verinice.PRO

verinice.

Datenschutzfolgenabschätzung mit verinice V-1.19.1 sowie dem DSM 3.1

<Robert Raczynski>
<Berlin, 27. Februar 2020>
<verinicexp 2020>

verinice.PARTNERS

Agenda

- ISO/IEC 27701
- ISO/IEC 29134
- Datenschutzmanagement Prozess DSFA
- Risikoanalyse/Risikoberechnung
- Risikobeurteilung
- Risikobehandlung
- Verinice Datenschutzmodul 3.1 - LIVE
- Reporting
- Praxis-Beispiele

ISO/IEC 27701:2019-08

- Die ISO/IEC 27000-Reihe beinhaltet eine Sammlung von Standards zur IT-Sicherheit und nunmehr auch zum Datenschutzmanagement.

- ISO/IEC 27701 ist eine Erweiterung zu ISO/IEC 27001 sowie ISO/IEC 27002 für das Datenschutzmanagement und dessen Anforderungen und Leitfaden.

  (Erstauflage: August 2019)

- Der Standard beschreibt formale Abläufe und Strukturen für ein systematisches und prozessorientiertes Datenschutzmanagement, das auch die Anforderungen an ein Risikomanagement nach ISO/IEC 27001 erfüllt.

- Aktuell: ISO/IEC 27701:2019
  Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
  (international, 2019)

- Ein neues Arbeitsfeld wurde von der JTC 1/SC 27 von JTC 1/SC 27/WG 5 "Identitätsverwaltung und Privatsphärentechniken" auf einer Initiative von Experten im April 2016 vorgeschlagen. Französisches nationales Gehäuse (JTC 1/SC 27).
- Das Projekt wurde damals in JTC 1/SC 27/WG 5 unter der Nummer ISO/IEC 27552 entwickelt.
  Britische Standards Institution (BSI) machte die erste CD von ISO/IEC 27552 publik sowie im Februar 2018 erstmalig im Web Store öffentlich zugänglich.
- Die zweite CD der ISO/IEC 27552 wurde im August 2018 herausgegeben.
- Die DIS der ISO/IEC 27552 wurde im Januar 2019 ausgegeben und im März 2019 genehmigt. Da keine technischen Änderungen notwendig waren, wurde die FDIS Abstimmung umgangen.
- Die ISO/IEC JTC 1/SC 27 beendeten die technische Arbeit an ISO/IEC 27552 im April 2019. Vor ihrer Veröffentlichung wurden ISO/IEC 27552 zu ISO/IEC 27701 neu nummeriert.
  Die Resolution 39/2019, vom ISO/technischer Vorstand stellt unter Mandat, dass jeder Managementsystem "Typ A" (der Erfordernisse enthält) eine Nummer haben soll, die fertig mit "01" als seine letzten zwei Ziffern wird. Das Nummerieren wurde im Juli 2019 abgeschlossen.
  Der Grenzwert wurde am 6. August herausgegeben.

ISO/IEC 27701:2019-08

- Dieses Dokument gibt die Erfordernisse an ein Datenschutzmanagement an und liefert die Lenkung dafür, um relevante Datenschutzprozesse festzustellen. Dabei führt sie ein Privatsphäreninformationsverwaltungssystem (PIMS) durch, wartet es und verbessert es ständig in der Form einer Erweiterung auf Basis der ISO/IEC 27001 sowie ISO/IEC 27002 für Privatsphärenverwaltung innerhalb des Kontexts der Organisation.
- Dieses Dokument gibt darüber hinaus PIMS gebundene Erfordernisse an und liefert die Lenkung für PII Kontroller und PII Prozessoren, die Verantwortung und Verantwortlichkeit für die PII Verarbeitung haben.
- Dieses Dokument ist auf alle Arten und Größen von Organisationen, der Öffentlichkeit sowie Privatunternehmen ausgerichtet einschl. Regierungsentitäten und nicht gewinnerzielenden Organisationen anwendbar, innerhalb welcher PII Kontroller und/oder PII Prozessoren verarbeiten.

ISO/IEC 29134:2020-01

Information technology - Security techniques - Guidelines for privacy impact assessment (ISO/IEC 29134:2017); German and English version prEN ISO/IEC 29134:2019

Dieses Dokument enthält: - Leitlinien für einen Prozess zur Datenschutzfolgeabschätzung und - eine Struktur und Inhalte eines PIA-Berichts.

Dieses Dokument gilt für alle Arten und Größen von Unternehmen, einschließlich öffentlicher Unternehmen, privater Unternehmen, Regierungseinrichtungen und gemeinnütziger Organisationen.

Dieses Dokument ist für diejenigen relevant, die an der Planung oder Durchführung von Projekten beteiligt sind, einschließlich der Parteien, die Datenverarbeitungssysteme und -dienste betreiben, die PII verarbeiten.

Datenschutzfolgenabschätzung

Art. 35 DSGVO schreibt vor Aufnahme der Verarbeitung eine Datenschutzfolgenabschätzung vor, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Um die Erforderlichkeit einer Datenschutzfolgenabschätzung beurteilen zu können, müssen zuerst die Risiken für die Rechte und Freiheiten der betroffenen Personen ermittelt und analysiert sowie der Höhe nach beurteilt werden. Ist das Risiko bzw. sind die Risiken als hoch einzuschätzen, ist die Datenschutzfolgenabschätzung zwingend durchzuführen. Der nachstehende Prozess zeigt die rechtlichen Regelungen zur Datenschutzfolgenabschätzung.

Prozess Datenschutzfolgenabschätzung

Link zum Datenschutzprozess Datenschutzfolgenabschätzung

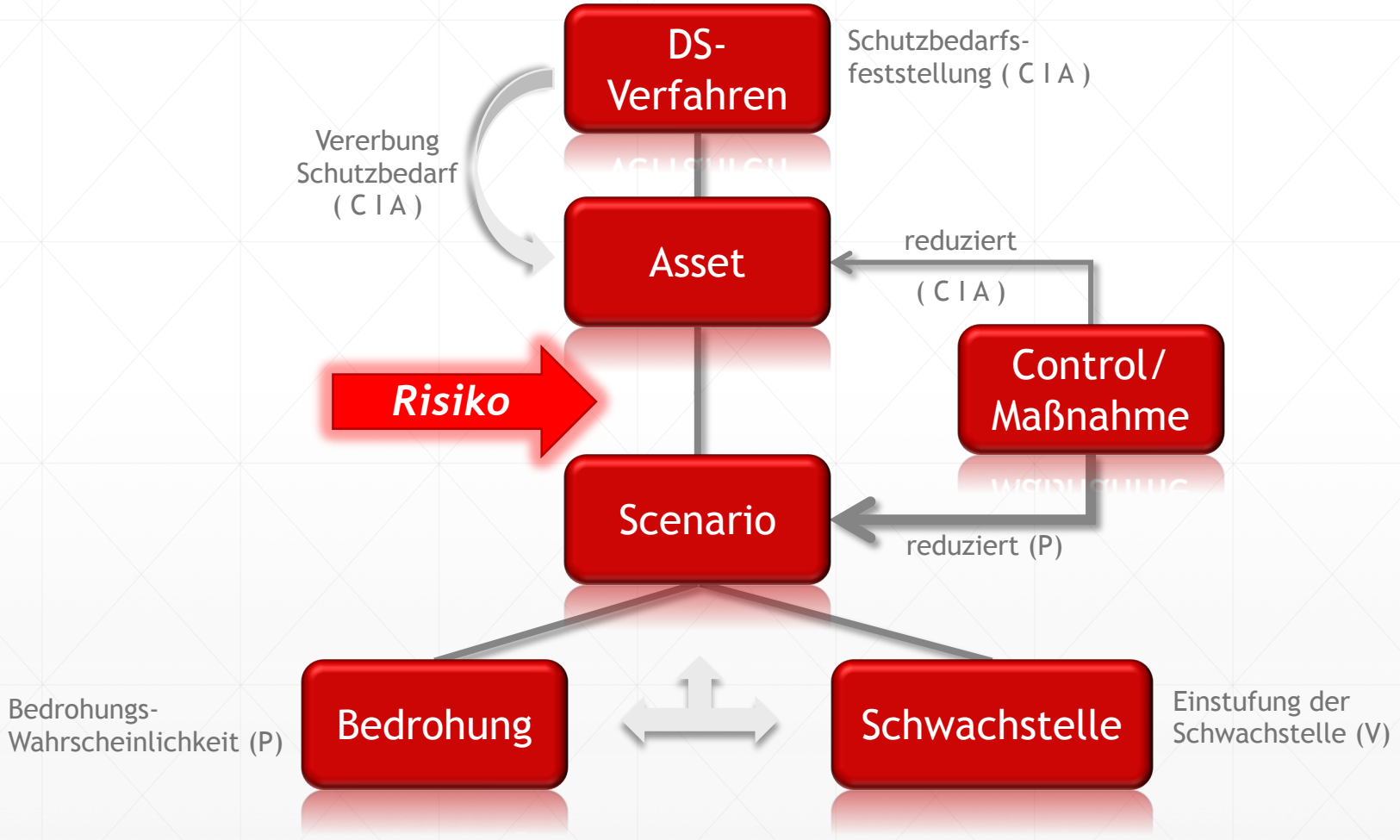
Bestandteile des DSFA/Risikomanagement-Prozesses in verinice

1. Festlegung des Kontext
2. Risikoassessment
   - Risikoidentifikation
   - Risikoanalyse
   - Risikobewertung
3. Risikobehandlung
4. Risikoakzeptanz
5. Risikokommunikation
6. Risikoüberwachung

Bestandteile des Risikoassessment

- Risikoidentifikation
  - Identifikation der Prozesse und Assets
  - Identifikation von Bedrohungen
  - Identifikation von Schwachstellen
  - Identifikation von Schadensauswirkungen
  - Identifikation bereits umgesetzter Maßnahmen
- Risikoanalyse
- Risikobewertung

Risikomanagementprozess in verinice



Festlegung der Wertebereiche (Klassifizierung)

Bedrohungswahrscheinlichkeit (P):

Wert	verinice 1.13	*weitere Varianten …*	
0	Selten	*Unwahrscheinlich*	*Normal*
1	Jährlich	*Möglich*	*Hoch*
2	Monatlich	*Wahrscheinlich*	*Sehr hoch*
3	Wöchentlich	*Sehr wahrscheinlich*	
4	Täglich		
5	Stündlich		

Wahrscheinlichkeit das die Bedrohung auftritt, in klarem Zeitraster oder pauschalisiert.

Schwachstelle (V):

Wert	verinice 1.13	*weitere Varianten …*	
0	Sehr niedrig	*Sehr komplex*	*Normal*
1	Niedrig	*Komplex*	*Hoch*
2	Hoch	*Möglich*	*Sehr hoch*
3	Sehr hoch	*Einfach*	
4		*Sehr einfach*	

Einstufung der Schachstelle
Wie groß ist das Schadenspotential der Schwachstelle?
Wie leicht ist sie Ausnutzbar?

Wert des Asset (Business Impact)

Wert	Vertraulichkeit (C)	Integrität (I)	Verfügbarkeit (A)
0	Öffentlich	Keine	Basis
1	Externer Gebrauch	Normal	Normal
2	Interner Gebrauch	Hoch	Hoch
3	Vertraulich		Sehr hoch
4			Außergewöhnlich

Der Wert des Asset vererbt sich üblicherweise aus dem Business Impact (Schutzbedarf) der vom Asset abhängigen Prozesse.

Risikoberechnung (ISO 27005)

Scenario

Bedrohungs-wahrscheinlichkeit:	0 normal			1 hoch			2 sehr hoch		
Einstufung der Schwachstelle:	0 normal	1 hoch	2 sehr hoch	0 normal	1 hoch	2 sehr hoch	0 normal	1 hoch	2 sehr hoch
Wert des Asset 0	0	1	2	1	2	3	2	3	4
Wert des Asset 1	1	2	3	2	3	4	3	4	5
Wert des Asset 2	2	3	4	3	4	5	4	5	6
Wert des Asset 3	3	4	5	4	5	6	5	6	7

Risikowert = Bedrohungswahrscheinlichkeit + Einstufung der Schwachstelle + Wert des Asset

Risikobeurteilung

Wahrscheinlichkeit \ Schwachstelle	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

< 4	Risikoakzeptanz
4-5	Risikotoleranz
> 5	Risikobehandlung

Risikobehandlungsmethoden

Modifizieren

Das Risikoniveau sollte soweit reduziert werden, dass das Restrisiko als akzeptabel eingestuft werden kann.

Vermeiden

Wenn identifizierte Risiken als zu hoch eingestuft werden oder die Kosten für die Durchführung anderer Risikobehandlungsmethoden den Nutzen übersteigen, kann das Risiko vollständig vermieden werden indem die Aktivität eingestellt wird.

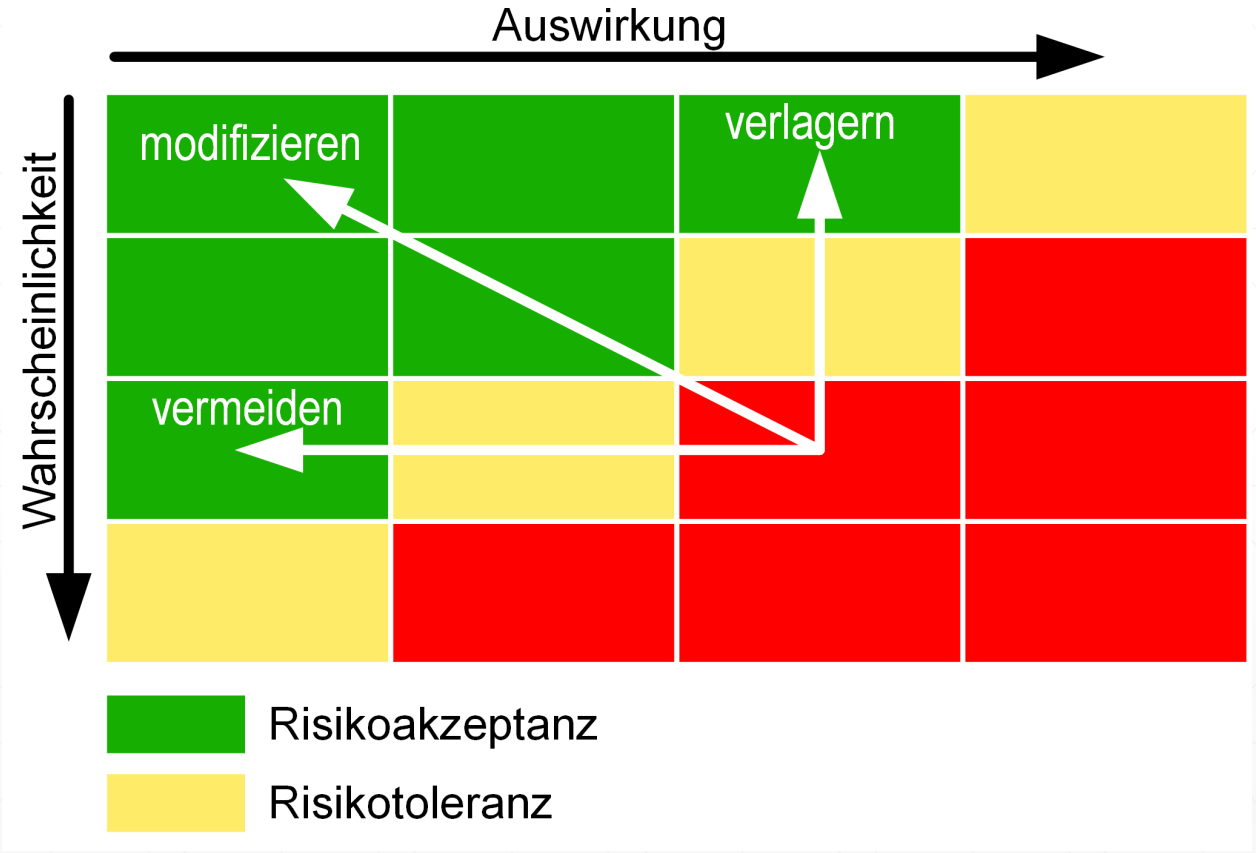
Verlagern

Das Risiko kann an Dritte übertragen werden. Das geschieht durch Versicherung von möglichen Folgen oder durch die Übertragung an einen Partner, der die Überwachung des Informationssystems sicherstellt und entsprechende Maßnahmen ergreift.

Zurückbehalten

Die Entscheidung, Risiken zu akzeptieren und die Verantwortung zu übernehmen wurde ausdrücklich vom Asset-Eigentümer dokumentiert. (siehe ISO 27001 Ch. 4.2.1 h).

Risikobehandlungsmethoden



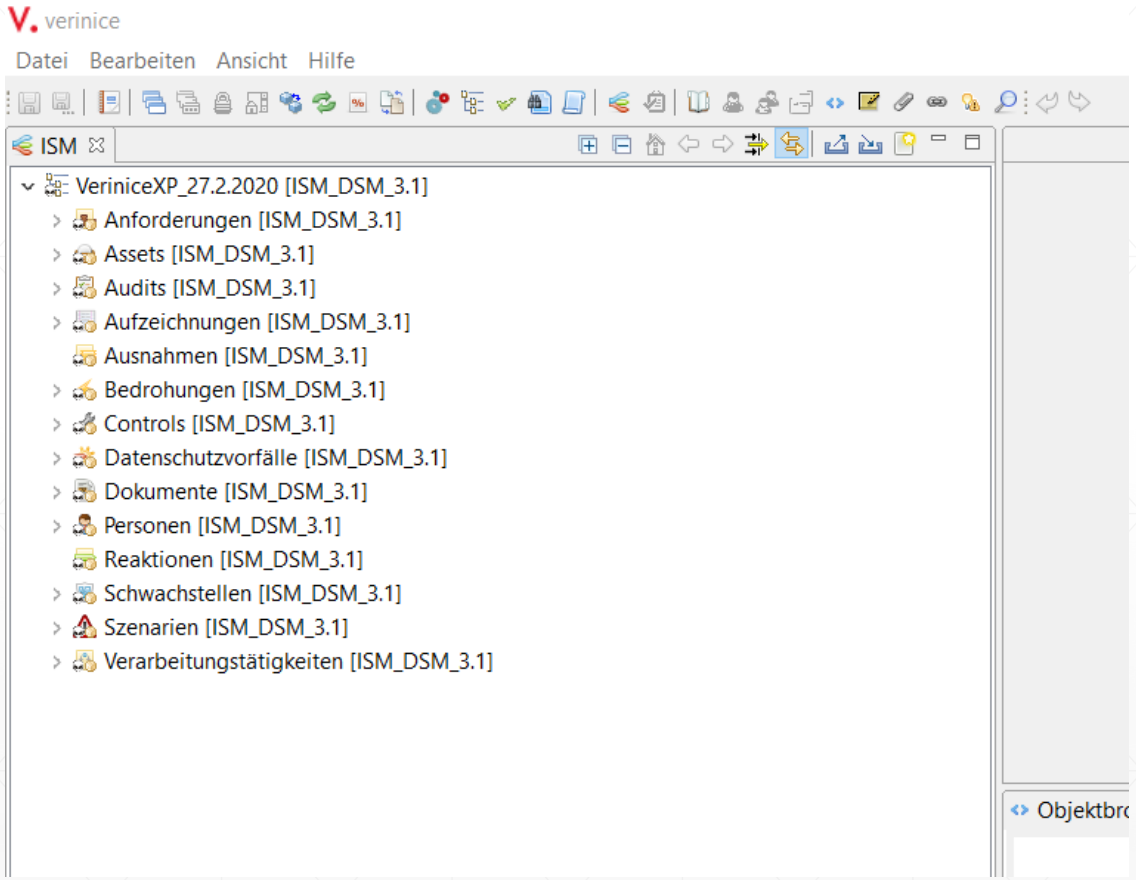
verinice Datenschutzmodul 3.1

Erhältlich in Shop.

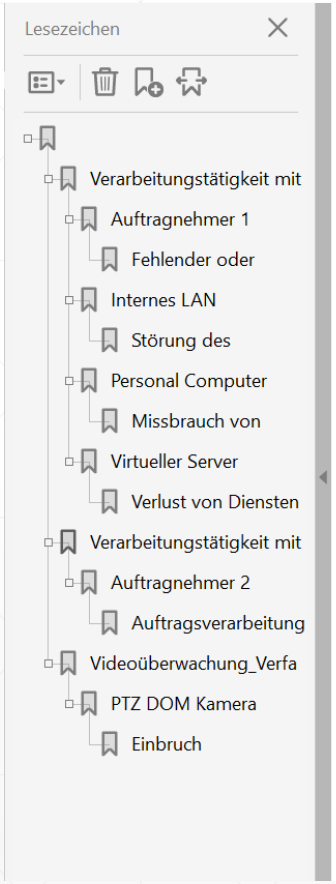
Inhalt:

- ~ Bericht Datenschutz-Folgenabschätzung
- ~ Bericht IT-Grundschutz-Check mit Datenschutzzielen
- ~ Bericht Risikobehandlung – Datenschutz
- ~ Bericht Risikobewertung – Datenschutz
- ~ Übersichtsreports DSGVO
- ~ Verzeichnis von Verarbeitungstätigkeiten DSGVO sowie MoGS

Kurze LIVE-Präsentation/Vorstellung Verinice Datenschutzmodul - DSM 3.1



Reporting - Risikobeurteilung

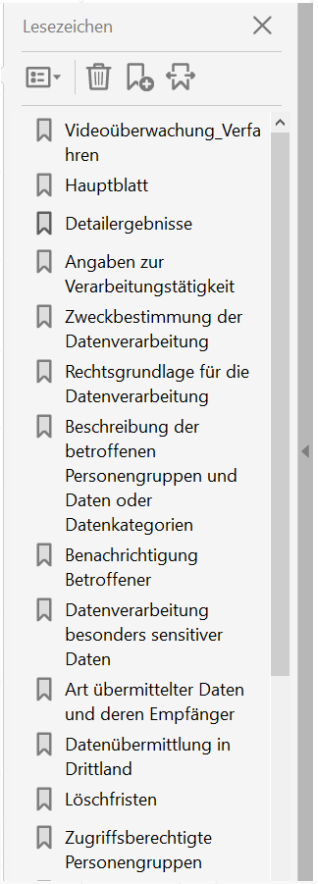


	Drittstaaten ohne adäquates Datenschutzniveau	0: Sehr niedrig	0	0	0	0

Abk.	Name	Vertraulichkeit	Integrität	Verfügbarkeit
VÜ	**Videoüberwachung_Verfahren**	**2**	**1**	**1**
		8	**7**	**7**	**22**

Assets und Risikoszenarien			Risiko			Gesamtrisiko
Abk.	Name	Typ	Vertraulichkeit	Integrität	Verfügbarkeit	
PTZ DOM Kamera	PTZ DOM Kamera		2	1	1	
	Einbruch	4: Täglich				
	Zu niedriger Zaun	3: Sehr hoch	8	7	7	22
	Straftäter	4: Täglich				

Reporting - Datenschutzfolgenabschätzung

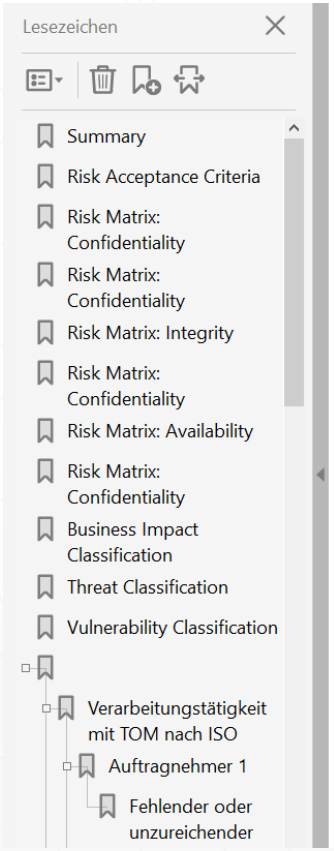


I. Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke

1. Angaben zur Verarbeitungstätigkeit	
Übergeordneter Geschäftsprozess / Verfahren Videoüberwachung_Verfahren	Bezeichnung der Verarbeitung / Verfahrensbeschreibung Diese Folgenabschätzung bezieht sich auf die Videoüberwachungsanlage der MUSTER GmbH am Standort Berlin.
Art der Verarbeitung Ersterhebung	
Auftragsverarbeitung i.S.d. Art. 30 II DS-GVO	Nein

2. Zweckbestimmung der Datenverarbeitung
Festgelegte Zwecke der Videoüberwachung § 4 Abs. 1 Nr. 3 BDSG(neu) 2018 - (DSAnpUG-EU) Personenbezogene Daten werden bei der MUSTER GmbH für festgelegte, eindeutige und legitime Zwecke erhoben und werden nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet („Zweckbindung"). Zusätzlich werden bei der MUSTER GmbH personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt („Datenminimierung"). Digitale Videoüberwachung ohne Tondaten des Einganges samt Zutrittsbereich des Verwaltungsgebäudes der MUSTER GmbH zum Zweck des Eigentumsschutzes und des Verantwortungsschutzes, der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens mit ausschließlicher Auswertung in dem durch den Zweck definierten

Reporting - Risikobehandlung



Abk.	Name	Vertraulichkeit	Integrit?t	Verf?gbarkeit	Totel Risk Figure
VÜ	Videoüberwachung_Verfahren	2	1	1	
		3	2	2	**7**

Assets			Risk			
Abbr.	**Name**	**Type**	**Confidentiality**	**Integrity**	**Availability**	
PTZ DOM Kamera	PTZ DOM Kamera	Physisch	3	2	2	**7**

Controls affecting asset	Implementiert	Effectiveness			
Scenario	Probability				
Einbruch	4: T?glich 2: Hoch	8	7	7	
Zu niedriger Zaun	3: Sehr hoch				
Straftäter	4: T?glich				
Controls affecting scenario	Implemented	Effectiveness			
Zaunfelder erhöhen	Ja	5			
Residual Risk		3	2	2	**7**

Treatment of residual risk* Modifizieren

Explanation:

*if above acceptance criteria

Beispiele für die Durchführung einer DSFA nicht-öffentlicher Bereich:

1. Datenverarbeitung mit Sozial, Berufs- oder bes. Amtsgeheimnis
   Bspw. Insolvenzverzeichnis, soziale Einrichtungen, Anwaltssozietät
2. Verarbeitung pbD über Aufenthalt natürlicher Personen
   Bspw. Car Sharing, Fahrzeugdaten, Offline-Tracking Kundenbewegungen, Verkehrsstromanalyse
3. Zusammenführung pbD aus versch. Quellen und Weiterverarbeitung
   Bspw. Fraud-Prevention-Systeme, Scoring durch Auskunfteien, Banken, Versicherungen
4. Mobile optisch-elektronische Erfassung pbD im öffentl. Bereich
   Bspw. Fahrzeugdatenverarbeitung
5. Bewertung des Verhaltens von Personen
   Bspw. Bewertungsportale, Inkassodienstleistungen Forderungsmgmgt sowie Factoring
6. Bewertung des Verhaltens von Beschäftigten
   Bspw. Data-Loss-Prevention-Systeme, Geolokalisierung

Beispiele für die Durchführung einer DSFA nicht-öffentlicher Bereich:

7. Erstellung umfassender Profile über Interessen, pers. Beziehungen oder Persönlichkeit
   Bspw. Dating- und Kontaktportale
8. Zusammenführung pbD aus versch. Quellen und Weiterverarbeitung
   Bspw. Big-Data-Analyse von Kundendaten mit Angaben aus Drittquellen
9. Einsatz von KI zur Verarbeitung pbD
   Bspw. Kundensupport mittels KI
10. Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgerätes
    Bspw. Offline-Tracking, Verkehrsstromanalyse
11. Automatisierte Auswertung von Video oder Audio Aufnahmen
    Bspw. Telefongespräch mittels Algorithmen
12. Erhebung pbD mittels elektronischer Geräte
    Bspw. RFID/NFC durch Apps oder Karten

Beispiele für die Durchführung einer DSFA nicht-öffentlicher sowie Öffentlicher Bereich:

13. Anonymisierung von bes. Kat. pbD
    Bspw. pbD nach Art. 9 DSGVO
14. pbD nach Art. 9
    Bspw. Telemedizin-Lösungen zur Bearbeitung von Krankheitsdaten sowie Speicherung der Messdaten von Sensoren, Fitnessarmbänder oder verbaut in Smartphones

DSFA im Öffentlichen Bereich:

- Verarbeitung pbD in Kinder- und Jugendhilfe
- Jobcenter
- Melderegister
- Personenstandsregister
- Personalausweis- und Passanträge
- Beantragung von Sozialhilfe
- Amtliche Statistik
- Schülerdaten, Lernplattform

Zusammenfassung

Verfahren zur Erkennung von relevanten Störfällen und zur Risikobeurteilung einrichten

- Beurteilung der Risikostufe (gering, mittel, hoch)
- Verfahren zur Risikobehandlung im Sicherheitsmanagement einrichten

Datenklassifizierung und Risikobeurteilung

- Klassifizierung der Daten nach ihrer Sensibilität
- Risikoklassifizierung der Verarbeitungen nach geringem, mittlerem und hohem Risiko (in der Dokumentation der Verarbeitungsverfahren)

Datenschutzfolgenabschätzung (Art. 35 DSGVO)

- Durchführung bei hohem Risiko für die Rechte und Freiheiten der Betroffenen
- Einrichtung von Maßnahmen zur Risikoreduzierung
- Vorherige Konsultation der Aufsichtsbehörde bei fortbestehendem hohen Risiko (Art. 36 DSGVO)

Vielen Dank!

verinice.PARTNERS

<Sicherheitsberatung
Robert Raczynski>
<KuDamm 195>
<D-10707 Berlin>

Telefon <+49 30 220 661 420>
FAX <+49 30 220 661 429>
Mail <myforensic@posteo.de>
Web <www.myforensic.de>
<www.mytutor.berlin>
<www.mysecurity.world>