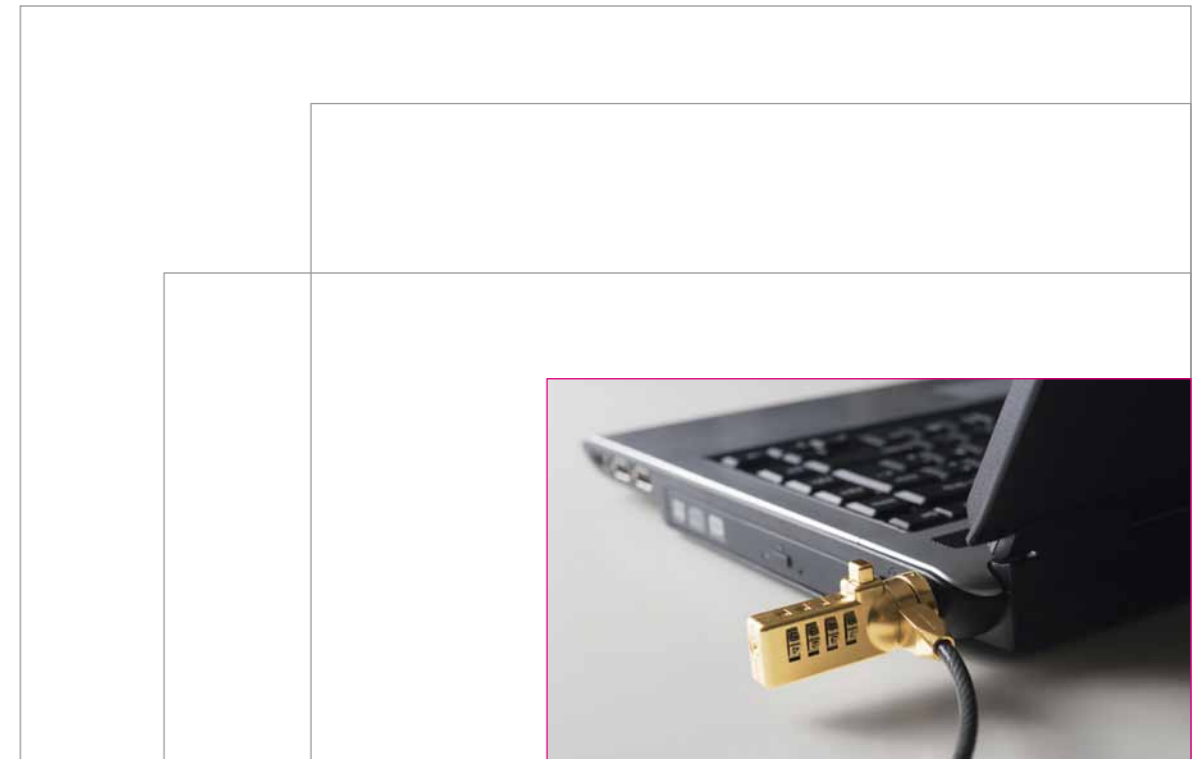


Privacy and Security Assessment.

Technische Sicherheit und Datenschutz in einem Verfahren.

Deutsche Telekom AG Friedrich-Ebert-Allee 140 D-53113 Bonn www.telekom.com			



Erleben, was verbindet.



Inhalt.



2 Technische Sicherheit und Datenschutz bei der Deutschen Telekom

2 Vorwort

4 Privacy and Security Assessment

4 Anwendungsbereich

6 Ziele

8 Beratungsansatz

10 Zusammenhang Projekt- und Systemebene

12 Nutzen des Verfahrens

14 Stimmen zum Verfahren

16 Anhang

16 Glossar

17 Impressum/Kontakt

Technische Sicherheit und Datenschutz bei der Deutschen Telekom.

Liebe Leserinnen und Leser,

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

Eines der Hauptziele des Vorstandsbereichs Datenschutz, Recht und Compliance (DRC) ist die Gewährleistung eines adäquaten Sicherheits- und Datenschutzniveaus. Seit der Gründung von DRC arbeiten unsere beiden Bereiche Group IT-Security (GIS) und Group Privacy (GPR) in diesem Vorstandsressort verstärkt zusammen. Inhaltlich sind die technischen und organisatorischen Anforderungen von GIS und GPR sehr stark miteinander verbunden. Vor diesem Hintergrund haben wir im Jahr 2009 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 neue standardisierte Verfahren implementiert Sicherheits- und Datenschutzanforderungen in die Produkt- und Systementwicklung und gewährleistet auf diese Weise eine höhere Transparenz, verbesserte Projektunterstützung sowie ein angemessenes Schutzniveau unserer Produkte. Mit dem PSA-Verfahren haben wir die Grundlage für eine einheitliche Betreuung in Sicherheits- und Datenschutzfragen geschaffen. Alle Entwicklungsprojekte, die zu Neuerungen oder Änderungen bei IT- oder NT-Systemen 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 werden von Sicherheits- und Datenschutzexperten begleitend beraten und geprüft. Vor Aufnahme des Wirkbetriebs müssen sie ausdrücklich freigegeben werden. Weniger komplexen und weniger kritischen Projekten 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, das zu Dokumentationszwecken hinterlegt wird.

Das PSA-Verfahren wurde im Jahr 2010 bereits in die wichtigsten nationalen Produkt- und Systementwicklungsprozesse in Deutschland sowie auf übergreifender Konzernebene integriert. Pro Jahr durchlaufen mehr als 2.000 Projekte das PSA-Verfahren. Zukünftig wird es auch bei den internationalen Beteiligungen der Deutschen Telekom zur Anwendung kommen. Das PSA-Verfahren stößt im gesamten Konzern bereits heute auf eine hohe Akzeptanz. Es wurde mit dem Gütesiegel des international anerkannten ISO 27001 Zertifikats ausgezeichnet und hat zudem auch im externen Unternehmensumfeld Vorbildcharakter erlangt.

Ihr



Dr. Stefan Pütz

Verantwortliche des PSA-Verfahrens seitens technischer Sicherheit und Datenschutz



Dr. Kornel Knöpfle



Dr. Stefan Pütz

Verantwortlicher des
PSA-Verfahrens seitens
technischer Sicherheit

Stefan Pütz leitet seit 2009 die Abteilung Sicherheit der Produktionsinfrastruktur der Group IT Security (GIS) im Vorstandsbereich Datenschutz, Recht und Compliance. Gemeinsam mit Dr. Kornel Knöpfle verantwortet er das PSA-Verfahren und steuert dessen Weiterentwicklung aus der Sicherheitsperspektive. 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.



Dr. Kornel Knöpfle

Verantwortlicher des
PSA-Verfahrens seitens
Datenschutz

Kornel Knöpfle arbeitet seit 2002 für die Deutsche Telekom. Er leitet seit April 2009 im Bereich Group Privacy (GPR) im Vorstandsbereich Datenschutz, Recht und Compliance die Abteilung Privacy Audit & Technical Knowhow Management. Zusammen mit Dr. Stefan Pütz hat er das PSA-Verfahren entwickelt, das er aus der Datenschutzperspektive betreut. Zuvor war Kornel Knöpfle mehrere Jahre bei der T-Online International AG in Darmstadt in verschiedenen Leitungsfunktionen in der Abteilung IT-Strategie und IT-Security tätig. Kornel Knöpfle studierte und promovierte in Physik an der Technischen Universität Darmstadt.

Privacy and Security Assessment: Anwendungsbereich.

Das PSA-Verfahren vereinheitlicht zentrale Aktivitäten aus den Verantwortungsbereichen von technischer 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 GIS und GPR sowie der sicherheitstechnischen und datenschutzrechtlichen Freigabe 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. Neuerstellungen oder Anpassungen von Systemen erfolgen typischerweise im Rahmen einer neuen Versionierung (Release-Hubs). Hierbei regelt das Verfahren, dass genau die Änderungen, die die neue Version verursacht, im Sicherheits- und Datenschutzkonzept angepasst werden. Das PSA-Verfahren kann auf alle IT- oder NT-Systeme, unabhängig von deren Größe und Komplexität, angewendet werden.

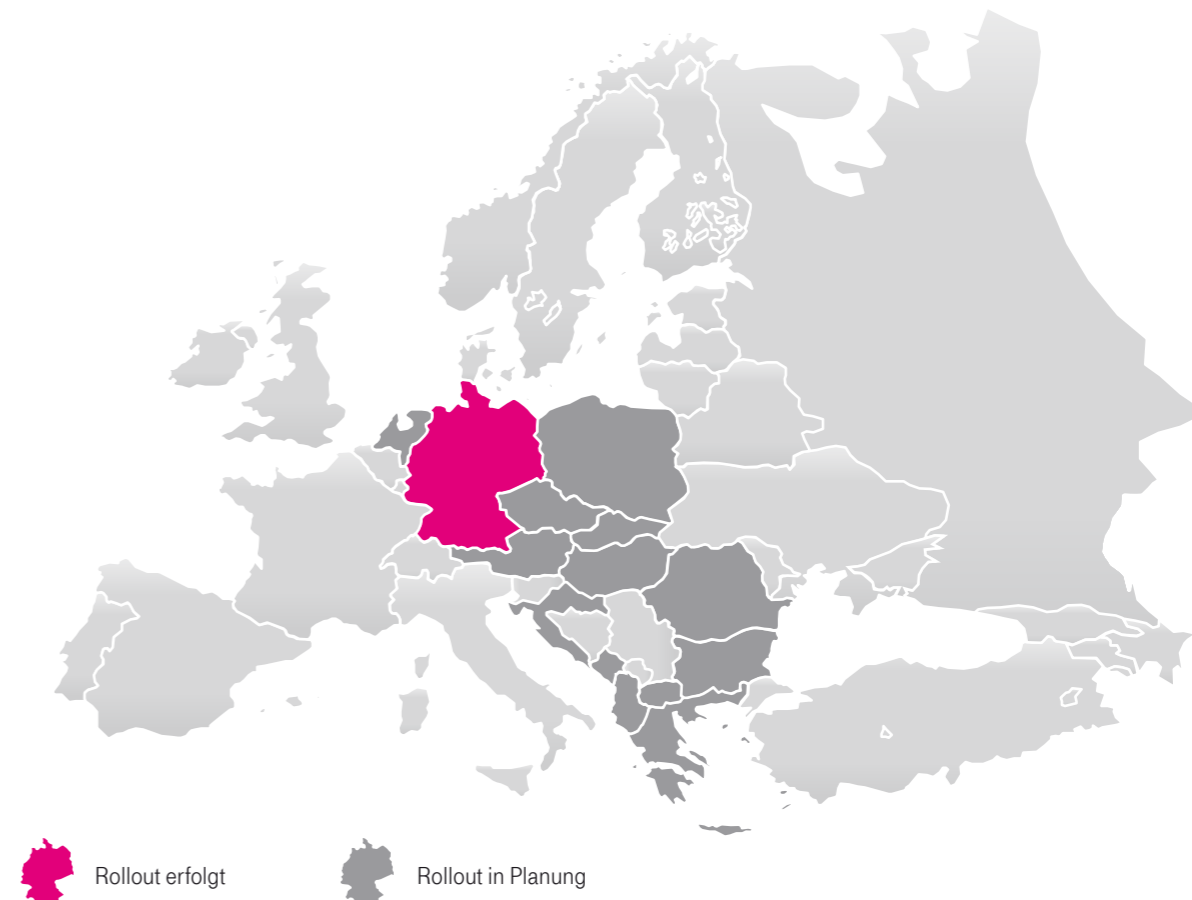
Alle älteren Vorgaben zur Erstellung von Sicherheits- oder Datenschutzkonzepten werden durch das neue PSA-Verfahren vollständig ersetzt. Um jedoch einen fließenden Übergang vom alten auf das neue Verfahren zu gewährleisten, bleiben existierende Sicherheits- und Datenschutzkonzepte bis Ende 2011 gültig. Bis zu diesem Zeitpunkt können die Verantwortlichen entscheiden, ob sie die alten Konzepte fortschreiben oder auf das neue Verfahren umsteigen möchten.

Die Anwendung des PSA-Verfahrens ist verbindlich für alle deutschen Gesellschaften sowie für länderübergreifende Projektvorhaben der Deutschen Telekom, sofern sie aus Deutschland gesteuert werden. Im Laufe des Jahres 2011 wird das PSA-Verfahren in enger Kooperation mit den IT- und Technikbereichen sukzessive auch in den ausländischen Gesellschaften der Deutschen Telekom – in einer an die lokalen Gegebenheiten angepassten Form – eingeführt. Die Einführung erfolgt gemeinsam mit der Sicherheitsorganisation der Corporate IT.

In Kürze

- ➔ Integration von Sicherheit und Datenschutz in Produkt- und Systementwicklung.
- ➔ Beratung, Dokumentation und Freigabe zu technischer Sicherheit und Datenschutz.
- ➔ PSA verbindlich in Deutschland, Einführung international in 2011.

Internationaler Rollout des PSA-Verfahrens.



Privacy and Security Assessment: Ziele.

GIS und GPR leisten innerhalb der Deutschen Telekom wichtige Grundlagenarbeit für verlässliche Produkte, die zudem hohen Anforderungen an Sicherheit und Datenschutz genügen. Sie haben das PSA-Verfahren gemeinsam eingeführt, um zu gewährleisten, dass alle Entwicklungsprojekte innerhalb des Konzerns die Anforderungen für technische Sicherheit und Datenschutz erfüllen können.

Group IT Security (GIS)



GIS trägt in der Deutschen Telekom die Verantwortung für die technische Sicherheit. Um dieser Aufgabe Rechnung zu tragen, gilt es, ein angemessenes Sicherheitsniveau festzulegen und dieses mit geeigneten Maßnahmen umzusetzen.

Group Privacy (GPR)



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

In Kürze

- ➔ Sicherstellung eines einheitlichen und adäquaten Sicherheits- und Datenschutzniveaus.
- ➔ Integriertes Verfahren für technische Sicherheit und Datenschutz.
- ➔ Projektbetreuungs niveau angepasst an Projektkomplexität und Kritikalität.



Das neue Verfahren adressiert die folgenden Ziele:

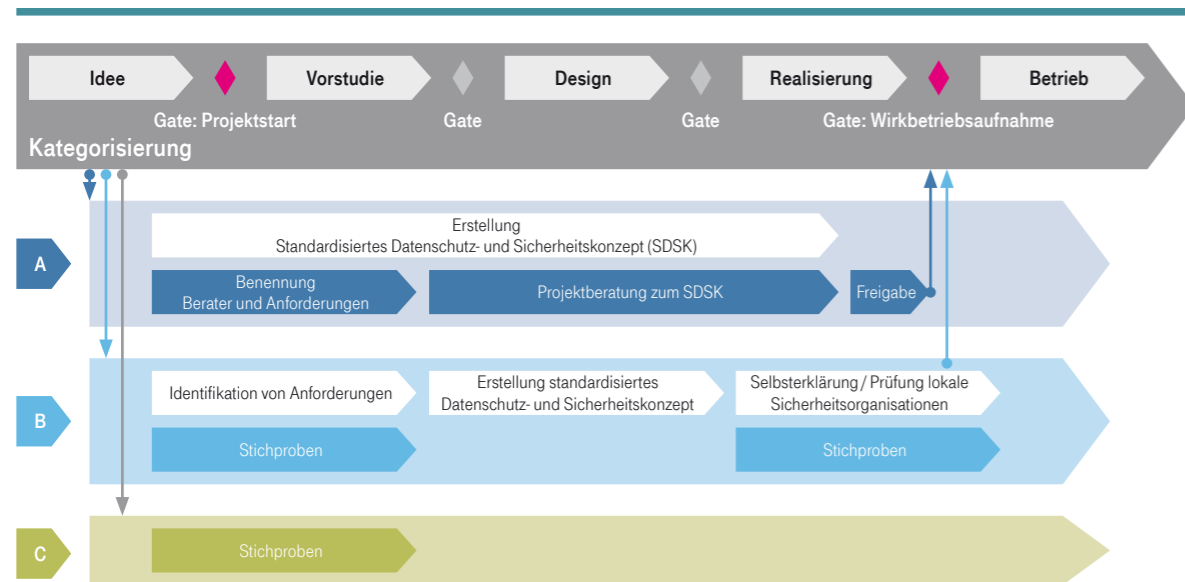
- Ein einheitliches und adäquates Sicherheits- und Datenschutzniveau in allen Produkten, Systemen und Plattformen, die aktualisiert oder neu erstellt werden.
- Ein integriertes Verfahren für technische Sicherheit und Datenschutz als Bestandteil der Produkt- und Systementwicklungsprozesse.
- Ein der Projektkomplexität und Kritikalität angepasstes Betreuungsniveau durch die Einführung einer Kategorisierung zu Beginn jedes Entwicklungsprojekts.

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 Aufsetzen 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 Vorhaben.

Privacy and Security Assessment: Beratungsansatz.

Im Folgenden wird die Methodik des PSA-Verfahrens entlang eines generischen Entwicklungsprozesses dargestellt. Dabei werden die Integration in den Entwicklungsprozess sowie die Unterschiede, die sich abhängig von der jeweiligen Projektkategorisierung ergeben, erläutert.

Der PSA-Prozess im Überblick.



In Kürze

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

Integration in die Entwicklungsprozesse.

Das PSA-Verfahren ist in die wesentlichen 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.

Das PSA-Verfahren ist an die Entscheidungspunkte (Gates) zum Projektstart und zur Wirkbetriebsaufnahme gekoppelt. Zum Projektstart erfolgt während der „Ideengenerierung“ eine Kategorisierung hinsichtlich der Sicherheits- und Datenschutzrelevanz. Mit dem Ende der Phase „Realisierung“, das heißt vor der Aufnahme des Wirkbetriebes, 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 GIS und GPR nicht direkt in die Projektbetreuung eingebunden, erfolgt die Wirksamkeitsprüfung des Verfahrens über Stichproben.

Projektkategorisierung.

Vor dem Entscheidungspunkt (Gate) zum Projektstart kategorisiert ein Projektleiter sein Projekt mithilfe eines Kategorisierungstools. Dieses Tool legt in drei verschiedenen Kategorien (A, B, C) die Kritikalität und Komplexität der aus dem Projekt resultierenden Anforderungen hinsichtlich technischer Sicherheit und Datenschutz fest. Daraus leitet sich ab, mit welcher

Detailtiefe das Projekt betreut und freigegeben wird. Die Kategorisierung basiert auf Eigenschaften wie der Verarbeitung besonders sensibler Daten, der Komplexität der betrachteten Plattformen oder Systeme oder der strategischen und finanziellen Bedeutung der Produkte.

Relevanz und Betreuungstiefe der Projekte.

Kategorie	Relevanz / Detailtiefe der Betreuung / Freigabe	Prozentuale Verteilung *
A	<ul style="list-style-type: none"> Hohe Relevanz, da komplexe und / oder kritische Projekte. Das Projekt wird durch Sicherheits- und / oder Datenschutzexperten aus den Bereichen GIS und GPR direkt begleitet, beraten sowie freigegeben. 	46%
B	<ul style="list-style-type: none"> Relevanz, aber weniger komplexe Projekte 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, ggf. geprüft durch lokale Sicherheitsorganisationen; die Bereiche GIS und GPR überprüfen stichprobenartig. 	35%
C	<ul style="list-style-type: none"> Keine Änderungen oder generell keine Relevanz. Die Projekte nehmen keine Änderungen vor, die Sicherheits- und / oder Datenschutzrelevanz haben. Es bedarf keiner Freigabe; die Bereiche GIS und GPR überprüfen die Projektkategorisierungen stichprobenartig. 	19%

* Verteilung der Kategorisierungen in 2010.

Privacy and Security Assessment: Zusammenhang Projekt- und Systemebene.

Das PSA-Verfahren basiert auf zwei zentralen Dokumenten, dem PSA-Template und dem standardisierten Sicherheits- und Datenschutzkonzept (SDSK).

PSA-Template.

Das PSA-Template ist das Formular zur Dokumentation der Projektkategorisierung und -freigabe. Es wird auf Projektebene durch den Projektleiter erstellt. Die Projektfreigabe und deren Dokumentation im PSA-Template erfolgen in der Regel erst nach Freigabe aller Systeme. Die Freigabe aller Systeme im PSA-Template ist somit Voraussetzung für die Projektfreigabe zur Wirkbetriebsaufnahme.

Privacy & Security Assessment
Dokumentation der Projekt-Kategorisierung und -Freigabe

1. Privacy Assessment
 A. Freigabe (A) ohne Auflage mit Auflage nicht erteilt*
 B1. Selbsterklärung (B1/B2) ohne Auflage mit Auflage nicht erteilt*
 B2. ohne Auflage mit Auflage nicht erteilt*
 C. Keine Angaben

2. Bestätigung der Datenschutz- und Security System-Freigaben für neue und modifizierte IT/NT-Systeme**

Systemname	Re-lease	Systemverantwortlicher				Datenschutz System-Freigabe/ Selbsterklärung & ggf. Prüfung lokaler DSBer				Security System-Freigabe/ Selbsterklärung & ggf. Prüfung lokaler PSM					
		Name, Telefon	Org. Einheit	Kategorie	Freigabe/ Selbsterkl. (Name)	Ggf. Prüfung (Name)	Ohne Auflage	Mit Auflage	nicht erteilt	Kategorie	Freigabe/ Selbsterkl. (Name)	Ggf. Prüfung (Name)	Ohne Auflage	Mit Auflage	nicht erteilt
System 1	Nr.	Name, Telefon	Org. Einheit	A	Name	n.a.				A	Name	n.a.			
System 2	Nr.	Name, Telefon	Org. Einheit	A	Name	n.a.	X			A	Name	n.a.	X		
System 3	Nr.	Name, Telefon	Org. Einheit	A	Name	n.a.		X		A	Name	n.a.		X	
System 4	Nr.	Name, Telefon	Org. Einheit	C	n.a.	n.a.				B	Name	Name			

Klassifikation gemäß Informationsschutzrichtlinie: Intern

* Falls eine Freigabe abgelehnt oder nur mit Auflagen erteilt wurde, dann fügen Sie bitte diesem Template ein formloses Dokument bei (oder betten es elektronisch ein), welches die jeweiligen Auflagen dokumentiert oder die Ablehnung begründet.
 ** Für weitere IT/NT Systeme: Öffnen Sie bitte hier das [Eckdaten-Formular](#) (Rechte Maustaste → "Hyperlink öffnen", dann „Dokument bearbeiten“)

← Erläuterungen zum PSA-Template.

1. Dokumentation der Projektkategorisierung und -freigabe durch den Projektleiter, die Sicherheits- und Datenschutzexperten aus den Bereichen GIS und GPR oder den lokalen Sicherheits- und Datenschutzeinheiten.
2. Liste der betroffenen neu erstellten oder modifizierten IT- oder NT-Systeme inklusive Freigabestatus.

In Kürze

- ➔ Dokumentation der Projektkategorisierung und -freigabe im PSA-Template.
- ➔ Dokumentation der Umsetzung der Sicherheits- und Datenschutzanforderungen und Freigaben im SDSK.

SDSK.

Das SDSK wird durch den Systemverantwortlichen pro System erstellt und gepflegt. Der Systemverantwortliche hat die Aufgabe, für sein jeweiliges System 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 über den gesamten Lebenszyklus eines Systems.

Erläuterungen zum SDSK.

1. Das SDSK setzt sich wie folgt zusammen:
 - Systembeschreibung
 - Datenschutzinformation
 - Berechtigungskonzept
 - Anforderungskataloge
 - Maßnahmenplan
 - Systemkategorisierung
2. Da das SDSK über den gesamten Lebenszyklus eines Systems gepflegt wird, enthält es die Fortschreibung der jeweiligen Releases inklusive Freigabestatus.

Standardisiertes Datenschutz- & Sicherheitskonzept

Systeminformation
 Systemname: *Kurztext* SDSK Version: *Nr.* Letzte Aktualisierung: *xx.xx.xxxx*
 Eindeutige Systemkennzeichnung: z.B. *App-ID, ICTO-ID*
 Systemverantwortlicher: *Name* Org.-Einheit: *Org.* Telefonnr.: *+49 (xxx) xxxxxxxx*

Dokumentation zum Standardisierten Datenschutz- & Sicherheitskonzept

Systembeschreibung	Berechtigungskonzept	Datenschutzinformation	Anforderungskataloge	Maßnahmenplan	Kategorisierung
Hier die Systembeschreibung als Datei einbinden. Link zum Template.	Hier das Berechtigungskonzept als Datei einbinden. Link zum Template.	Hier die ausgefüllte Datenschutzinformation als Datei einbinden. Wählen Sie das Template des Datenschutzes	Hier die ausgefüllten SoC als Datei einbinden. Wählen Sie das SoC des Datenschutzes	Hier die ausgefüllte Maßnahmenplanung als Datei einbinden. Link zum Template. Wählen Sie das Template der Maßnahmenplanung	Optionen** (siehe Rückseite) Hier das Kategorisierungstool für Systeme als Datei einbinden. Wählen Sie das Kategorisierungstool
Datum: dd.mm.yyyy	Datum: dd.mm.yyyy	Datum: dd.mm.yyyy	Datum: dd.mm.yyyy	Datum: dd.mm.yyyy	Datum: dd.mm.yyyy

2. Änderungshistorie

SDSK Vers.	System Id.	Datenschutz Kategorie	Datum	Freigabe/ Selbsterkl. (Name)	Ggf. Prüfung (Name)	Ohne Auflage	Mit Auflage	Keine Freigabe	Security Kategorie	Datum	Freigabe/ Selbsterkl. (Name)	Ggf. Prüfung (Name)	Ohne Auflage	Mit Auflage	Keine Freigabe
1.0.2	1.0	B1	31.01.2005	Name (Name)	Name (Name)	X			A	15.02.2005	Name (Name)	n.a.		X	
1.1	1.1	B1	10.09.2006	Name (Name)	Name (Name)		X		A	10.09.2006	Name (Name)	n.a.		X	
1.2.3	1.2	B1	30.06.2007	Name (Name)	Name (Name)	X			C	30.06.2007	n.a.	n.a.			X
2.0.7	2.0	B1	31.05.2008	Name (Name)	Name (Name)		X	X	A	30.04.2008	Name (Name)	n.a.			X

Klassifikation gemäß Informationsschutzrichtlinie: Vertraulich

* Eine Systemfreigabe ist nicht erforderlich, wenn mit dem Release des IT/NK-Systems keine datenschutz- oder sicherheitsrelevanten Änderungen erfolgen.

Privacy and Security Assessment: Nutzen des Verfahrens.

Die Einführung des Privacy and Security Assessments (PSA-Verfahrens) verleiht der Sicherheits- und Datenschutzarbeit der Deutschen Telekom mehr Struktur und Transparenz. Entwicklungsprojekte erhalten durch das Verfahren ein einheitliches und adäquates Sicherheits- und Datenschutzniveau, das effizient in standardisierten Templates dokumentiert wird. Die Projektunterstützung erfolgt für technische Sicherheit und Datenschutz entlang eines einheitlichen Vorgehensmodells. Durch dieses Vorgehensmodell ist sichergestellt, dass alle Sicherheits- und Datenschutzanforderungen frühzeitig bekannt sind. Die rechtzeitige Einbindung hat den Vorteil, dass kostenintensive Nachbesserungen sowie unnötige Kompromisse vermieden werden können.



Außerdem wird verhindert, dass durch eine zu späte Einbindung Projekte möglicherweise vor Wirkbetriebeaufnahme noch gestoppt werden müssen. DRC kann dank der Projektkategorisierung die Beratungsintensität für technische Sicherheit und Datenschutz optimal auf die wichtigsten Themen fokussieren und eine schnelle Projektarbeit nachhaltig unterstützen.

In Kürze

- ➔ Mehr Struktur und Transparenz der Sicherheits- und Datenschutzarbeit.
- ➔ Adäquates Sicherheits- und Datenschutzniveau durch standardisiertes Vorgehensmodell.
- ➔ Mehr Effizienz durch frühzeitige Einbindung.

Der Nutzen des PSA-Verfahrens im Überblick.

Nutzen	Beschreibung des Nutzens
Einheitlichkeit	Die Prüfung und Bewertung von technischer Sicherheit und Datenschutz basiert auf einheitlichen Anforderungen und Kriterien.
Aufwandsreduktion	Redundanzen in der Dokumentation sind durch einheitliche und standardisierte Templates minimiert.
Frühzeitigkeit	Die Integration in die Entwicklungsprozesse stellt eine frühzeitige Einbindung von technischer Sicherheit und Datenschutz in die relevanten Themen sicher.
Ressourcenoptimierung	Eine Priorisierung der Projekte stellt sicher, dass die kritischen und komplexen Projekte durch Experten aus GIS und GPR unterstützt werden.
Verlässliche Umsetzung	Der modulare anforderungsbasierte Ansatz ermöglicht den Projekten die sichere Umsetzung der relevanten Maßnahmen.

Anhang.

Glossar.

Anforderungskataloge

Dokumentation des Erfüllungsgrades der Anforderungen aus technischer Sicherheit und Datenschutz

Berechtigungskonzept

Beschreibung von Rollen und Funktionen

Datenschutzinformation

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

DRC

Vorstandsbereich Datenschutz, Recht und Compliance

GIS

Group IT Security

GPR

Group Privacy

IT- oder NT- System

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

Maßnahmenplan

Dokumentation von Maßnahmen, durch die Anforderungen in Zukunft erfüllt werden

PSA

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

SDSK

Standardisiertes Datenschutz- und Sicherheitskonzept

Systembeschreibung

Dokumentation der Verantwortlichkeiten sowie funktionale und technische Systembeschreibung

Impressum.

Deutsche Telekom AG
Group IT Security / Group Privacy
Friedrich-Ebert-Allee 140
D-53113 Bonn

Gestaltung:
HGB Hamburger Geschäftsberichte GmbH & Co. KG

Stand der Broschüre: März 2011

Kontakt.

Group IT Security:
SecurityDemandManagement@telekom.de

Group Privacy:
datenschutz@telekom.de