Kurz und knapp erklärt:

Risikobewertung

[Anforderung] Was sagt das Gesetz?

Die DSGVO fordert einen den Risiken entsprechenden Schutz von personenbezogenen Daten:

> ***Artikel 32 Absatz 1:***
>
> *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; […]*
>
> ***Artikel 35 Absatz 1:***
>
> *„Hat 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“*

[Maßnahmen] Was ist zu tun?

Unter folgenden Prämissen ist das Risiko für die Betroffenen (nicht das Risiko des Unternehmens) zu bewerten:

» Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
[qualitative Bewertung]

» Eintrittswahrscheinlichkeit und Schwere des Risikos durch die Datenverarbeitung
[quantitative Bewertung]

Zu den o. g. Prüfkriterien liefert das Verzeichnis von Verarbeitungstätigkeiten eine gute Informationsbasis.

Hinweis: Beachte auch One Pager „Verfahrensverzeichnis“.

[Nutzen] Was bringt mir das?

Dieser gesetzliche Aufwand hat auch wesentliche Vorteile für das durchführende Unternehmen:

» Erhöhung des Schutzniveaus und Verbesserung der „Resilienz“ der Unternehmens-IT

» Budget-Optimierung in der IT, da keine „überzogenen“ (in der Regel kostspieligen) Sicherheitsmaßnahmen ergriffen werden

» Erhöhung der Akzeptanz von Sicherheitsmaßnahmen bei den Usern durch Angemessenheit

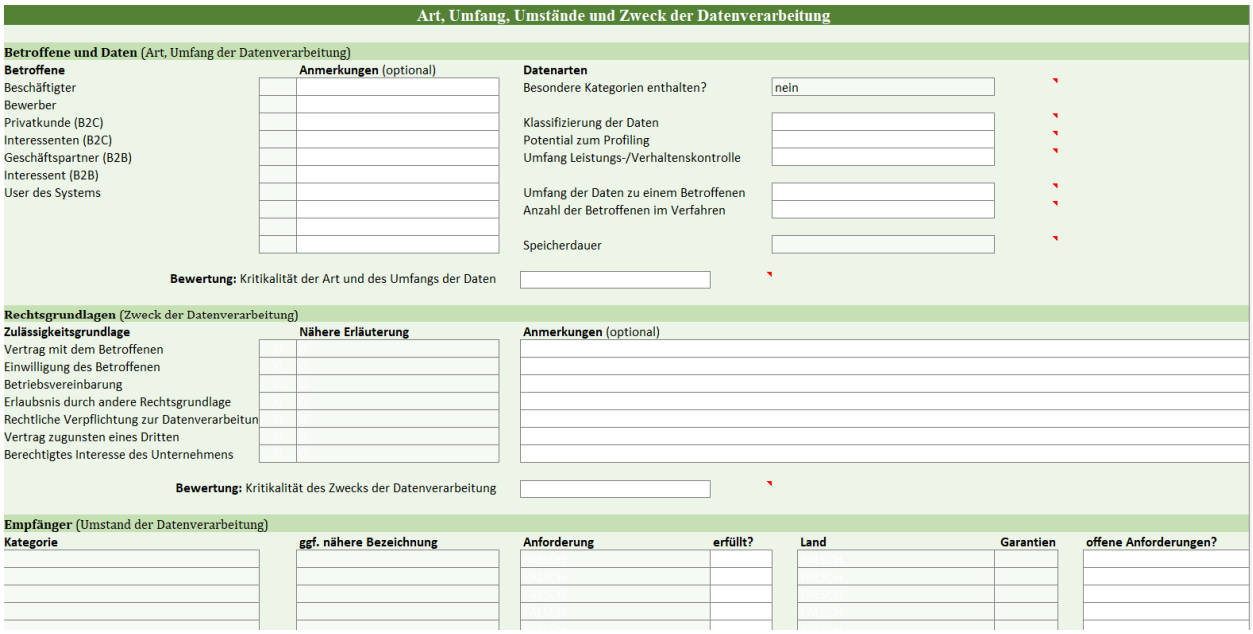
[UIMC] Wie hilft die UIMC?

Die UIMC hat ein pragmatisches Verfahren etabliert, eine Risikobewertung effizient und lösungsorientiert durchzuführen. Hierbei kommen Datenschutz-Berater mit langjähriger Erfahrung zum Einsatz.

[Anlage] Beispiel eines Bewertungsschemas

Wenn mindestens ein Kritikalitätswert hoch/rot ist, dann ist eine Datenschutz-Folgenabschätzung erforderlich (siehe One Pager „Datenschutz-Folgenabschätzung“)

Qualitative Bewertung:



Art, Umfang, Umstände und Zweck der Datenverarbeitung

Betroffene und Daten (Art, Umfang der Datenverarbeitung)

Betroffene	**Anmerkungen** (optional)
Beschäftigter	
Bewerber	
Privatkunde (B2C)	
Interessenten (B2C)	
Geschäftspartner (B2B)	
Interessent (B2B)	
User des Systems	

Datenarten	
Besondere Kategorien enthalten?	nein
Klassifizierung der Daten	
Potential zum Profiling	
Umfang Leistungs-/Verhaltenskontrolle	
Umfang der Daten zu einem Betroffenen	
Anzahl der Betroffenen im Verfahren	
Speicherdauer	

Bewertung: Kritikalität der Art und des Umfangs der Daten

Rechtsgrundlagen (Zweck der Datenverarbeitung)

Zulässigkeitsgrundlage	**Nähere Erläuterung**	**Anmerkungen** (optional)
Vertrag mit dem Betroffenen		
Einwilligung des Betroffenen		
Betriebsvereinbarung		
Erlaubsnis durch andere Rechtsgrundlage		
Rechtliche Verpflichtung zur Datenverarbeitun		
Vertrag zugunsten eines Dritten		
Berechtigtes Interesse des Unternehmens		

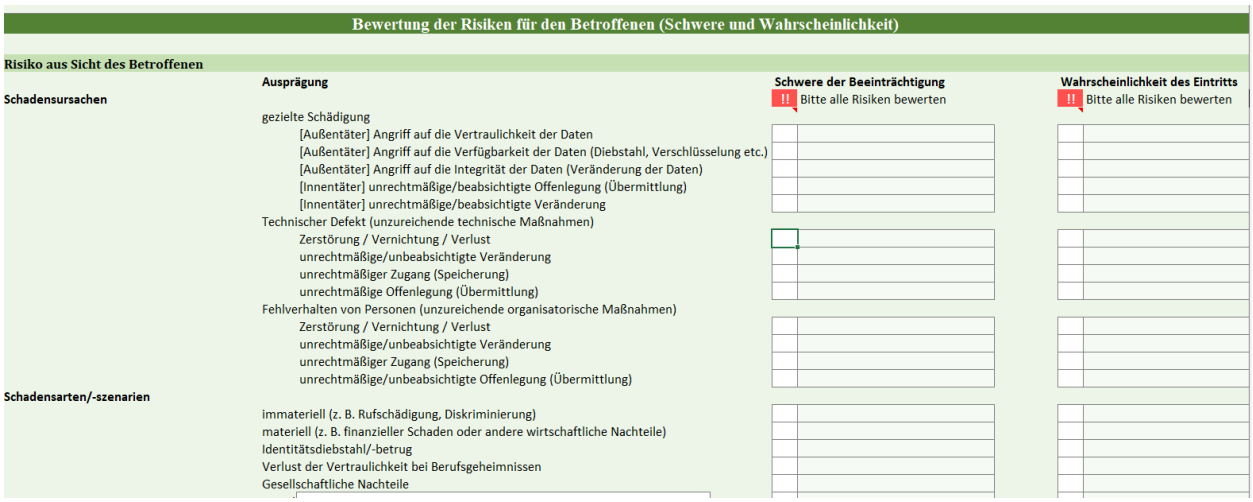
Bewertung: Kritikalität des Zwecks der Datenverarbeitung

Empfänger (Umstand der Datenverarbeitung)

Kategorie	**ggf. nähere Bezeichnung**	**Anforderung**	**erfüllt?**	**Land**	**Garantien**	**offene Anforderungen?**

- » Je umfangreicher die Datenverarbeitung und je mehr persönliche und je sensibler die Daten, desto höher das Risikopotential.
- » Je klarer die Rechtsgrundlage (Vertrag, Einwilligung, Gesetzeserlaubnis/-anordnung) desto geringer das Risikopotential.
- » Je mehr Datenempfänger und je mehr Empfänger im Nicht-EU-Ausland, desto größer das Risikopotential.

Quantitative Bewertung:



Bewertung der Risiken für den Betroffenen (Schwere und Wahrscheinlichkeit)

Risiko aus Sicht des Betroffenen

	Ausprägung	**Schwere der Beeinträchtigung**	**Wahrscheinlichkeit des Eintritts**
Schadensursachen		!! Bitte alle Risiken bewerten	!! Bitte alle Risiken bewerten
	gezielte Schädigung		
	[Außentäter] Angriff auf die Vertraulichkeit der Daten		
	[Außentäter] Angriff auf die Verfügbarkeit der Daten (Diebstahl, Verschlüsselung etc.)		
	[Außentäter] Angriff auf die Integrität der Daten (Veränderung der Daten)		
	[Innentäter] unrechtmäßige/beabsichtigte Offenlegung (Übermittlung)		
	[Innentäter] unrechtmäßige/beabsichtigte Veränderung		
	Technischer Defekt (unzureichende technische Maßnahmen)		
	Zerstörung / Vernichtung / Verlust		
	unrechtmäßige/unbeabsichtigte Veränderung		
	unrechtmäßiger Zugang (Speicherung)		
	unrechtmäßige Offenlegung (Übermittlung)		
	Fehlverhalten von Personen (unzureichende organisatorische Maßnahmen)		
	Zerstörung / Vernichtung / Verlust		
	unrechtmäßige/unbeabsichtigte Veränderung		
	unrechtmäßiger Zugang (Speicherung)		
	unrechtmäßige/unbeabsichtigte Offenlegung (Übermittlung)		
Schadensarten/-szenarien			
	immateriell (z. B. Rufschädigung, Diskriminierung)		
	materiell (z. B. finanzieller Schaden oder andere wirtschaftliche Nachteile)		
	Identitätsdiebstahl/-betrug		
	Verlust der Vertraulichkeit bei Berufsgeheimnissen		
	Gesellschaftliche Nachteile		