme des Wirkbetriebes.

Das PSA-Verfahren ist immer an die Entscheidungspunkte (Gates) zum Entwicklungsstart und zur Wirkbetriebsaufnahme gekoppelt. Zum Entwicklungsstart erfolgt eine PSA-Kategorisierung durch den Projektleiter oder Systemverantwortlichen für Projekte bzw. Systemreleases hinsichtlich der Sicherheits- und Datenschutzrelevanz.

Mit dem Ende der Phase „Realisierung", das heißt vor der Aufnahme des Wirkbetriebs, muss das PSA-Verfahren erfolgreich abgeschlossen sein. Damit geht einher, dass alle notwendigen Freigaben vorliegen müssen. Wurden Auflagen zum Wirkbetrieb erteilt, wird die Umsetzung der daraus resultierenden Maßnahmen bis zum Projektabschluss nachverfolgt.

Sind DT-SEC und GPR nicht direkt in die Projektbetreuung eingebunden, erfolgt eine Wirksamkeitsprüfung des Verfahrens über Stichproben. Ausgewählte Projekte und Systemreleases werden zusätzlich von GPR und DT-SEC auf Einhaltung besonders kritischer Vorgaben direkt am System kontrolliert.

Agile Systementwicklung

Für die agile Systementwicklung wurde das etablierte PSA-Verfahren angepasst.

Agil entwickelte Systemreleases werden so betreut, wie andere Systemreleases auch, also je nach Kategorie von einem PSM und/oder einem DSB oder – falls in der Organisationseinheit vorhanden – von lokalen Betreuern.

Im agilen Team werden die Rollen Privacy Champion und Security Champion besetzt. Sie tragen Sorge, dass Datenschutz und Sicherheit dauerhaft während der agilen Entwicklung im Fokus stehen, und beantworten grundlegende Fragen umgehend. Datenschutz- und Sicherheitsexperten oder lokale Betreuer unterstützen die Champions mit Ihrer Expertise bei komplexeren Fragestellungen und erteilen ihre Freigaben vor Wirkbetriebsaufnahme bzw. bei kleineren Änderungen spätestens nach 6 Monaten.

„Agil“ im Sinne des PSA-Verfahrens ist ein Systemrelease, wenn

- es häufige Inbetriebnahmen neuer oder geänderter Features gibt (mindestens 4 pro Jahr)
- es kurze Entwicklungszyklen gibt (2 - 4 Wochen)
- eine agile Methode für die Entwicklung genutzt wird, z.B. Scrum oder Kanban

Projekt- und Systemrelease-Kategorisierung

Vor dem Entscheidungspunkt (Gate) zum Start der Entwicklung kategorisiert ein Projektleiter/ Systemverantwortlicher sein Projekt/Systemrelease mithilfe eines toolunterstützten Fragebogens. Aus der Kategorisierung (A, B, C) leitet sich ab, mit welcher Detailtiefe das Projekt bzw. das Systemrelease betreut und freigegeben wird. In der agilen Entwicklung erfolgt zudem eine Relevanzbewertung je Sprint.

Im PSA Prozess werden Projekte und Systemreleases, die auf A kategorisiert sind von Datenschutzeratern (DSBs) und Sicherheitsberatern (PSMs) betreut.

Bei Konzerneinheiten, die eine dezentrale B Betreuung haben, müssen diese Projekte und Systemreleases von den jeweiligen dezentralen Datenschutz- und Sicherheitseinheiten (zusammen mit den agilen Champions der IT/Fachseite) bearbeitet und freigegeben werden (auch lokale Betreuer genannt).

Bei Konzerneinheiten, die keine dezentrale B Betreuung haben, werden die B-Releases durch die Fachseiten/IT selbst freigegeben werden.

Die Kategorisierung basiert auf Eigenschaften wie der Verarbeitung besonders sensibler Daten, der Komplexität der betrachteten Plattformen oder Systeme, deren Erreichbarkeit aus dem Internet oder der strategischen und finanziellen Bedeutung der Produkte.

Bei Kategorie B- und C-Projekten/Systemreleases erfolgen obligatorische Stichproben durch GPR und/oder DT-SEC zur Überprüfung des Verfahrens.

Relevanz und Betreuungstiefe der Projekte und Systeme

Kategorie	Relevanz/Detailtiefe der Betreuung/Freigabe	Jahr	Systeme	Projekte
A	▪ Hohe Relevanz, da komplexe und/oder kritische Projekte und Systeme ▪ Das Projekt oder System wird durch Sicherheits- und/oder Datenschutzexperten aus den Bereichen DT Sec und GPR direkt begleitet, beraten sowie freigegeben.	2020: 2019: 2018:	57,1% 59,4% 52,9%	38,8% 37,1% 36,4%
B	▪ Relevanz, aber weniger komplexe Projekte oder Systeme mit weniger sensiblen Daten ▪ Die Umsetzung von Standardanforderungen erfolgt durch die Projekte selbst, ggf. mit Unterstützung lokaler Sicherheitsorganisationen. ▪ Die Freigabe erfolgt durch Selbsterklärung des Projektleiters/Systemverantwortlichen, ggf. geprüft durch lokale Sicherheitsorganisationen; die Bereiche DT Sec und GPR überprüfen stichprobenartig.	2020: 2019: 2018:	36,0% 32,6% 39,7%	33,2% 26,0% 23,4%
C	▪ Keine Änderungen oder generell keine Relevanz. ▪ Die Projekte/Systeme nehmen keine Änderungen vor, die Sicherheits- und/oder Datenschutzrelevanz haben. ▪ Es bedarf keiner Freigabe; die Bereiche DT Sec und GPR überprüfen die Projektkategorisierungen stichprobenartig.	2020: 2019: 2018:	6,9% 8,0% 7,4%	27,9% 37,0% 40,2%

Quelle: AGIS, KPI-Report, Stand: 04.01.2021

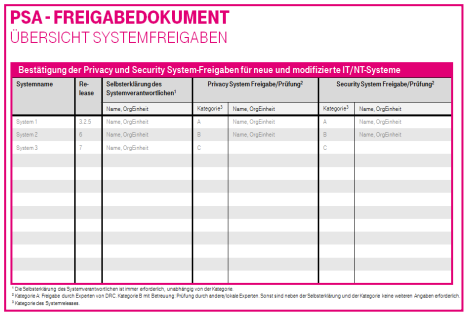
PRIVACY AND SECURITY ASSESSMENT

ZUSAMMENHANG VON PROJEKT- UND SYSTEMEBENE

Das PSA-Verfahren basiert neben der Kategorisierung auf zwei weiteren zentralen Elementen, dem PSA-Freigabedokument und dem standardisierten Datenschutz- und Sicherheitskonzept (SDSK).

PSA-Freigabedokument

Das PSA-Freigabedokument ist das Formular zur Dokumentation der Projektkategorisierung und -freigabe. Es wird auf Projektebene durch den jeweiligen Projektleiter/-verantwortlichen erstellt.
Die Projektfreigabe und deren Dokumentation im PSA-Freigabedokument erfolgen in der Regel erst nach Freigabe aller Systemreleases, die von dem Projekt betroffen sind. Die Freigabe aller Systeme im PSA-Freigabedokument ist somit Voraussetzung für die Projektfreigabe zur Wirkbetriebsaufnahme.



IN KÜRZE – PROJEKTEBENE VS. SYSTEMEBENE IM PSA-VERFAHREN

- Dokumentation der Kategorisierung, Freigabe sowie möglicher Auflagen für Projekte im PSA-Freigabedokument.
- Dokumentation der Kategorisierung, Freigabe sowie möglicher Auflagen sowie Umsetzung der Sicherheits- und Datenschutzanforderungen für Systemreleases im SDSK.
- Freigabe vor Aufnahme des Wirkbetriebes.

Das SDSK wird durch den Systemverantwortlichen pro System erstellt und wird im Rahmen der Systemreleases gepflegt. Der Systemverantwortliche hat die Aufgabe, für seine jeweiligen Systemreleases die Einhaltung der Vorgaben der technischen Sicherheit und des Datenschutzes sicherzustellen. Er dokumentiert die Umsetzung der Sicherheits- und Datenschutzanforderungen auf IT- oder NT-Systemebene sowie deren Freigabe bzw. Selbsterklärung im SDSK.

Die Rolle und der Verantwortungsbereich der Systemverantwortlichen sind unabhängig von einem konkreten Projekt und bestehen in der Regel über den gesamten Lebenszyklus eines Systems.

Das PSA-Portal – Ihre Unterstützung für die Durchführung des PSA-Verfahrens

Das PSA-Portal ist eine Web-Anwendung zur toolgestützten Durchführung des PSA-Verfahrens. Dabei wird das zu bearbeitende Projekt oder System komplett online von der anfänglichen Kategorisierung bis zur Freigabe begleitet. Alle Beteiligten haben jederzeit eine aktuelle Sicht auf den Status Ihrer Projekte/Systeme.
Das PSA-Portal verwaltet zusätzlich alle Anforderungskataloge und Dokumente.

STANDARDISIERTES DATENSCHUTZ- UND SICHERHEITSKONZEPT

Systeminformation

Systemname:	*Kurztext*	Systemverantwortlicher, OrgE:	*Name, OrgE*
System Release:	*aktuelles Release*	Telefonnr.:	*+49 (xxx) xxxxxxx*
Systemkennzeichnung:	*z.B. App-ID, ICTO-ID*	SDSK Version:	*Nr.*

❶ **SDSK-Dokumentation** — SDSK-Dokumentation: Mustervorlage → **ZIP-Archiv**

SDSK-Dokumentation erfolgt innerhalb eines ZIP-Archivs mit folgenden Bestandteilen:

1. Systembeschreibung
2. Berechtigungskonzept
3. Datenschutzinformation
4. Anforderungskataloge/SoC
5. Maßnahmenkatalog
6. Kategorisierung des Systemreleases
7. Privacy Rahmenvorgabe/Prüfprotokoll (nur bei Privacy–Kategorie A)
8. ggf. Testergebnisse
9. ggf. Freigabemail

ZIP Archiv bitte hier einbetten

Datum: TT.MM.JJJJ

❷ **SDSK-Freigabeerklärung**

SDSK Version	System Release	Selbsterklärung des Systemverantwortlichen[1]		Privacy Systemfreigabe/-prüfung[2]		Security Systemfreigabe/-prüfung[2]	
		Datum	Name, OrgEinheit	Kategorie[3]	Name, OrgEinheit	Kategorie[3]	Name, OrgEinheit
1.0.2	1.0	31.01.2005	Name, OrgEinheit	A	Name, OrgEinheit	A	Name, OrgEinheit
1.1.4	1.1	02.10.2006	Name, OrgEinheit	C	n.a.	A	Name, OrgEinheit
1.2.3	1.2	30.06.2007	Name, OrgEinheit	B	Name, OrgEinheit	C	n.a.
2.0.7	2.0	31.05.2008	Name, OrgEinheit	B	Name, OrgEinheit	A	Name, OrgEinheit

[1] Die Selbsterklärung des Systemverantwortlichen ist immer erforderlich, unabhängig von der Kategorie.
[2] Kategorie A: Freigabe durch Experten von DRC. Kategorie B mit Betreuung: Prüfung durch andere/lokale Experten. Sonst sind neben der Selbsterklärung und der Kategorie keine weiteren Angaben erforderlich.
[3] Kategorie des Systemreleases.

Erläuterungen zum SDSK

❶ Das SDSK setzt sich wie folgt zusammen:

- Systembeschreibung
- Berechtigungskonzept
- Datenschutzinformation
- Anforderungskataloge/Statement of Compliance (SoC)
- Maßnahmenplan
- Systemkategorisierung
- Datenschutz Rahmenfreigabe

❷ Da das SDSK über den gesamten Lebenszyklus eines Systems gepflegt wird, enthält es die Fortschreibung der jeweiligen Releases inklusive Freigabestatus.

PRIVACY AND SECURITY ASSESSMENT

NUTZEN DES VERFAHRENS

Das Privacy & Security Assessment (PSA-Verfahren) verleiht der Sicherheits- und Datenschutzarbeit der Deutschen Telekom Struktur und Transparenz und bildet die Anforderungen der DSGVO ab.

Projekte und Systeme erhalten durch das Verfahren bei der Neu- oder Weiterentwicklung ein einheitliches und adäquates Sicherheits- und Datenschutzniveau, das effizient und standardisiert dokumentiert und kontrolliert wird. Die Unterstützung durch Experten erfolgt für technische Sicherheit und Datenschutz entlang eines einheitlichen Vorgehensmodells.

Durch dieses Vorgehensmodell ist sichergestellt, dass alle Sicherheits- und Datenschutzanforderungen frühzeitig bekannt sind.

Die frühzeitige Einbindung hat den Vorteil, dass kostenintensive Nachbesserungen sowie unnötige Kompromisse vermieden werden können.

Die Einbindung erfolgt für kritische und komplexe Projekte/Systemrelease (Kategorie A) in der Regel unmittelbar nach dem Projekt-/Systemreleasestart und stellt sicher, dass bei den relevanten A Kategorisierungen die notwendigen Folgeschritte und Maßnahmen erkannt, erarbeitet und dokumentiert werden.

Außerdem wird verhindert, dass Projekte bzw. Systemreleases durch eine zu späte Einbindung möglicherweise vor Wirkbetriebsaufnahme noch gestoppt werden müssen.

Die Datenschutz- und Sicherheitsbereiche können sich dank der Kategorisierungssystematik hinsichtlich Beratungsintensität für Datenschutz und technische Sicherheit optimal auf die wichtigsten Themen fokussieren und die Projektarbeit bzw. Systementwicklung nachhaltig unterstützen und soweit erforderlich auch vor Wirkbetriebsaufnahme am System kontrollieren.

IN KÜRZE – NUTZEN DES PSA-VERFAHRENS

- Struktur und Transparenz der Sicherheits- und Datenschutzarbeit.
- Adäquates Sicherheits- und Datenschutzniveau durch standardisiertes Vorgehensmodell.
- Effizient durch frühzeitige Einbindung.

Der Nutzen des PSA-Verfahrens im Überblick

- Das PSA-Verfahren bildet die Anforderungen der DSGVO ab.
- Datenschutz und Sicherheit werden in einem Verfahren gebündelt – das optimiert den Ressourceneinsatz.
- Die Bearbeitung der Projekte und Systemreleases kann im PSA-Verfahren toolgestützt erfolgen.
- Die Anforderungen von Datenschutz und Sicherheit sind harmonisiert, aufeinander abgestimmt und standardisiert. Sie sind nachvollziehbar und bilden eine verlässliche Basis.
- Die Prüfung und Bewertung von technischer Sicherheit und Datenschutz basiert auf bekannten und einheitlichen Anforderungen und Kriterien.
- Redundanzen in der Dokumentation sind durch einheitliche und standardisierte Templates minimiert.
- Die Integration in die Entwicklungsprozesse stellt eine frühzeitige Einbindung von technischer Sicherheit und Datenschutz in die relevanten Themen sicher.
- Eine Priorisierung der Projekte/Systemreleases stellt sicher, dass die kritischen und komplexen Projekte/Systemreleases durch Sicherheits- und Datenschutzexperten unterstützt werden.
- Der modulare, anforderungsbasierte Ansatz ermöglicht den Projekten und Systemreleases maximalen Spielraum bei der Umsetzung der notwendigen Maßnahmen.

ANHANG

GLOSSAR

Anforderungskataloge / Statements of Compliance (SoC)
Dokumentation der Anforderungen aus technischer Sicherheit und Datenschutz und deren Erfüllungsgrad

Berechtigungskonzept
Beschreibung von Rollen und Funktionen

Datenschutzinformation
Beschreibung des Zwecks der Verarbeitung von personenbezogenen oder -beziehbaren Daten im betreffenden IT- / NT-System

Datenschutzbetreuer (DSB)
Betreuer eines Projekt- oder Systemrelease zum Thema Datenschutz inkl. Prüfung und Freigabe.

DSGVO
Datenschutzgrundverordnung

GPR
Group Privacy (Datenschutz)

IT- oder NT- System
Systeme, die Informationen in elektronischer Form verarbeiten oder übertragen. Diese bestehen typischerweise aus einer Anzahl von Applikationen, Rechnersystemen oder Netzwerkelementen mit gleicher oder ähnlicher Zweckbestimmung, z. B. Server, IT- oder NT-Netze und Plattformen

Privacy Champion (PC)
Ist Multiplikator für das Thema Datenschutz im agilen Team, betrachtet alle Aktivitäten im agilen Team auch aus Sicht des Datenschutzes. Der PC identifiziert in User Stories datenschutzrelevante Themen und weist das agile Team darauf hin. Er erkennt bei datenschutzrelevanten Themen, ob diese mit den bisherigen Rahmenvereinbarungen aus der Erstberatung abgedeckt sind.

Project Security Manager (PSM)
Betreuer eines Projekt- oder Systemrelease zum Thema Sicherheit inkl. Prüfung und Freigabe

PSA
Privacy and Security Assessment: Das PSA-Verfahren dient der Gewährleistung eines adäquaten Datenschutz- und Sicherheitsniveaus

SDSK
Standardisiertes Datenschutz- und Sicherheitskonzept

Security Champion (SC)
Ist Multiplikator für das Thema Sicherheit im agilen Team und betrachtet alle Aktivitäten im agilen Team aus Sicht der Sicherheit. Der SC identifiziert sicherheitsrelevante Themen in User Stories, weist das agile Team darauf hin und unterstützt bei der Umsetzung. Er erkennt sicherheitsrelevante Themen, die mit Standard-Vorgaben bzw.

Maßnahmenplan
Dokumentation von Maßnahmen, durch die Anforderungen in Zukunft erfüllt werden

eigenem Know-How nicht zu lösen sind, und kontaktiert den Sicherheitsexperten.

Systembeschreibung
Dokumentation der Verantwortlichkeiten sowie funktionale und technische Systembeschreibung

DT-SEC
Deutsche Telekom Security GmbH (Interne Sicherheit)

Kontakt
Telekom Security (Interne Sicherheit):
SecurityDemandManagement@telekom.de

Group Privacy:
datenschutz@telekom.de

Impressum
Deutsche Telekom AG
Deutsche Telekom Security GmbH (Interne Sicherheit) / Group Privacy
Friedrich-Ebert-Allee 140
D-53113 Bonn
Gestaltung: PSA-Office, psa-office@telekom.de
Stand der Broschüre: März 2021

ERLEBEN, WAS VERBINDET.