scope & focus
Service-Gesellschaft mbH

Durchführung einer DSFA mit verinice auf Grundlage der ISO 29134:2017

Dipl.-Ök. Stephan Rehfeld

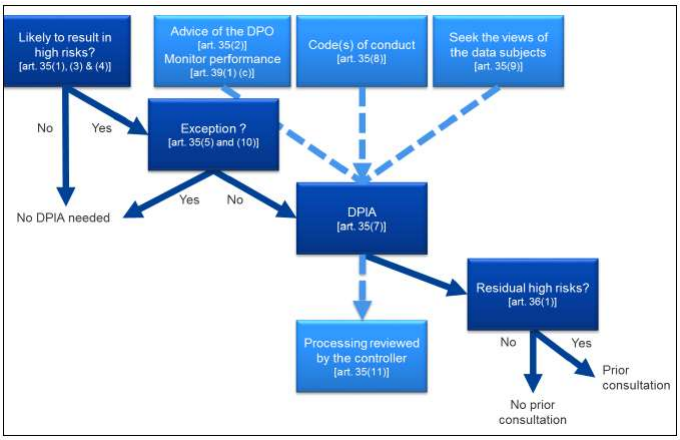
1

scope & focus
Service-Gesellschaft mbH

DATENSCHUTZ-FOLGENABSCHÄTZUNG

scope & focus Service-Gesellschaft mbH

Prüfung der Pflicht zur Durchführung einer DSFA



Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4.10.2017

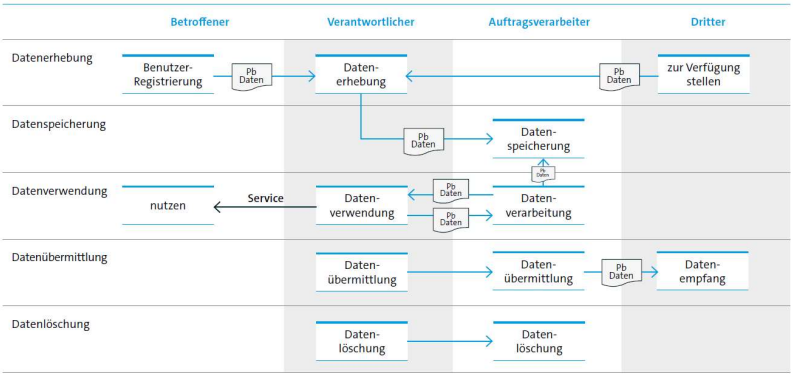
scope & focus Service-Gesellschaft mbH

Kriterien für »hohes Risiko« von Art. 29-Datenschutzgruppe (WP 248)

1. Evaluierung oder Scoring, inklusive Profilbildung und Vorhersagen
2. Automatisierte Entscheidungen mit rechtlicher oder ähnlich beeinträchtigender Wirkung
3. Systematische Beobachtung
4. Sensible Daten
5. In großem Umfang verarbeitete Daten
6. Datensätze, die abgeglichen oder kombiniert wurden
7. Daten, die verletzliche Datensubjekte betreffen
8. Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen
9. Datenübermittlung in Drittstaaten außerhalb der EU
10. Datenverarbeitungen, die den Betroffenen davon abhalten, ein Recht geltend zu machen oder einen Dienst oder Vertrag zu nutzen

scope & focus Service-Gesellschaft mbH

Systembeschreibung



Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung, 2017

scope & focus Service-Gesellschaft mbH

Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen

- Rechtmäßigkeit und Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Verfügbarkeit (Belastbarkeit)
- Persönliche Teilhabe und Zugang
- Rechenschaftspflicht

scope & focus Service-Gesellschaft mbH

Abhilfemaßnahmen

	Es sind für die Verarbeitung **keine genehmigten Verhaltensregeln vorhanden**		Es sind für die Verarbeitung **genehmigten Verhaltensregeln vorhanden**
	Vorschläge für Maßnahmenkataloge (zu modifizieren auf die Anforderungen der DS-GVO)	zu beachten beim Technikeinsatz:	Sofern die Organisation sich vorhandenen genehmigten Verhaltensregeln unterwerfen will
Compliance-Sicht	Möglicher Maßnahmenkatalog der CNIL: CNIL, Measures for the privacy risk treatment, 2012 Möglicher Maßnahmenkatalog aus der ISO-Welt Für Verantwortliche: ISO/IEC DIS 29151, Annex A Für Auftragsverarbeiter: ISO/IEC 27018, Annex A	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO	Anwendungen der genehmigten Verhaltensregeln
Risiko-Sicht	Möglicher Maßnahmenkatalog der CNIL: CNIL, Measures for the privacy risk treatment, 2012 Möglicher Maßnahmenkatalog aus der ISO-Welt Für Verantwortliche: ISO/IEC DIS 29151 Für Auftragsverarbeiter: ISO/IEC 27018 mit den Erläuterungen der ISO/IEC 27002		

Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung, 2017

scope & focus Service-Gesellschaft mbH

DSFA-Bericht

- Ein Bericht für eine Datenschutz-Folgenabschätzung muss gemäß Artikel 35 Absatz 7 mindestens die folgenden Angaben enthalten:
  - eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
  - eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
  - eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
  - die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

scope & focus Service-Gesellschaft mbH

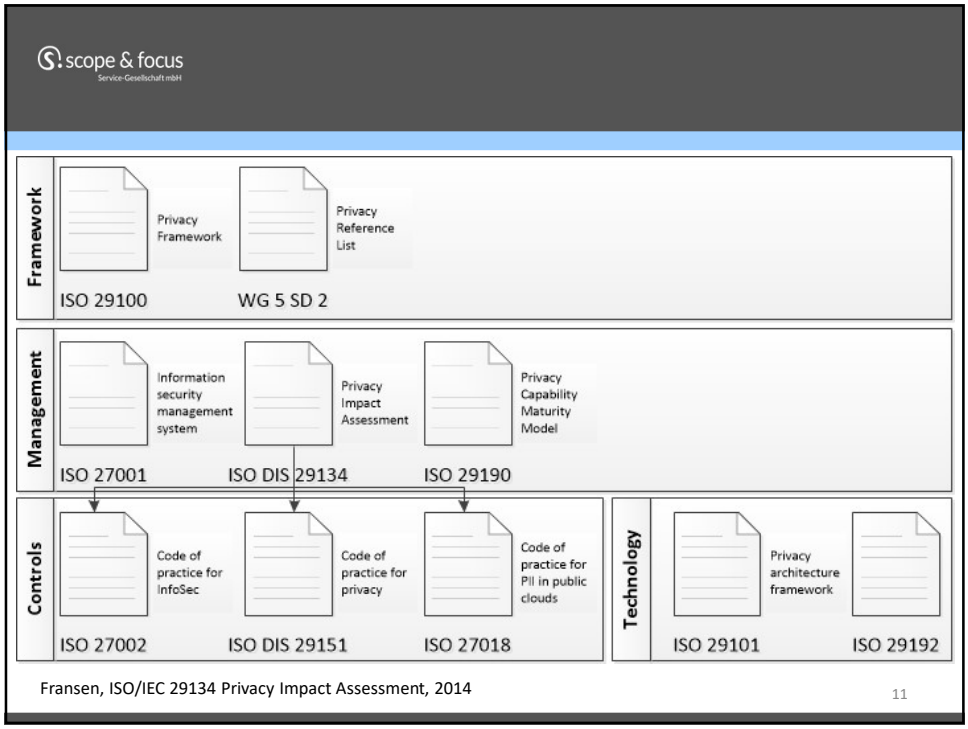
DSFA-Bericht mit Konsultation

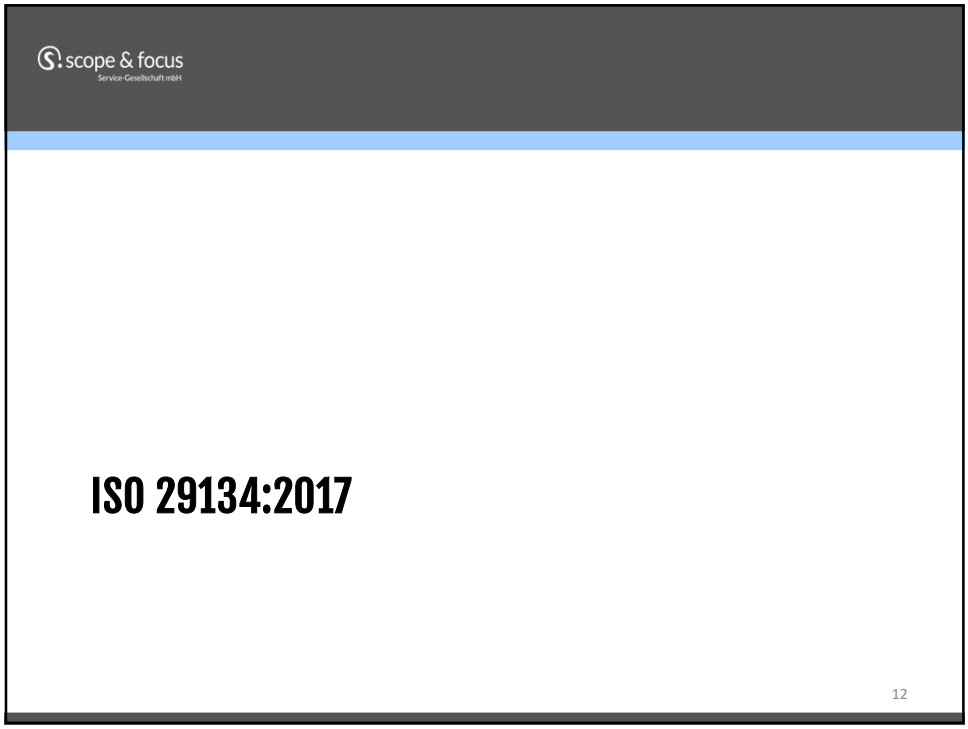
- Sofern eine Konsultation der Aufsichtsbehörde notwendig ist, muss ein DSFA-Bericht um die folgenden Angaben ergänzt werden (Artikel 36 Absatz 3):
  - gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
  - die Zwecke und die Mittel der beabsichtigten Verarbeitung;
  - die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
  - gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
  - die Datenschutz-Folgenabschätzung gemäß Artikel 35 und
  - alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

scope & focus Service-Gesellschaft mbH

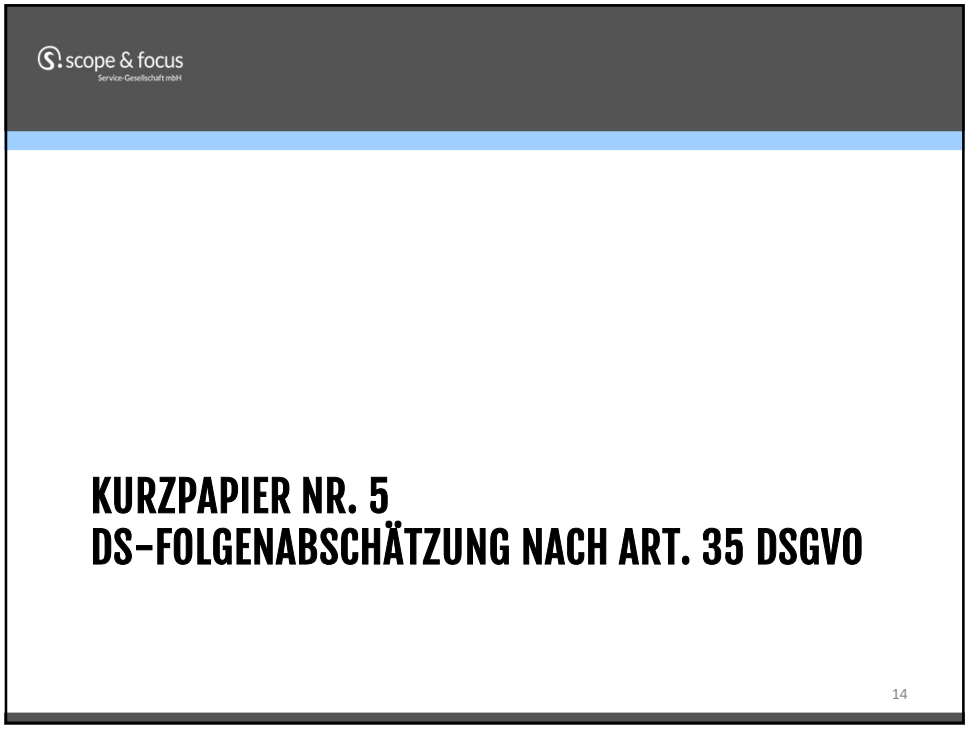
DS-NORMEN DER ISO

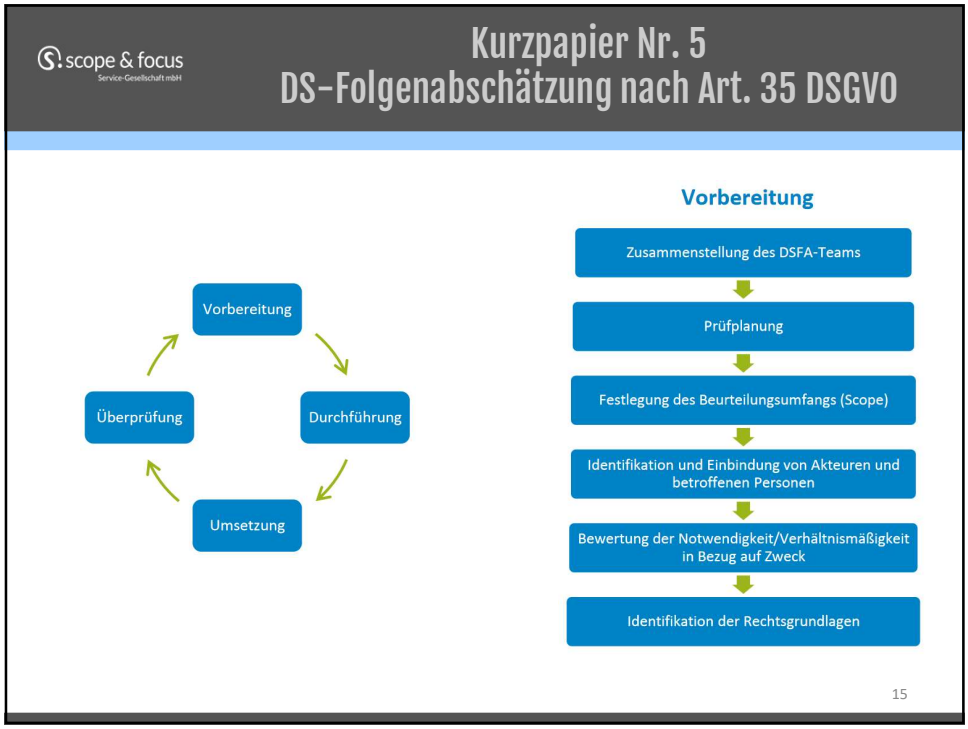
10

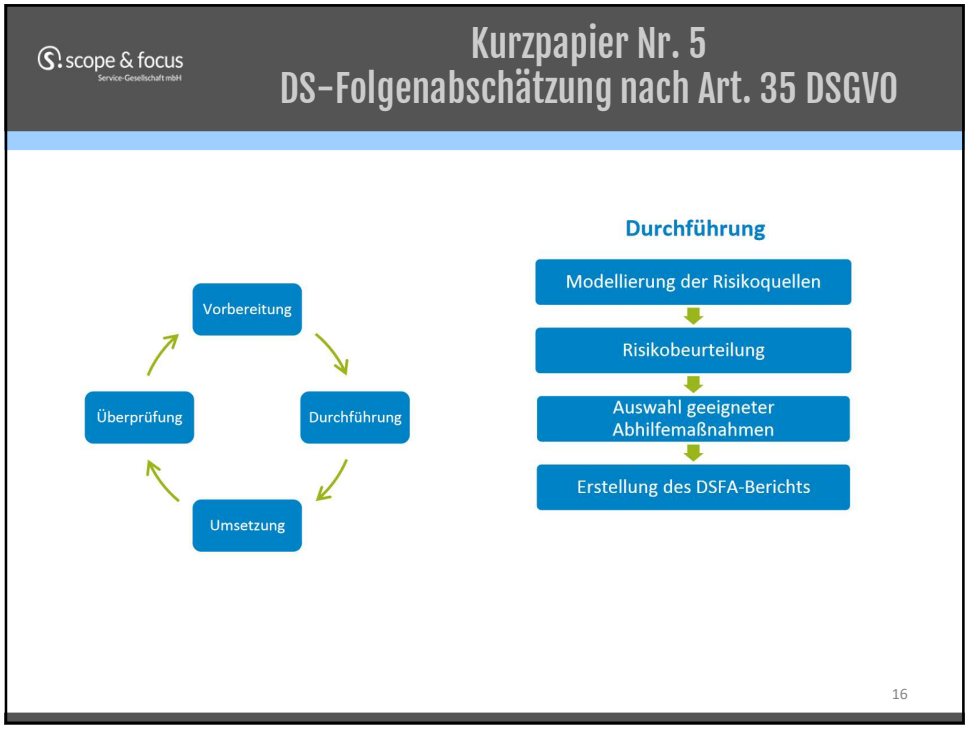

scope & focus
Framework
Privacy Framework
Privacy Reference List
ISO 29100
WG 5 SD 2
Management
Information security management system
Privacy Impact Assessment
Privacy Capability Maturity Model
ISO 27001
ISO DIS 29134
ISO 29190
Controls
Code of practice for InfoSec
Code of practice for privacy
Code of practice for PII in public clouds
ISO 27002
ISO DIS 29151
ISO 27018
Technology
Privacy architecture framework
ISO 29101
ISO 29192
Fransen, ISO/IEC 29134 Privacy Impact Assessment, 2014
11

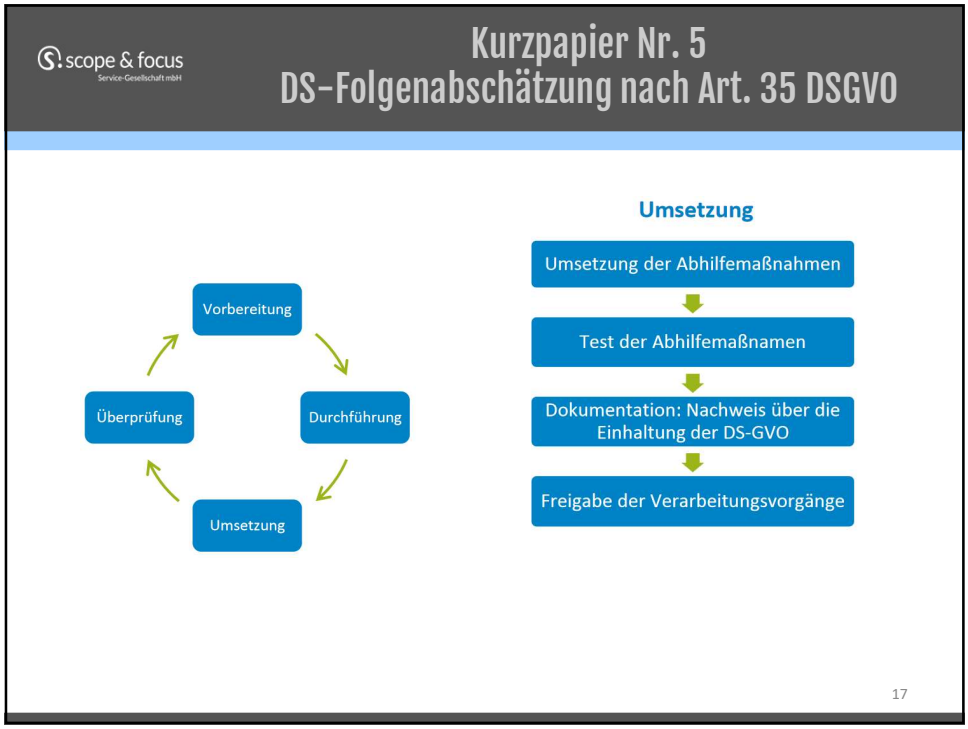

scope & focus
ISO 29134:2017
12

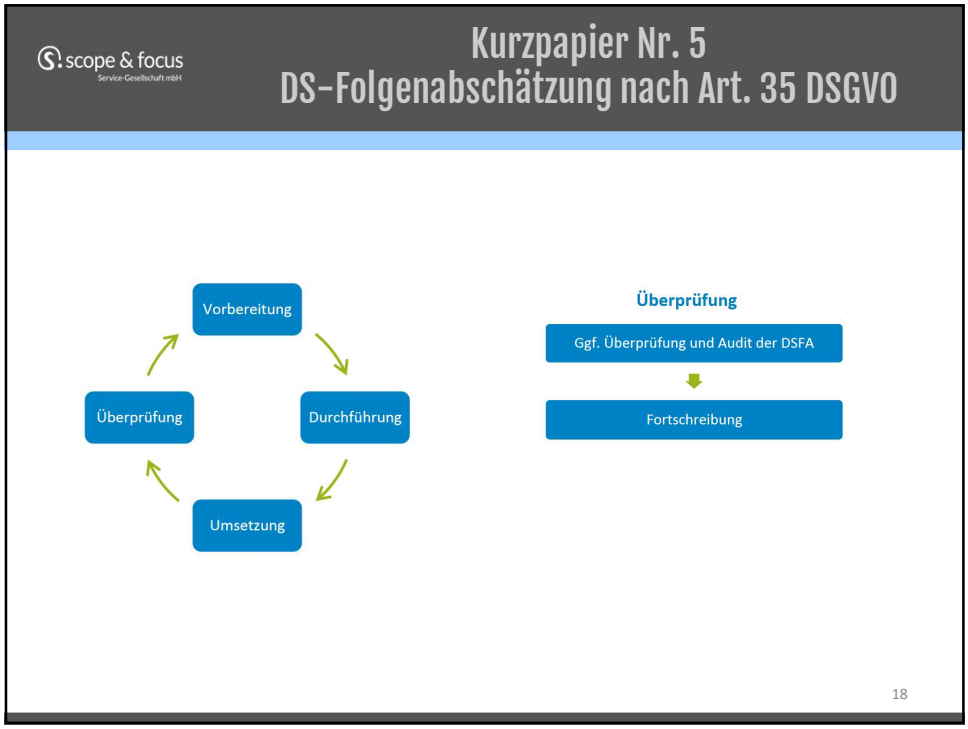

scope & focus
Service-Gesellschaft mbH
scope & focus
Ihre Daten - mit Sicherheit!
Privacy Impact Assessments (PIA)
www.scope-and-focus.com
Ausgaben
Ansichten
Prozesslandschaft
Mgmt.
Determine whether a PIA is necessary
Mgmt.
conduct a threshold analysis
Assessor
Preparation of the PIA
Assessor
Set up the PIA team an provide it with direction
Assessor
Prepare a PIA plan and deter-mine ressources
Assessor
Describe what is being assessed
Stakeholder engagement
Assessor
Perform the PIA
Assessor
Identify information flows of PII
Assessor
Analyse the implications of the use case
Assessor
Determine the relevant privacy safeguarding r...
Assess privacy risks
Prepare for treating privacy risks
Assessor
Follow up of the PIA
Assessor
Prepare the report
Assessor
Publication
Vorgese...
Implement privacy risk treatment plans
Mgmt.
Review and/or audit of the PIA
Mgmt.
Reflect changes to the process
13


scope & focus
Service-Gesellschaft mbH
KURZPAPIER NR. 5
DS-FOLGENABSCHÄTZUNG NACH ART. 35 DSGVO
14


scope & focus
Service-Gesellschaft mbH
Kurzpapier Nr. 5
DS-Folgenabschätzung nach Art. 35 DSGVO
Vorbereitung
Durchführung
Umsetzung
Überprüfung
Vorbereitung
Zusammenstellung des DSFA-Teams
Prüfplanung
Festlegung des Beurteilungsumfangs (Scope)
Identifikation und Einbindung von Akteuren und betroffenen Personen
Bewertung der Notwendigkeit/Verhältnismäßigkeit in Bezug auf Zweck
Identifikation der Rechtsgrundlagen
15


scope & focus
Service-Gesellschaft mbH
Kurzpapier Nr. 5
DS-Folgenabschätzung nach Art. 35 DSGVO
Vorbereitung
Durchführung
Umsetzung
Überprüfung
Durchführung
Modellierung der Risikoquellen
Risikobeurteilung
Auswahl geeigneter Abhilfemaßnahmen
Erstellung des DSFA-Berichts
16


scope & focus
Service-Gesellschaft mbH
Kurzpapier Nr. 5
DS-Folgenabschätzung nach Art. 35 DSGVO
Vorbereitung
Durchführung
Umsetzung
Überprüfung
Umsetzung
Umsetzung der Abhilfemaßnahmen
Test der Abhilfemaßnamen
Dokumentation: Nachweis über die Einhaltung der DS-GVO
Freigabe der Verarbeitungsvorgänge
17


scope & focus
Service-Gesellschaft mbH
Kurzpapier Nr. 5
DS-Folgenabschätzung nach Art. 35 DSGVO
Vorbereitung
Durchführung
Umsetzung
Überprüfung
Überprüfung
Ggf. Überprüfung und Audit der DSFA
Fortschreibung
18

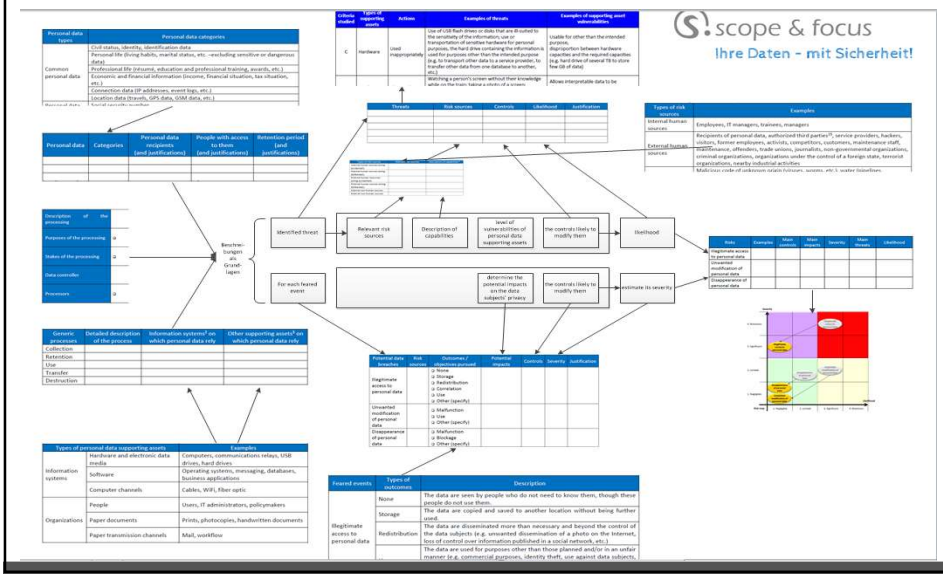
scope & focus
Service-Gesellschaft mbH

DATENSCHUTZ-RISIKOANALYSE

19

scope & focus
Service-Gesellschaft mbH

Berechnung nach CNIL



scope & focus Service-Gesellschaft mbH

Risikoquellen

Risikoquellen (Typ)			Relevante Risikoquellen	Beschreibung der Potenz der Risikoquellen
Menschliche Risikoquellen	intern	unbeabsichtigt	Mitarbeiter, Vorgesetzte	Relevante Risikoquellen verwenden keine Ressourcen auf versehentliche Aktionen.
		vorsätzlich		Relevante Risikoquellen verwenden minimale Ressourcen auf vorsätzliche Aktionen (z.B. bei Kündigung oder Abmahnungen).
	extern	unbeabsichtigt	Wartungspersonal, Mitbewerber, Hacker	Relevante Risikoquellen verwenden keine Ressourcen auf versehentliche Aktionen.
		vorsätzlich		
Nichtmenschliche Risikoquellen	intern		Wasserschaden durch Rohrbruch, Feuer	Wasserschaden durch Rohrbruch und Feuer traten in den letzten 15 Jahren Betriebstätigkeit nicht auf.
	extern		Stromausfall, Ausfall der Internet-Leitung	Ausfall der Internet-Leitung und Stromausfall treten regelmäßig auf, die Betriebsunterbrechungen sind aber bisher nicht relevant gewesen.

21

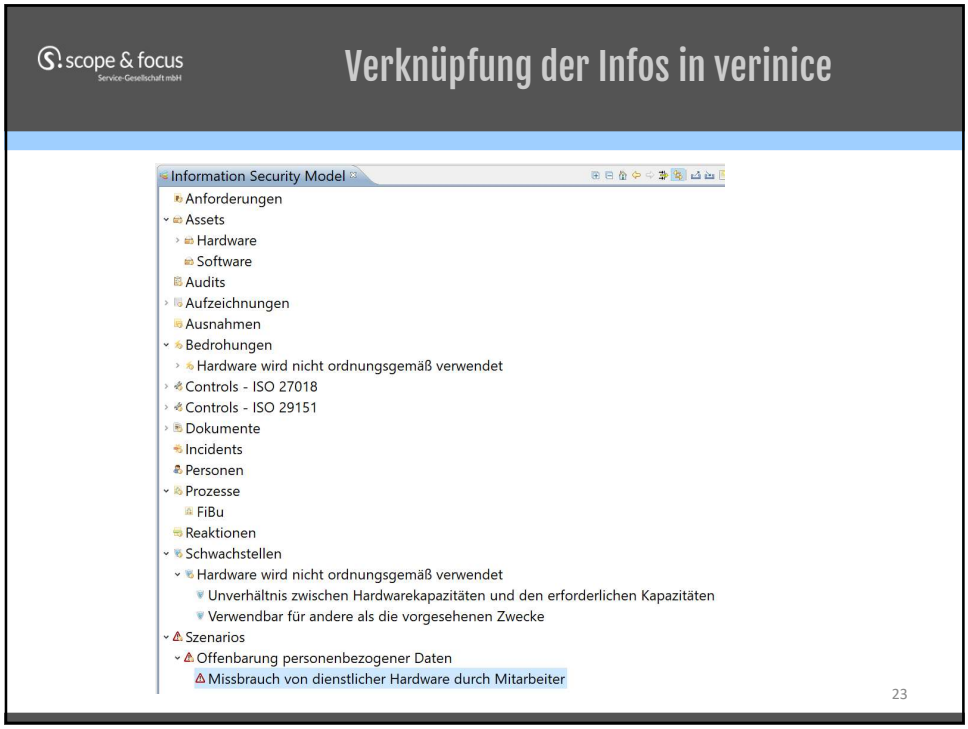
scope & focus Service-Gesellschaft mbH

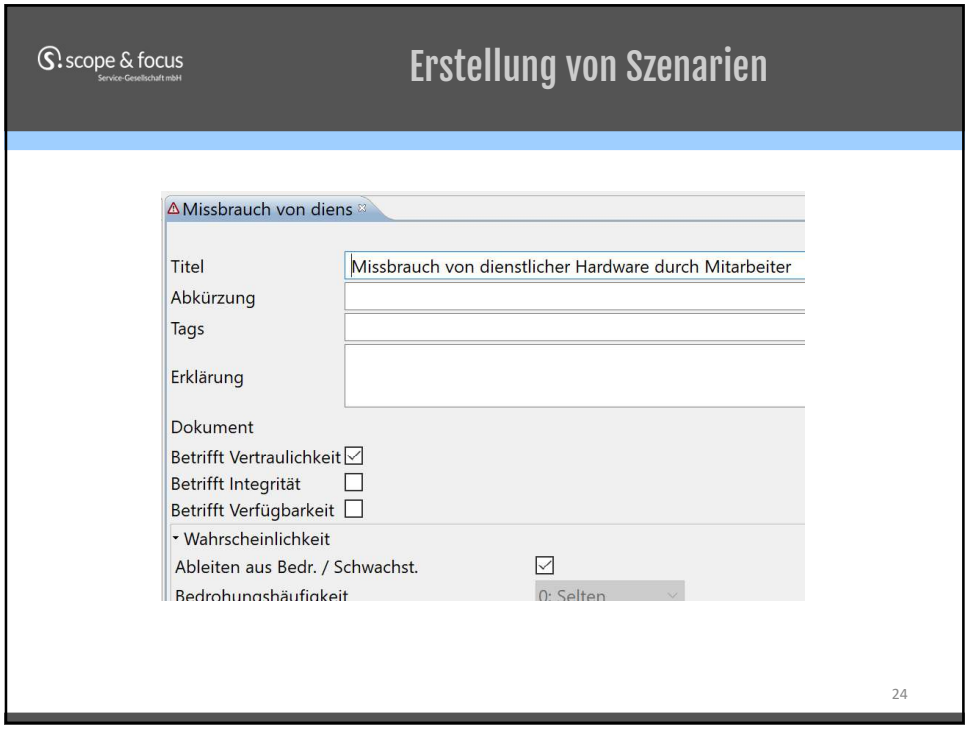
Katalog: Bedrohungen, Schwachstellen etc.

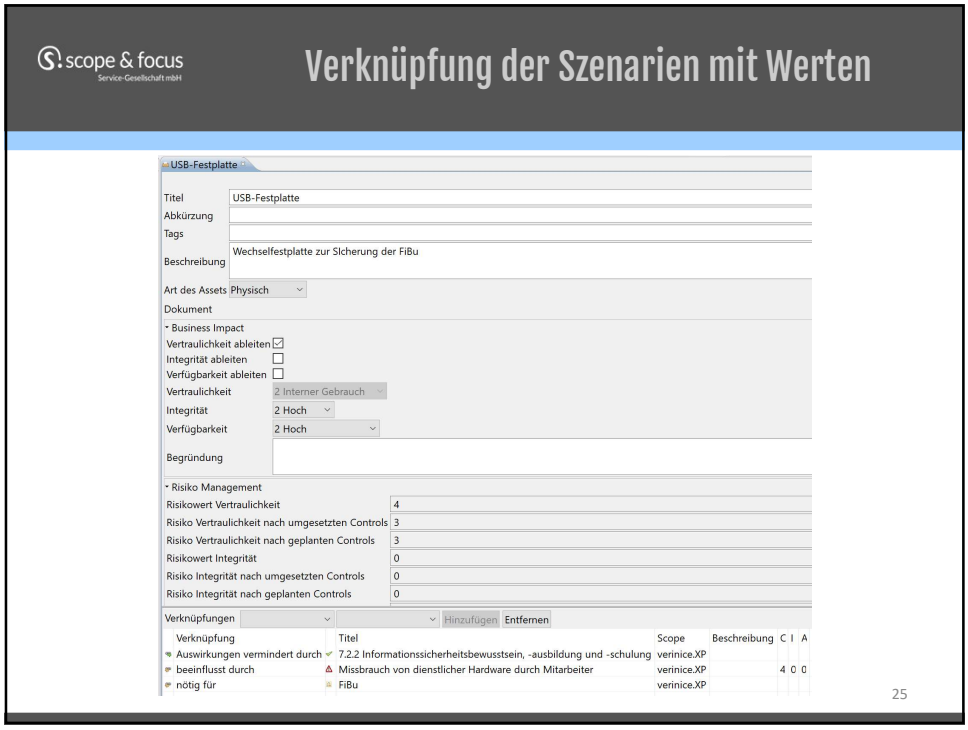
1.7. Threats that can lead to an illegitimate access to personal data

Criteria studied	Types of supporting assets	Actions	Examples of threats	Examples of supporting asset vulnerabilities
C	Hardware	Used inappropriately	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, the hard drive containing the information is used for purposes other than the intended purpose (e.g. to transport other data to a service provider, to transfer other data from one database to another, etc.)	Usable for other than the intended purpose, disproportion between hardware capacities and the required capacities (e.g. hard drive of several TB to store few GB of data)
C	Hardware	Observed	Watching a person's screen without their knowledge while on the train; taking a photo of a screen; geolocation of hardware; remote	Allows interpretable data to be observed; generates compromising emanations

22


scope & focus
Service-Gesellschaft mbH
Verknüpfung der Infos in verinice
Information Security Model
Anforderungen
Assets
Hardware
Software
Audits
Aufzeichnungen
Ausnahmen
Bedrohungen
Hardware wird nicht ordnungsgemäß verwendet
Controls - ISO 27018
Controls - ISO 29151
Dokumente
Incidents
Personen
Prozesse
FiBu
Reaktionen
Schwachstellen
Hardware wird nicht ordnungsgemäß verwendet
Unverhältnis zwischen Hardwarekapazitäten und den erforderlichen Kapazitäten
Verwendbar für andere als die vorgesehenen Zwecke
Szenarios
Offenbarung personenbezogener Daten
Missbrauch von dienstlicher Hardware durch Mitarbeiter
23


scope & focus
Service-Gesellschaft mbH
Erstellung von Szenarien
Missbrauch von diens
Titel
Missbrauch von dienstlicher Hardware durch Mitarbeiter
Abkürzung
Tags
Erklärung
Dokument
Betrifft Vertraulichkeit
Betrifft Integrität
Betrifft Verfügbarkeit
Wahrscheinlichkeit
Ableiten aus Bedr. / Schwachst.
Bedrohungshäufigkeit
0: Selten
24


scope & focus
Service-Gesellschaft mbH
Verknüpfung der Szenarien mit Werten
USB-Festplatte
Titel
USB-Festplatte
Abkürzung
Tags
Beschreibung
Wechselfestplatte zur SIcherung der FiBu
Art des Assets
Physisch
Dokument
Business Impact
Vertraulichkeit ableiten
Integrität ableiten
Verfügbarkeit ableiten
Vertraulichkeit
2 Interner Gebrauch
Integrität
2 Hoch
Verfügbarkeit
2 Hoch
Begründung
Risiko Management
Risikowert Vertraulichkeit
4
Risiko Vertraulichkeit nach umgesetzten Controls
3
Risiko Vertraulichkeit nach geplanten Controls
3
Risikowert Integrität
0
Risiko Integrität nach umgesetzten Controls
0
Risiko Integrität nach geplanten Controls
0
Verknüpfungen
Hinzufügen
Entfernen
Verknüpfung
Titel
Scope
Beschreibung
C I A
Auswirkungen vermindert durch
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung
verinice.XP
beeinflusst durch
Missbrauch von dienstlicher Hardware durch Mitarbeiter
verinice.XP
4 0 0
nötig für
FiBu
verinice.XP
25


scope & focus
Service-Gesellschaft mbH
... und Verknüpfung mit Verarbeitungen
FiBu
Titel
FiBu
Beschreibung
FiBu - Geschäftsprozess zur Erfüllung der Buchführungspflichten.
Abkürzung
Tags
Dokument
Business Impact
Vertraulichkeit ableiten
Integrität ableiten
Verfügbarkeit ableiten
Vertraulichkeit
2 Interner Gebrauch
Integrität
2 Hoch
Verfügbarkeit
2 Hoch
Begründung
Aufnahme in Verfahrensverzeichnis
Verfahrensangaben
Art des Verfahrens
Neues Verfahren
Ort der Datenverarb.
Intern
Betriebsstadium
Betrieb
Anzahl Mitarbeiter
Bemerkungen
Verknüpfungen
Hinzufügen
Entfernen
Verknü...
Titel
Scope
Beschreibung
C I A
benötigt
USB-Festplatte
verinice.XP
26

scope & focus Service-Gesellschaft mbH

Anwendung von Reporten

Detaillierte Risikobeurteilung (mit Controls)

Abk.	Name	Vertraulichkeit	Integrität	Verfügbarkeit
	FiBu	2	2	2

Assets und Risikoszenarien			Risiko			Summe Gesamtrisiko
Abk.	Name	Typ	Vertraulichkeit	Integrität	Verfügbarkeit	
	Gesamtrestrisiko für FiBu:		**4**	**0**	**0**	**4**
	USB-Festplatte	**Physisch**	**4**	**0**	**0**	**4**
	Missbrauch von dienstlicher Hardware durch Mitarbeiter		4	0	0	4
Die Festplatte mit den Informationen wird für andere als die vorgesehenen Zwecke verwendet		0: Selten				
Verwendbar für andere als die vorgesehenen Zwecke		2: Hoch				

27

scope & focus Service-Gesellschaft mbH

FAZIT

28


scope & focus
Service-Gesellschaft mbH
scope & focus
Ihre Daten - mit Sicherheit!
Privacy Impact Assessments (PIA)
www.scope-and-focus.com
Ausgaben
Ansichten
Prozesslandschaft
Mgmt.
Determine whether a PIA is necessary
Mgmt.
conduct a threshold analysis
Assessor
Preparation of the PIA
Assessor
Set up the PIA team an provide it with direction
Assessor
Prepare a PIA plan and deter-mine ressources
Assessor
Describe what is being assessed
Stakeholder engagement
Assessor
Perform the PIA
Assessor
Identify information flows of PII
Assessor
Analyse the implications of the use case
Assessor
Determine the relevant privacy safeguarding r...
Assess privacy risks
Prepare for treating privacy risks
Assessor
Follow up of the PIA
Assessor
Prepare the report
Assessor
Publication
Vorgese...
Implement privacy risk treatment plans
Mgmt.
Review and/or audit of the PIA
Mgmt.
Reflect changes to the process
29


scope & focus
Service-Gesellschaft mbH
AUSBLICK
30

scope & focus
Service-Gesellschaft mbH

SICHERHEIT IN DER VERABREITUNG

31

scope & focus
Service-Gesellschaft mbH

Art. 32 Abs. 1 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: […]

32

scope & focus Service-Gesellschaft mbH

Art. 32 Abs. 1 DSGVO

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

33

scope & focus Service-Gesellschaft mbH

Art. 32 Abs. 2 DSGVO

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

34

scope & focus Service-Gesellschaft mbH

Der Gesetzgeber beschreibt im Gesetzestext, was für Informationssicherheits-Managementsysteme (ISMS) bereits seit Jahren ein völlig normales Vorgehen ist:

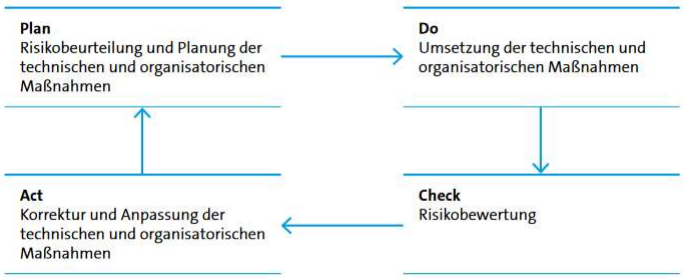
1. Als Motor des Management-Systems wird der PDCA-Zyklus eingesetzt.
2. Es werden die Phasen des Risiko-Prozesses beschrieben: Risiko-Assessments (Risiko-Beurteilung, der Erstellung und Umsetzung eines SoA und Risikobehandlungsplanes, interne Audits, Managementbewertung und Ergreifen von Korrekturmaßnahmen vorgeschrieben.

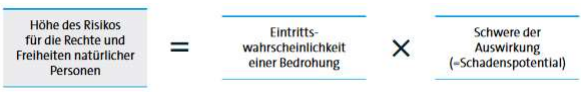
35

scope & focus Service-Gesellschaft mbH

Risikoorientierte Informationssicherheit

PDCA und risikobasierter Ansatz



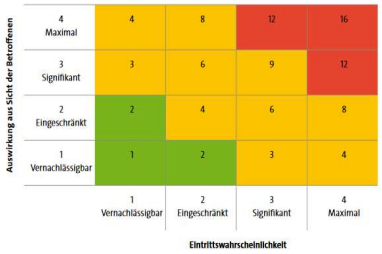


… und Einsatz eines „ISMS“

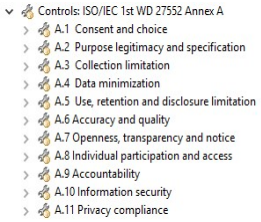
scope & focus
Service-Gesellschaft mbH

Datenschutz-Risikomanagement
Individueller Projektplan

- Risikoorientierte Maßnahmenauswahl



- Individueller Projektplan



scope & focus
Service-Gesellschaft mbH

scope & focus

Ihre Daten - mit Sicherheit!

Leonhardtstr. 2
30175 Hannover
T: 0511 | 364 221-0
F: 0511 | 364 221-99

Hoerneckestr. 19-21
28217 Bremen
T: 0421 | 369 3530-0
F: 0421 | 369 3530-99

www.scope-and-focus.com
information@scope-and-focus.com

Dipl.-Ök. Stephan Rehfeld
Dipl.-Wirt.-Ing. Ulrike Hauser

38