GDPRism

Vorlage:
Prüfung Drittanbieter

Diese Vorlage unterstützt bei der datenschutzrechtlichen Risikobewertung eines Drittanbieters bzw. Dienstleisters.

Wichtig: Dieses Merkblatt stellt keine Rechtsberatung dar. Die Inhalte haben keinen Anspruch auf Vollständigkeit und sind ohne Gewähr. Sie dienen lediglich als Einstieg und geben einen ersten Überblick über die datenschutzrechtlichen Bestimmungen.

Angaben zum Dienstleister

Um welchen Service, Internetdienst oder Dienstleister handelt es sich?

Wo hat der Dienstleister seinen Sitz? (Bitte Adresse eingeben)

Teil I. Prüfung des Risikos

Einsatzzweck

Wofür soll der Service, Internetdienst oder Dienstleister eingesetzt werden? Was ist der Anwendungsfall bzw. der Einsatzzweck der Dienstleistung?

Risikoeinschätzung Betrieb

Wie hoch stufen Sie das Risiko des Einsatzes des Anbieters ein? Bewerten Sie hierzu die Auswirkungen auf den eigenen Betrieb, sollte der Dienst oder Service ausfallen und nicht mehr zur Verfügung stehen.

Niedriges Risiko	**Mittleres Risiko**	**Hohes Risiko**
Die Nichtverfügbarkeit der Software stellt für den Betrieb kein nennenswertes Risiko dar. Ein Ausfall der Anwendung hat keine nachhaltigen Auswirkungen	Die Anwendung ist für den Geschäftsbetrieb wichtig. Ein Ausfall könnte den Betrieb zwar kurzfristig behindern oder negativ beeinflussen, jedoch ohne nachhaltige Auswirkungen.	Ein Ausfall des Systems hätte extreme Auswirkungen auf den Geschäftsbetrieb. Das System ist wichtig für die Aufrechterhaltung wichtiger Funktionen. Ein Ausfall würde zu direkten Kosten führen.

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden

GDPRism

Schwellwertanalyse – Möglicher Schaden für die betroffenen Personen

Beim Risikomanagement hat ein Risiko grundsätzlich zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Bewerten Sie das mögliche Risiko anhand der untenstehenden Tabelle.

Schwere des Schadens				
Maximal				
Wesentlich				
Begrenzt		X		
Vernachlässigbar				
	Vernachlässigbar	Begrenzt	Wesentlich	Maximal
	Eintrittswahrscheinlichkeit			

Schwere des Schadens:

- **Vernachlässigbar:** Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
- **Begrenzt**: Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.
- **Wesentlich**: Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.
- **Maximal**: Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

Eintrittswahrscheinlichkeit:

- **Vernachlässigbar:** Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.
- **Begrenzt**: Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.
- **Wesentlich**: Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich.
- **Maximal**: Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.

Quelle:
Dokument „Risikoanalyse und Datenschutz- Folgenabschätzung“ des bayerischen Landesbeaufragten für den Datenschutz

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden

GDPRism

Teil II. Anbietercheck

Zugriff durch den Anbieter

Um was für einen Dienst handelt es sich? Handelt es sich um eine Software, die lokal installiert wird oder über eine Internetanwendung?

Im Falle einer Internetanwendung: Besteht für den Anbieter Fernzugriff des Anwenders im Wartungsfall?

ja	**nein**	**unklar**

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden

Prüfung Drittlandbezug

Werden personenbezogene Daten in ein Drittland übertragen, so muss das entsprechende Zielland identifiziert und überprüft werden. Dies kann anhand der folgenden Länderkategorien erfolgen:

- **Länder ohne nennenswerte Risiken:** Länder der EU sowie alle Länder für die seitens der EU ein Angemessenheitsbeschluss verabschiedet wurde (u.a. Norwegen, Liechtenstein, Island, Andorra, Argentinien, Färöer Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Kanada, Neuseeland, Schweiz, Uruguay, UK, USA)
- **Risikobehaftete Länder:** Länder, die nicht in der Liste der Länder ohne nennenswerte Risiken aufgelistet sind.
- **Kritische Länder:** Kritische Länder sind u.a. China, Indien sowie Länder ohne rechtsstaatliche Strukturen.

Wo hat der Dienstleister seinen Sitz?

Länder ohne nennenswerte Risiken	**Risikobehaftete Länder**	**Kritische Länder**

Gibt es eine Muttergesellschaft und wenn ja, wo hat diese ihren Sitz?

Länder ohne nennenswerte Risiken	**Risikobehaftete Länder**	**Kritische Länder**

Setzt der Dienstleister ggf. Subunternehmer mit Sitz in einer der Länderklassen ein?

Länder ohne nennenswerte Risiken	**Risikobehaftete Länder**	**Kritische Länder**

In welchem Land findet die Datenverarbeitung statt?

Länder ohne nennenswerte Risiken	**Risikobehaftete Länder**	**Kritische Länder**

Prüfung vertraglicher Pflichten

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden

Informiert der Anbieter umfänglich über seine datenschutzrechtlichen wie IT-sicherheitsrelevanten Aktivitäten?

ja	**nein**	**unklar**

Bietet der Anbieter eine AV-Vertrag an? Nur relevant wenn es sich um eine klassische Auftragsverarbeitung handelt.

ja	**nein**	**unklar**

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden

GDPRism

Teil III. Abschließende Beurteilung

Risikoeinordnung

Notieren Sie, wie oft Sie im vorliegenden Fragebogen Antwortmöglichkeiten der entsprechenden Farbe ausgewählt haben:

Sollten Sie **ROT** markierte Felder ausgewählt haben, sollten Sie vor Einsatz des Dienstleisters dringend datenschutzrechtlichen Rat einholen.

Sollten Sie **ORANGE** markierte Felder ausgewählt haben, sollten Sie den Einsatz des Dienstleisters im Detail prüfen. Die markierten Bereiche sollten nochmals geprüft und ggf. mit dem Dienstleister direkt geklärt werden. Der Einsatz des Dienstleisters ist zumindest risikobehaftet. Eventuell ist die Durchführung einer gesonderten Risikobewertung oder weiterführende Prüfungen notwendig.

Alle **GRÜN** markierten Felder stehen für „normale“ Risiken. Das bedeutet nicht, dass der Einsatz des Dienstleisters absolut risikofrei ist. Für die Nutzung der Dienstleistung müssen Sie als Verantwortlicher trotzdem entsprechend technische und organisatorische Maßnahmen treffen, um die datenschutzrechtliche Verarbeitung der Daten zu gewährleisten.

Fazit / Maßnahmen

Führen Sie gemäß den vorliegenden Informationen eine abschließende Beurteilung durch. Beschreiben Sie, welche Maßnahmen Sie planen, um eventuell identifizierte Risiken zu minimieren oder weiter im Detail zu prüfen.

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden