Geschäftsbereich
Recht, Zentrale Dienste

Nr. 11/2018

Newsletter Datenschutz

In dieser Ausgabe: Risikobewertung und Datenschutz-Folgeabschätzung

Vorbemerkung

Jedes Unternehmen musste schon immer dokumentieren, wie es welche Daten verarbeitet. Diese Dokumentation erfolgte über das Verfahrensverzeichnis. Mit Geltung der DSGVO wurde aus dem Verfahrensverzeichnis ein Verarbeitungsverzeichnis. Mit der Erstellung des Verzeichnisses kann und muss jeder Unternehmer nachweisen, dass er den Datenschutz bei der Verarbeitung der bei ihm anfallenden personenbezogenen Daten einhält. Einzelheiten, was alles in das Verarbeitungsverzeichnis gehört, gibt Ihnen unser Newsletter Datenschutz 10/2018. Spätestens bei der Errichtung des Verarbeitungsverzeichnisses muss sich jeder Unternehmer Gedanken darum machen, ob die personenbezogenen Daten, die in seinem Unternehmen anfallen und verarbeitet werden, auch rechts- und IT-sicher verarbeitet werden. Auf der Basis des Verarbeitungsverzeichnisses kann sich jeder Unternehmer selbst Gewissheit verschaffen, ob er alles nötige veranlasst hat, um die bei ihm verarbeiteten Daten IT-sicher zu nutzen und letztendlich auch zu speichern. Das bedeutet: Er muss sich Gedanken darüber machen, ob die bei ihm vorhandene IT-Absicherung ausreicht, um das Datenschutzniveau der DSGVO halten zu können.

Die Datenschutz-Grundverordnung (DSGVO) vertritt einen **risikobasierten Ansatz** für die Verarbeitung von personenbezogenen Daten. Dies bedeutet: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die DSGVO an den Verarbeitungsvorgang. Umso mehr Vorkehrungen muss auch der Unternehmer als verantwortliche Stelle dann treffen. Immer dann, wenn eine **Datenverarbeitung für die Rechte und Freiheiten einer Person ein hohes oder ein sehr hohes Risiko zur Folge hat**, hat der Unternehmer vor deren Einführung eine sog. **Datenschutz-Folgenabschätzung (DSFA) vorzunehmen.** Es muss ermittelt werden, welche Folgen eine geplante Verarbeitung für den Schutz der Daten Betroffener hätte. Wie eine solche Ermittlung durchzuführen ist, zeigen wir Ihnen anhand eines Praxisbeispiels am Ende unseres Newsletters.

Stellt sich heraus, dass eine Datenverarbeitung ein (sehr) hohes Risiko für die Rechte und Freiheiten einer Person bedeutet, müssen angemessene technische und/oder organisatorische Maßnahmen ergriffen werden, um das Risiko zu reduzieren. Gelingt dies nicht, ist für den Einsatz der Anwendung vorab eine Genehmigung der zuständigen Datenschutzaufsichtsbehörde einzuholen.

Die DSFA ist **regelmäßig** - mindestens jährlich - zu **überprüfen** und anzupassen, wenn neue Risiken hinzukommen, bereits behandelte Risiken geändert oder wesentlich erschwert werden.

Für mehrere ähnliche Verarbeitungsvorgänge reicht eine DSFA, sofern diese ein ähnlich hohes Risiko haben.

Wann ist eine Datenschutz-Folgeabschätzung erforderlich?

Eine Datenschutz-Folgeabschätzung ist notwendig, wenn ein **hohes** oder ein **sehr hohes Risiko für die Rechte und Freiheiten einer Person** besteht. Nach Erwägungsgrund 75 besteht unter anderen ein (sehr) hohes Risiko, wenn

- die Verarbeitung personenbezogener Daten, zu einem physischen, materiellen oder immateriellen Schaden führen könnte (z.B. Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verlust, Rufschädigung oder Verlust der Vertraulichkeit);
- sensible Daten, z.B. über die rassische oder ethnische Herkunft, die Zugehörigkeit zu einer Gewerkschaft, genetische Daten oder Gesundheitsdaten, verarbeitet werden,
- ein Profiling stattfindet oder
- die Verarbeitung eine große Anzahl von personenbezogenen Daten oder Personen betrifft.

In Art. 35 Abs. 3 DSGVO sind Fälle genannt, wann eine **DSFA** insbesondere **notwendig** ist:

- bei der systematischen und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- bei der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder
- bei der systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Ein Fall der systematischen Überwachung öffentlich zugänglicher Bereiche liegt insbesondere bei einer **Videoüberwachung** vor.

Die Datenschutzbehörden der Länder haben eine **Blacklist** erstellt, die auflistet **bei welchen Verarbeitungsvorgängen eine Datenschutz-Folgenabschätzung erforderlich** ist:
https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/ds-folgenabschaetzung/DSFA_Muss-Liste_DSK_1_0.pdf

Zu dem Thema **Risiko für die Rechte und Freiheiten natürlicher Personen** hält die Datenschutzkonferenz (DSK) ein **Kurzpapier** bereit:
https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/kurzpapiere/KP_18_Risiko.pdf

Die DSFA ist **vor dem Beginn des Verarbeitungsvorgangs** durchzuführen. Bei Verarbeitungsvorgängen, die bereits bestehen und bei denen sich herausstellt, dass eine DSFA notwendig ist, sollte diese rechtzeitig auf den Weg gebracht werden.

Wie prüfe ich, ob ich eine Datenschutz-Folgenabschätzung durchführen muss?

Ergibt sich aus der **Blacklist** nicht, dass eine Datenschutz-Folgeabschätzung durchzuführen ist oder ist eine der Alternativen nach **Art. 35 Abs. 3 DSGVO** nicht einschlägig, ist eine **eigene Risikobewertung** vorzunehmen:

1. Zunächst ist für das geplante Vorhaben ein **Verzeichnis von Verarbeitungstätigkeiten** zu erstellen. Ein Muster dafür finden Sie hier: https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/kurzpapiere/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf
2. Für die Datenverarbeitung ist sodann eine **systematische Risikobewertung** (sog. „Schwellenwertanalyse“) vorzunehmen. Das Ergebnis dieser Bewertung ist zu dokumentieren. Liegt kein (sehr) hohes Risiko vor, ist dies ebenfalls zu dokumentieren. In diesem Fall bedarf es keiner DSFA.

   Für die Risikobewertung gibt es keine einheitliche, gesetzlich vorgeschriebene Methode. Daher sollte eine Risikobestimmung nach einem gängigen Verfahren (Best Practice: CNIL, ISO) erfolgen wie z. B. nach dem Standard-Datenschutzmodell oder dem Muster einer Datenschutzaufsicht.
3. Bei der Risikobewertung muss zunächst der **Schutzbedarf** der zu verarbeitenden personenbezogenen Daten festgestellt werden (= Risikoidentifikation). Welche Daten geschützt werden müssen, ergibt sich aus dem Verfahrensverzeichnis. Zu ermitteln ist, **welche Schäden** und **wodurch** diese Schäden eintreten können. Zu berücksichtigen ist hier die Risiko-Quelle, also das Ereignis bzw. der Umstand, der zum Schadenseintritt führen könnte. Die Schutzbedarfsfeststellung kann folgendermaßen aussehen (3-stufig):

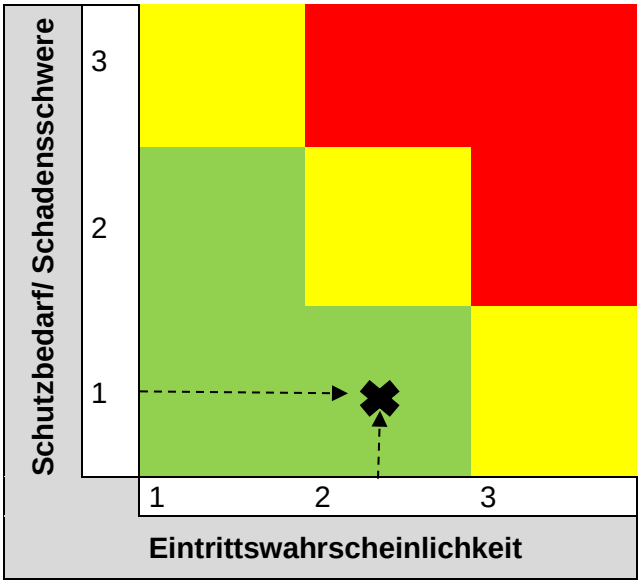
Schutzbedarfskategorien - Schadensschwere

Schutzbedarf	Klasse	Beeinträchtigung des Persönlichkeitsrechts	Beispiele
Normal (Gering oder mittel)	1	Wäre für Betroffene als tolerabel einzustufen. Ein möglicher Datenmissbrauch hätte nur geringfügige Auswirkungen (wirtschaftlich/gesellschaftspolitisch) für Betroffene. • Nicht zur Veröffentlichung bestimmte Daten • Geringfügige Schäden bei Veröffentlichung/Verfälschung	Gering: Anschrift, Kontaktdaten Mittel: Daten über Geschäfts- und Vertragsbeziehungen, Kontostände, Personaldaten (soweit nicht Stufe 2), Kreditauskünfte
hoch	2	Wäre für Betroffene als erheblich einzustufen. Ein möglicher Datenmissbrauch hätte erhebliche Auswirkungen (wirtschaftlich/gesellschaftspolitisch, ggf. Beeinträchtigung der persönlichen Unversehrtheit) für Betroffene/ Hohe Folgeschäden bei Veröffentlichung/ Verfälschung.	Steuerdaten, Daten, die einem Berufs-, Geschäfts-oder Fernmeldegeheimnis unterliegen; sensible Personaldaten (z.B. berufliche Laufbahn, Angaben über Behinderung, etc.)

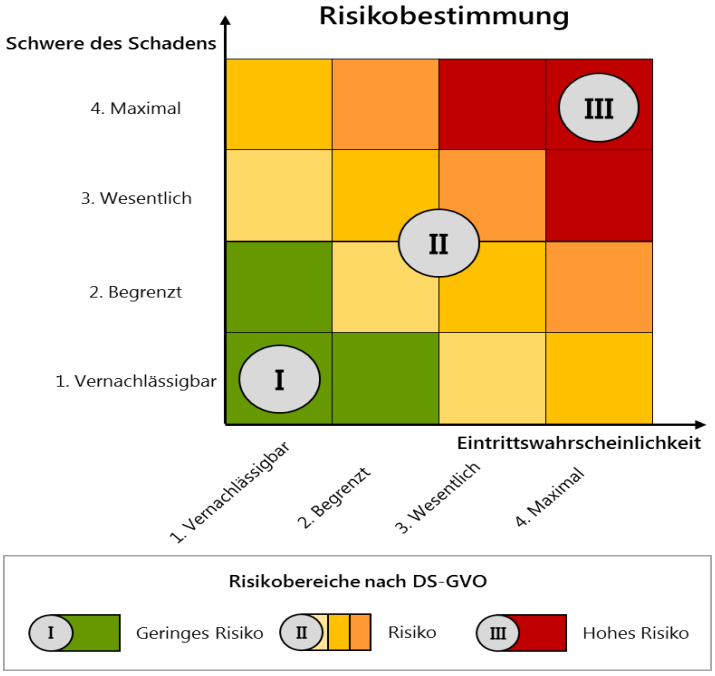
sehr hoch	3	Wäre für Betroffene als besonders bedeutsam und als nicht tolerabel einzustufen. Ein möglicher Datenmissbrauch bedeutet für Betroffene wirtschaftlichen/gesellschaftspolitischen Ruin oder beeinträchtigt die persönliche Unversehrtheit gravierend. Veröffentlichung/Verfälschung verletzt Persönlichkeitsrechte, verursacht Schaden an Leib und Leben oder dem Ansehen.	Hochsensible Daten wie etwa Aussagen zur sexuellen Orientierung, Gesundheitsdaten, etc.

4. Nachdem der Schutzbedarf festgestellt wurde, sind die **Eintrittswahrscheinlichkeit** und die **Schwere des Schadens** zu ermitteln.

Das Ergebnis ist in einer Risiko-Matrix darzustellen. Diese kann so:



oder so aussehen:



Quelle: BayLDA

5. **Ergibt** die **Risikoanalyse** ein **(sehr) hohes Risiko**, sind Maßnahmen zu ergreifen, die das Risiko minimieren - damit beginnt die **Datenschutz-Folgeabschätzung.**

6. Kann das Risiko nicht minimiert werden, ist die Aufsichtsbehörde zu konsultieren.

Bestellung eines Datenschutzbeauftragten

Ist eine Datenschutz-Folgeabschätzung notwendig, ist ein Datenschutzbeauftragter zu bestellen - unabhängig von der Anzahl der Beschäftigten. Dieser ist bei der DSFA miteinzubeziehen. Er unterstützt und berät den Verantwortlichen bei der Durchführung.

➔**D06** „Betrieblicher Datenschutzbeauftragter nach der DSGVO und dem BDSG, **Kennzahl 2158** unter www.saarland.ihk.de.

Wie sieht die Datenschutzfolgeabschätzung aus?

Die DSFA muss mindestens folgende Punkte enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge
2. eine Beschreibung der Zwecke der Verarbeitung und eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen;
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.

a) Systematische Beschreibung der Verarbeitungsvorgänge

Der Verarbeitungsvorgang muss genauer beschrieben werden. Insbesondere die Prozessschritte und die eingesetzten Informationssysteme sollten dargestellt werden. Dies kann z.B. folgendermaßen aussehen:

Beispiel: Kundenverwaltung

Verarbeitungsschritt	**Beschreibung**	**eingesetzte Informationssysteme**	**sonstige Faktoren**
Erhebung der Daten	Kunde meldet sich für die Erstellung eines Angebotes. Die Kundendaten werden in einem Formular von dem Sachbearbeiter erfasst.	E-Mail-Programm, Telefon, Desktop-PC, Fileserver	Erfasst durch Mitarbeiter/ Sachbearbeiter

Verarbeitung der Daten	Daten werden in einem Programm erfasst, mit dem das Angebot erstellt wird.	E-Mail-Programm, Telefon, Desktop-PC, Fakturierungssoftware, Fileserver	Verarbeitung durch Mitarbeiter/ Sachbearbeiter Ausdruck des Angebots
Übermittlung der Daten	Angebot wird an Kunden übermittelt per Post/per Mail. Übermittlung der Daten an Finanzbuchhaltung.	E-Mail-Programm, Telefon, Desktop-PC, Fakturierungssoftware, Fileserver	Übermittlung per Postweg an Kunden Übermittlung an Finanzbuchhaltung
Aufbewahrung der Daten	Daten werden in Papierform in Ordnern und auf dem PC aufbewahrt. Aufbewahrungszeitraum: 10 Jahre	E-Mail-Programm, Telefon, Desktop-PC, Fakturierungssoftware, Fileserver	Abschließbare Schränke, Berechtigungssystem
Löschung der Daten	Datenträger werden vernichtet, Löschung auf PCs.	Desktop-PC, Fakturierungssoftware, Fileserver	Aktenvernichter/ Datenträgervernichter

b) Beschreibung der Zwecke und Bewertung der Verhältnismäßigkeit

Die **Zwecke** ergeben sich bereits aus dem **Verfahrensverzeichnis**. Daher sollte darauf zurückgegriffen werden. Darüber hinaus ist eine **Bewertung der Notwendigkeit** und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck vorzunehmen. Zu fragen ist, ob die Verarbeitung erforderlich ist oder ob es ein milderes, gleich effektives Mittel gibt, das weniger stark in die Rechte und Freiheiten der Betroffenen eingreift.

c) Bewertung der Risiken

Der Verantwortliche **muss beschreiben**, **welche Datenschutzrisiken** den Betroffenen bei der Verletzung der Datenschutzprinzipien drohen. Folgende Datenschutzprinzipien können durch die Verarbeitung betroffen sein:

- Rechtmäßigkeit der Verarbeitung: Existiert eine Grundlage für die Datenverarbeitung? Vertrag, Einwilligung, Verpflichtung, berechtigte Interessen?
- Transparenz: Wurde über die Datenverarbeitung informiert?
- Zweckbindung: Für welchen Zweck wird die Verarbeitung genutzt? Besteht ein Risiko, dass die Verarbeitung für andere Zwecke verwendet wird?
- Datenminimierung: Werden nur die notwendigen Daten verarbeitet? Besteht ein Risiko, dass auch andere Daten verwendet werden?
- Datenrichtigkeit: Sind die Daten richtig? Gibt es einen Prozess für die Berichtigung von Fehlern?
- Speicherbegrenzung: Wann werden die Daten gelöscht (Löschkonzept)? Existiert ein Prozess für die Löschung?

- Integrität und Vertraulichkeit: Existieren Sicherheitsmaßnahmen zum Schutz vor Kenntnisnahme durch Unbefugte?
- Verfügbarkeit: Sind die Daten dauerhaft verfügbar und wieder herstellbar im Falle eines Verlustes?
- Rechenschaftspflicht: Werden die Prinzipen eingehalten? Existiert eine Dokumentation?

Risikoquellen können z.B. unbeabsichtigtes oder beabsichtigtes Fehlverhalten von Mitarbeitern, Wasserschäden, Feuer, Stromausfall, Ausfall der Internet-Leitung, Verarbeitungen durch Auftragsverarbeiter, Cyberkriminelle etc. sein. Als Risiken kommen wirtschaftliche Nachteile, Rufschädigung, Geheimnisoffenbarung, etc. in Betracht (s. oben)

Das Ergebnis dieser Risikobewertung muss dokumentiert werden.

d) Abhilfemaßnahmen

Der Verantwortliche muss **beschreiben**, **welche Maßnahmen** er ergreifen wird, um eine Verletzung der Datenschutzprinzipien zu vermeiden.

Was ist nach Erstellung der Datenschutz-Folgeabschätzung zu beachten?

Mit dem Erstellen der Datenschutz-Folgeabschätzung endet die Arbeit nicht. Die Abhilfemaßnahmen sind umzusetzen und auf ihre Wirksamkeit zu testen.

Die **DSFA** ist **kein einmaliger Vorgang**, sondern ein ständig zu betrachtender und überprüfender **Prozess**. Ergeben sich neue Risiken oder ändern sich bereits erkannte Risiken, so ist die DSFA zu überprüfen und ebenso anzupassen. Zu diesem Zweck sollte ein Prozess implementiert werden, um eine regelmäßige Kontrolle zu gewährleisten.

Die Datenschutz-Folgeabschätzung sollte in einem **Bericht** zusammengefasst werden. Dort sollte auch dokumentiert werden, ob die Abhilfemaßnahmen zu einer Reduzierung der Risiken geführt hat.

Können die Risiken durch die Abhilfemaßnahmen nicht reduziert werden, ist die **Aufsichtsbehörde** vor Einführung des Verarbeitungsvorgangs zu **konsultieren**.

Der DSFA-Bericht ist der Aufsichtsbehörde zur Verfügung zu stellen.

Veranstaltungen

„Die neue FinVermV in 90 Minuten“
Donnerstag, 17. Januar 2019, Raum 1, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Referent: Rechtsanwalt Dr. Martin Andreas Duncker, Fachanwalt für Bank- und Kapitalmarktrecht, Zertifizierter Compliance-Beauftragter (IHK), Compliance-Officer (TÜV), Schlatter Rechtsanwälte Steuerberater PartG mbB, Heidelberg

Anmeldungen **bis 16. Januar 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

„Das Direktionsrecht des Arbeitgebers“
Dienstag, 5. Februar 2019, 18.00 - 20.00 Uhr, Raum 1-3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Referent: Herr RA Eric Schulien - Eric Schulien GmbH Rechtsanwaltsgesellschaft, Saarbrücken

Anmeldungen **bis 4. Februar 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

„180 Tage DSGVO - wo stehen wir“
Montag, 11. Februar 2019, 15.00 – 17.00 Uhr, Raum 1-3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Referent: Stefan Staub, Geschäftsführer der Verimax GmbH

Anmeldungen **bis 8. Februar 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

„Arbeitszeitflexibilisierung im Rahmen der neuen Gesetzgebung“
Donnerstag, 28. März 2019, 18.00 - 20.00 Uhr, Raum 1, Saalbau, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Referent: Rechtsanwalt Frank Gust, Training und Beratung im Arbeitsrecht.

Anmeldungen **bis 27. März 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

„1 Jahr DSGVO“
Donnerstag, 23. Mai 2019, 18.00 - 20.00 Uhr, Raum 1-3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Referenten: Herr RA Hubert Beeck und Frau RAin Jennifer Hohmann, Homburg

Anmeldungen **bis 22. Mai 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

Verantwortlich und Redaktion:

Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de
IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß
Tel.: (0681) 9520-600
Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines
Tel.: (0681) 9520-640
Fax: (0681) 9520-690
E-Mail: kim.pleines@saarland.ihk.de

Impressum:
IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dipl.-Volkswirt Dr. Heino Klingen, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, UST.- Ident.- Nummer: DE 138117020