Der Landesbeauftragte für den

DATENSCHUTZ und die INFORMATIONSFREIHEIT

Rheinland-Pfalz

Aktuell – Vorabkontrolle § 9 Abs. 5 LDSG

Soweit Verfahren **automatisierter** Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle).

Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1.besondere Arten personenbezogener Daten (§ 3 Abs. 9 LDSG) verarbeitet werden

Art der Daten

oder

2.die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit der Betroffenen zu bewerten (z.B. Kreditwürdigkeit) einschließlich ihrer Fähigkeiten, ihrer Leistung oder ihres Verhaltens,

Zweckbestimmung

es sei denn, dass ……..

In Zweifelsfällen soll der LfDI konsultiert werden, die wesentlichen Erwägungen dokumentieren.

Künftig – Datenschutz-Folgenabschätzung Art. 35, 36 DS-GVO

Art. 35 Abs. 1: Wahrscheinlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen, sog. Schwellwertanalyse

- Recht auf Schutz personenbezogener Daten (Art. 8 GRCh)
- Recht auf Achtung des Privat- und Familienlebens (Art. 7 GRCh)
- Recht auf Meinungs- und Informationsfreiheit (Art. 11 GRCh)
- Gedanken-, Gewissens- und Religionsfreiheit (Art. 10 GRCh)
- Recht auf Nichtdiskriminierung (Art. 21 GRCh)

Risiko für die Rechte und Freiheiten natürlicher Personen

Art. 24 Abs. 1 – Verantwortung des für die Verarbeitung Verantwortlichen

Art. 32 Abs. 1 – Sicherheit der Verarbeitung

Art. 39 Abs. 2 – Aufgaben des Datenschutzbeauftragten

Art. 32 Abs. 1

Diese Risikobewertung muss grundsätzlich erfolgen.

Auch ein niedriges Risiko kann Eindämmungsmaßnahmen notwendig machen.

Erst ein hohes Risiko führt zu einer DSFA.

Instrument zur Bewertung von Risiken

Die DSFA stellt ein Instrument dar, welches es ermöglicht, Risiken zu erkennen und systematisch zu bewerten, die bei **der Verarbeitung** von personenbezogenen Daten insbesondere durch den Einsatz von neuen Technologien auftreten können. Sie soll es ermöglichen, Strategien und Maßnahmen zu entwickeln, die geeignet sind, diese Risiken zu minimieren.

ErwGr 84
Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere eines Risikos evaluiert werden

ErwGr 90
Risiko - Produkt aus Eintrittswahrscheinlichkeit und Schadensschwere für substanzielle Freiheitsrechte – Prognose
Droht ein hoher Schaden, genügt eine geringe Eintrittswahrscheinlichkeit und umgekehrt.

Regelfälle

Art. 35 Abs. 3 lit. a-c benennt typische risikogeneigte Verarbeitungstätigkeiten, bei denen ein hohes Risiko ohne weiteres unterstellt wird.

Die Art. 29 Datenschutzgruppe hat Fälle zur Frage veröffentlicht, wann eine Daten-Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen i.S.v. Art. 35 Abs. 1 S. 1 DS-GVO darstellt (vgl. Leitlinien wp 248 der Artikel-29-Datenschutzgruppe unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236).

- Datenverarbeitung zur Bewertung, zum Scoring oder zum Profiling, insbesondere in den Bereichen Arbeit, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben und Interessen, Bonität, Verhaltensweisen, Aufenthaltsort (z. B. Bewertung der Kreditwürdigkeit durch Wirtschaftsauskunfteien, Angebote von Krankenkassen für Vorzugstarife nach einer erweiterten Gesundheitsprüfung, Erfassung von Daten durch Partnervermittlungsportale)

Es werden auch rechtliche Aussagen getroffen.
vgl. auch ErwGr. 71, 75, 76

- Formen automatisierter Entscheidungsfindung mit weitreichenden rechtlichen oder persönlichen Folgen (z. B. die automatisierte Ablehnung eines Online-Vertragsabschlusses, nicht jedoch z. B. personalisierte Werbung)

- systematisches Monitoring in Netzwerken und systematische Überwachung von öffentlich zugänglichen Bereichen (z. B. eine Überwachung der Internetnutzung, Verkehrsüberwachung, die Videoüberwachung von Bahnhöfen und Flughäfen)

  Als Zweck kommt auch eine Verhaltenskontrolle in Betracht.

- Verarbeitung sensibler Daten (z. B. Gesundheitsdaten oder Daten über Straftaten und strafrechtliche Verurteilungen),

- umfangreiche Verarbeitungsvorgänge (sowohl im Hinblick auf die Anzahl der Betroffenen als auch im Hinblick auf die Menge der erhobenen Daten und die Verarbeitungsintensität, die Dauer der Verarbeitung, das geographische Ausmaß; z. B. eine Mailingliste eines überregionalen Onlinemagazins)

- Verarbeitung von zusammengeführten oder kombinierten Datensätzen aus Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden (aus verschiedenen Verarbeitungsvorgängen bei verschiedenen Verantwortlichen, z. B. Social-Media-Portal, Rasterfahndung)

- Verarbeitung von Daten schutzbedürftiger Personen wie Kindern, älteren Menschen, Patienten oder Mitarbeitern (z. B. in Schulen oder Kindertagesstätten)

- Nutzung neuer Technologien wie Smart Car, Smart Health, Smart Metering, Big Data, Tracking-, Sicherheits- und Überwachungstechnik, Internet-of-Things, Gesichtserkennung, Fingerabdruck-Scanner

- die Verarbeitung kann dazu führen, dass ein Betroffener ein Recht nicht ausüben oder einen Vertrag nicht schließen kann (z. B. Prüfung auf Kreditwürdigkeit).

Nach den Richtlinien ist von einem hohen Risiko auszugehen, wenn mindestens zwei der vorgenannten Kriterien erfüllt sind. In diesen Fällen wäre eine DSFA durchzuführen.

Beispiele

Dokumentenmanagementsystem:

- Sensible Daten im Sinne von Art. 9 DS-GVO
- Umfangreiche Verarbeitung

Krankenhausinformationssystem:

- Schutzbedürftige Personen
- Sensible Daten im Sinne von Art. 9 DS-GVO
- Umfangreiche Verarbeitung

Listen gemäß Art. 35 Abs. 4 und 5 DS-GVO

Außerdem erstellt die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge, für die eine DSFA durchzuführen ist (Art. 35 Abs. 4 DS-GVO).

Sog. „Muss“-Liste

Die „Muss“-Liste ersetzt die Risikoabschätzung nach Art. 35 Abs. 3

Die sog. „Muss-Nicht“-Liste nach Art. 35 Abs. 5 ist optional.

Fraglich ist, ob eine solche Liste erstellt wird, weil sich Verfahren bzw. Verarbeitungsvorgänge verändern können.

Art. 35 Abs. 10 DS-GVO – Ausnahme von der Pflicht zur DSFA

… und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, ……

ErwGr. 92

Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder ……

§ 9 Abs. 1 LDSG-E

Eine DSFA kann unterbleiben, wenn z.B. das fachlich zuständige Ministerium eine solche für den Verarbeitungsvorgang bereits durchgeführt hat.

Art. 35 Abs. 7 beschreibt die Mindestinhalte einer DSFA

DSFA vor erstmaliger Durchführung der Verarbeitungstätigkeit

Mehrere Phasen :

- Vorbereitungsphase: Beschreibung der Verarbeitungsvorgänge von Erhebung bis Löschung; Identifikation der Akteure, betroffenen Personen und Rechtsgrundlagen

- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge, milderes Mittel ? (rechtliche Prüfung?

- Identifikation möglicher Angreifer, Angriffsmotive und –ziele sowie Bewertung der Risiken für die Rechte und Freiheiten

- Beschreibung von Abhilfemaßnahmen

Aus der Bewertung ergibt sich das Abwägungsmaterial für die Antwort auf die Frage, ob und unter welchen Bedingungen eine Verarbeitung zulässig ist.

Mögliche Risikobereiche bzw. Gewährleistungsziele

- Datensparsamkeit
  (Datenumfang & Datenminimierung)
- Transparenz
  (Dokumentation & Nachvollziehbarkeit)
- Nichtverkettbarkeit
  (Berechtigungskonzept & Zweckbindung)
- Intervenierbarkeit
  (Betroffenenrechte & Löschung)
- Verfügbarkeit
- Integrität
- Vertraulichkeit

Welche Folgen ergeben sich durch die vorgesehene Verarbeitung dafür?

Mögliche Ursachen für ein Risiko hinsichtlich eines Gewährleistungszieles

- Keine Lösch- oder Sperrfrist festgelegt – Datensparsamkeit
- Kein Rollen-/Berechtigungskonzept – Transparenz
- Unzureichende Einschränkung von Verarbeitungsrechten – Nichtverkettbarkeit
- Keine Protokollierung zur Nachvollziehbarkeit der Verarbeitung – Transparenz
- Fehlende Prozesse für die Wahrnehmung der Betroffenenrechte - Intervenierbarkeit

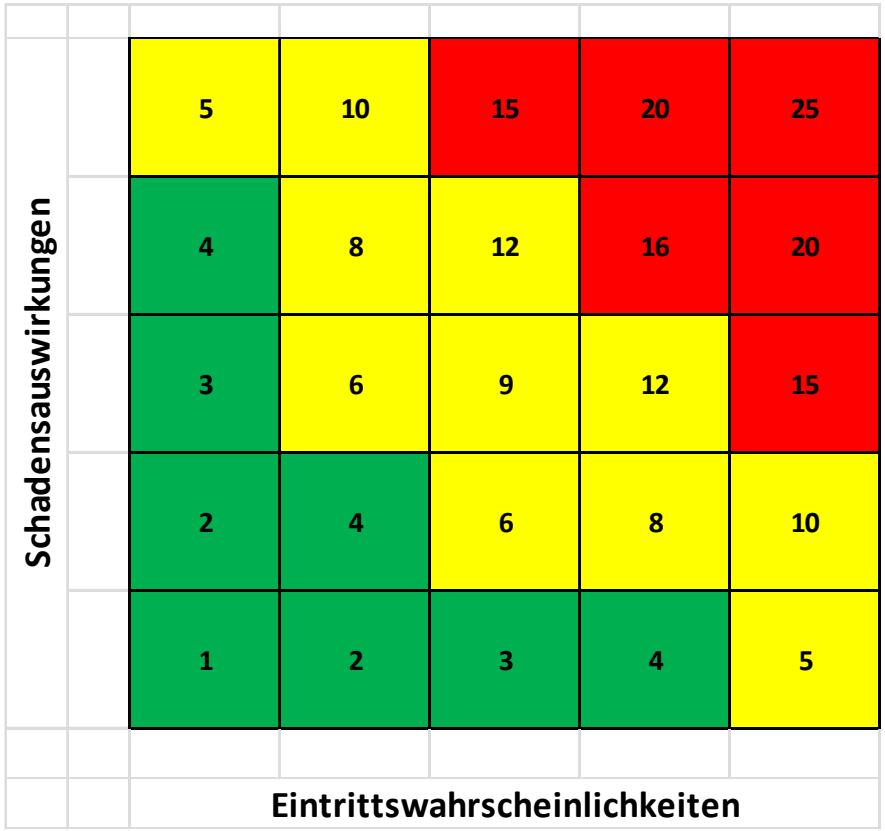
Beschreibung der Eintrittswahrscheinlichkeiten

Eintrittswahrscheinlichkeit	Beschreibung
1 = sehr selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle 10 Jahre eintreten
2 = selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle 5 Jahre eintreten
3 = mittel	Ereignis tritt einmal alle 5 Jahre bis einmal im Jahr ein
4 = häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein
5 = sehr häufig	Ereignis tritt mehrmals im Monat ein

Beschreibung der Schadensauswirkungen

Schadensauswirkung	Beschreibung
1 = vernachlässigbar	Die Schadensauswirkungen sind sehr gering und können vernachlässigt werden.
2 = zeitlich und räumlich begrenzt	Die Schadensauswirkungen sind gering sowie zeitlich und räumlich begrenzt
3 = zeitlich oder räumlich begrenzt	Die Schadensauswirkungen sind gering sowie zeitlich oder räumlich begrenzt
4 = beträchtlich	Die Schadensauswirkungen sind beträchtlich
5 = existenzbedrohend	Die Schadensauswirkungen sind existenzbedrohend

Matrix



Risiko - Produkt aus Eintrittswahrscheinlichkeit und Schadensschwere

Welche Methodik kann angewendet werden? vgl. das wp 248 der Art. 29 Gruppe

Beispiele für EU-weite allgemeine Rahmenbestimmungen:

- DE: Standard-Datenschutzmodell, V.1.0 – Erprobungsfassung, 2016[31].
  https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V_1_1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Auswahlermessen für den Verantwortlichen

Beispiel: elektronisches Schließsystem unter Verwendung von Transponderchips

Risikobeschreibung und -analyse

Nr.	Eindeutige Bezeichnung des Risikos	Betrachtetes Zielobjekt im Informationsverbund	Art des Zielobjekts gem. DSM	Beschreibung des Risikos und der möglichen Folgen	Ausprägung des Risikos gem. Art. 35 DS-GVO	Betroffene Gewährleistungsziele des SDM	Eintritts-wahrschein-lichkeit	Schadens-auswirkung	Risiko	Gegen-maßnahmen (GM)	Eintritts-wahrschein-lichkeit nach GM	Schadensaus-wirkung nach GM	Risiko nach GM
1	Ausfall der Stromversorgung, der Netzwerkanbindung oder der Hardware des Applikationsservers	Applikationsserver	System	Im Falle des Ausfalls der Stromversorgung, der Netzwerkanbindung oder der Hardware des Applikationsservers wäre ein Zugriff auf die Anwendung und somit auf die Datenbank nicht mehr möglich. Eine Sachbearbeitung könnte nicht erfolgen (z. B. Vergabe von Zutrittsrechten oder Korrekturen an Zeitkonten). Buchungen an den ZE-Terminals würden gepuffert, ZK-Terminals würden noch funktionieren.	Umstände	Verfügbarkeit	3	2	6	Absicherung durch USV, SLA's für Hardware (Server und Netzwerk) mit definierten Reaktionszeiten	2	2	4
2	Ausfall der Stromversorgung, der Netzwerkanbindung oder der Hardware des Datenbankservers	Datenbankserver	System	Im Falle des Ausfalls der Stromversorgung, der Netzwerkanbindung oder der Hardware des Datenbankservers wäre ein Zugriff auf die Anwendung und somit auf die Datenbank nicht mehr möglich. Eine Sachbearbeitung könnte nicht erfolgen (z. B. Vergabe von Zutrittsrechten oder Korrekturen an Zeitkonten). Buchungen an den ZE-Terminals würden gepuffert, ZK-Terminals würden noch funktionieren.	Umstände	Verfügbarkeit	3	2	6	Absicherung durch USV, SLA's für Hardware (Server und Netzwerk) mit definierten Reaktionszeiten	2	2	4
3	Ausfall der Stromversorgung, der Netzwerkanbindung oder der Hardware des Webservers	Webserver	System, Prozesse	Über einen Webserver wird im Intranet eine Portalseite bereitgestellt. An dieser Seite können sich die Bediensteten mit ihrem Transpondercode und einem Passwort anmelden und dort ihre Zeitkonten einsehen und Buchungen vornehmen. Telearbeiter nutzen diese Möglichkeit regelmäßig. Im Falle des Ausfalls der Stromversorgung, der Netzwerkanbindung oder der Hardware des Webservers könnten diese dann nicht mehr ihre Arbeitszeiten im Home Office erfassen. Alle Mitarbeiter könnten nicht mehr auf ihre Zeitkonten zugreifen.	Umstände	Verfügbarkeit, Transparenz	3	1	3	keine GM erforderlich (vgl. Risiko). Ggf. können die Telearbeiter ihre Arbeitszeiten notieren und über einen Korrekturbeleg nachbuchen lassen.	1	3	3
5	Ausfall der Stromversorgung oder der Netzwerkanbindung eines oder mehrerer ZE-Terminals, Defekt eines ZE-Terminals	Zeiterfassungsterminal	System	Im Fall des Ausfalls der Stromversorgung oder der Netzwerkanbindung eines oder mehrerer ZE-Terminals oder bei einem Defekt eines ZE-Terminals können an diesem Terminal keine Buchungen oder Abfragen mehr vorgenommen werden.	Umstände	Verfügbarkeit, Transparenz	2	2	4	keine GM erforderlich (vgl. Risiko). Ggf. können die Mitarbeiter ein anderes Terminal nutzen oder über das Portal ihre Buchung vornehmen oder ihre Arbeitszeiten notieren und über einen Korrekturbeleg nachbuchen lassen. Die Terminals selbst sind sehr robust und wenig fehleranfällig.	2	2	4
6	Ausfall der Stromversorgung oder der Netzwerkanbindung eines oder mehrerer ZK-Terminals, Defekt eines ZK-Terminals	Zutrittskontrollterminal	System	Im Fall des Ausfalls der Stromversorgung oder der Netzwerkanbindung eines oder mehrerer ZK-Terminals oder bei einem Defekt eines ZK-Terminals können an diesem Terminal keine Buchungen mehr vorgenommen werden. Der Zugang zu den durch die betroffenen ZK-Terminals kontrollierten Bereiche ist ggf. nicht mehr möglich.	Umstände	Verfügbarkeit	2	3	6	redundante Stromversorgung, ggf. USV für ZK-Terminals, Abschluss einer Servicevertrags für ZK-Terminals	2	2	4
7	Zugriffe durch Unbefugte auf die Datenbank	Datenbank	Daten, System	Es könnten sich unbefugte Personen Zugriff auf das System und/oder die Datenbank verschaffen und lesenden und/oder schreibenden Zugriff auf die Daten nehmen. Dies könnte durch Angreifer innerhalb oder außerhalb der Organisation erfolgen. So könnten innerhalb der Organisation die Zugangsdaten von Berechtigten kompromittiert und aus verschiedenen Motiven missbräuchlich genutzt werden. Für den Fall, dass das System über das Internet erreichbar ist, könnte der Angriff auch durch Externe erfolgen (z.B. SQL-Injection). Es könnten Auswertungen zu unzulässigen Zwecken erfolgen.	Art, Zweck	Verfügbarkeit, Vertraulichkeit, Integrität, Nichtverkettbarkeit	2	4	8	regelmäßige Auswertung der Zugriffshistorie im 4-Augen-Prinzip nach vorgegebenen Regeln, Passwortrichtlinie, organisatorische Regelungen zum Umgang mit Zugangsdaten, Durchführung eines Penetrationstests, ggf. Segmentierung des Systems im Netzwerk	1	3	3
8	Fehlerhafte Bearbeitung durch Befugte	Datenbank	Daten	Befugte Personen könnten aus verschiedenen Motiven absichtlich oder unabsichtlich eine fehlerhafte oder unzulässige Bearbeitung vornehmen. Dies könnte z. B. aus Unkenntnis der rechtlichen Rahmenbedingungen, auf Grund fehlender Kenntnisse der Software oder aus Unachtsamkeit erfolgen.	Art, Zweck	Verfügbarkeit, Vertraulichkeit, Integrität	2	4	8	regelmäßige Auswertung der Zugriffshistorie im 4-Augen-Prinzip nach vorgegebenen Regeln, Schulung der befugten Personen im Umgang mit der Software, Schulung im Hinblick auf die Zulässigkeit und Zwecke der Datenverarbeitung	1	3	3
9	Unzulässige Auswertungen der Datenbank durch Befugte	Datenbank	Daten, Prozesse	Befugte Personen könnten aus verschiedenen Motiven absichtlich oder unabsichtlich unzulässige Auswertungen vornehmen. Dies könnte z. B. aus Unkenntnis der rechtlichen Rahmenbedingungen, aber auch vorsätzlich erfolgen.	Art, Zweck, Umfang	Nichtverkettbarkeit	2	4	8	regelmäßige Auswertung der Zugriffshistorie im 4-Augen-Prinzip nach vorgegebenen Regeln, klare Regeln im Hinblick auf die zulässigen Auswertungen der Daten, Sensibilisierung und Schulung der Anwender im Hinblick auf die Zulässigkeit und Zwecke der Datenverarbeitung	1	3	3
10	Nutzung eines Transponderchips mit umfassenden Zugangsberechtigungen durch Unbefugte	Transponderchip	Daten, System	Im Falle des Verlusts oder Diebstahls eines Transponderchips könnte dieser durch Unbefugte genutzt werden. Für den Fall, dass dieser Chip den Zutritt zu kritischen Unternehmensbereichen ermöglicht (z. B. Archiv mit Personalakten oder Server- oder Technikraum) bestehen beträchtliche Gefährdungen	Umstände, Zweck, Umfang	Verfügbarkeit, Vertraulichkeit, Integrität, Nichtverkettbarkeit	3	5	15	restriktive Vergabe von Zugangsberechtigungen und regelmäßige Überprüfung, organisatorische Regelungen im Falle des Verlusts eines Transponderchips treffen und bekannt machen, Möglichkeit der zeitnahen Löschung des verlorenen Transponderchips sicherstellen, Mitarbeiter im Umgang mit dem Transponderchip sensibilisieren	2	2	4

Eindeutige Bezeichnung des Risikos	Betrachtetes Zielobjekt im Informationsverbund	Art des Zielobjekts gem. DSM	Beschreibung des Risikos und der möglichen Folgen	Ausprägung des Risikos gem. Art. 35 DS-GVO	Betroffene Gewährleistungsziele des SDM	Eintrittswahrscheinlichkeit	Schadensauswirkung	Risiko	Gegenmaßnahmen (GM)	Eintrittswahrscheinlichkeit nach GM	Schadensauswirkung nach GM	Risiko nach GM
Nutzung eines Transponderchips mit umfassenden Zugangsberechtigungen durch Unbefugte	Transponderchip	Daten, System	Im Falle des Verlusts oder Diebstahls eines Transponderchips könnte dieser durch Unbefugte genutzt werden. Für den Fall, dass dieser Chip den Zutritt zu kritischen Unternehmensbereichen ermöglicht (z. B. Archiv mit Personalakten oder Server- oder Technikraum) bestehen beträchtliche Gefährdungen	Umstände, Zweck, Umfang	Verfügbarkeit, Vertraulichkeit, Integrität Nichtverkettbarkeit	3	5	15	organisatorische Regelungen bei Verlust eines Chips treffen, zeitnahe Löschung des verlorenen Chips, im Umgang mit dem Chip sensibilisieren	2	2	4

Beispiel: Videoüberwachung mit Netzwerk-Kameras

Ursache für Risiko	Unverschlüsselte drahtlose Übertragung zum Server
Risiko	Zugriff auf Daten von unberechtigten Dritten
Betroffenes Gewährleistungsziel	Vertraulichkeit
Eintrittswahrscheinlichkeit	Videoüberwachung 24 h
Schadensauswirkung	unberechtigte Dritte greifen Daten ab

Hohes Risiko

Eindämmungsmaßnahmen	Verschlüsselung der drahtlosen Übertragung
Schadensauswirkung	wird herabgesetzt

Geringes Risiko

Potentielle Abhilfe- und Eindämmungsmaßnahmen

Art. 36 Konsultation der Aufsichtsbehörde

wenn z.B.

- eine erfolgreiche Eindämmungsmaßnahme zu teuer wäre
- eine Anonymisierung mit dem Forschungsdesign nicht in Einklang gebracht werden kann
- ……

Art. 58 Abs. 3 lit. a – die Aufsichtsbehörde berät den Verantwortlichen

Aufsichtsbehörde „findet“ keine Eindämmungsmaßnahme und kommt zu einem negativen Ergebnis – rechtsmittelfähige Entscheidung

Vgl. noch Leitlinie wp 248 der Art. 29 Datenschutzgruppe

Die DSFA ist kein abgeschlossener Prozess

Nach einer durchgeführten DSFA ist es nach einer gewissen Zeit erforderlich, die Maßnahmen zur Risikoeindämmung im Hinblick auf deren Wirksamkeit zu überprüfen und ggf. anzupassen.

Für fortlaufende Überwachung bietet sich ein Datenschutz-Managementsystem an.

Diesem Gedanken folgend sollten auch bereits eingeführte Bestandsverfahren regelmäßig überprüft werden, ob die im Rahmen einer durchgeführten Vorabkontrolle eingeführten technisch-organisatorischen Sicherungsmaßnahmen noch aktuell sind und dem Stand der Technik entsprechen.

Kernpunkte der Leitlinien wp 248 – Bestehende Verarbeitungen

- Eine DSFA ist für bestehende Datenverarbeitungen dann nicht durchzuführen, wenn diese einer Vorabkontrolle unterzogen wurden und sich keine wesentlichen Änderungen ergeben haben (III.C).

- Eine DSFA ist für bestehende Datenverarbeitungen durchzuführen, wenn sich seit der Vorabkontrolle Änderungen ergeben haben, die voraussichtlich mit einen hohen Risiko verbunden sind (III.C).

- Bestehende Verarbeitungen ggf. im Hinblick auf die neuen Schutzziele prüfen.

- Eine DSFA sollte regelmäßig überprüft bzw. evaluiert werden (III.C), auch im Falle von Art. 35 Abs. 10.

Landesdatenschutzgesetz–E neu

Teil 2
§ 9 Datenschutz-Folgenabschätzung

Vereinfachung des Verfahrens bzw. Ermessen bei der Durchführung

Teil 3
§56 Durchführung einer Datenschutz-Folgenabschätzung

Voraussetzungen zur Durchführung

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Michael Smolle

Referent

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

Postanschrift:	Postfach 30 40 55020 Mainz
Büroanschrift:	Hintere Bleiche 34 55116 Mainz
Telefon:	+49 (6131) 208-2449
Telefax:	+49 (6131) 208-2497
E-Mail:	poststelle@datenschutz.rlp.de
Web:	www.datenschutz.rlp.de