IV. Datenschutzfolgeabschätzung gemäß Art. 35 EU DS-GVO

Bei Annahme eines voraussichtlich hohen Risikos für die Rechte und Freitheiten natürlicher Personen muss eine „*Datenschutzfolgeabschätzung*“ (DSFA) vorgenommen werden. In der DSFA wird durch den Verantwortlichen eine Risikoabwägung durchgeführt. Dazu werden die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen berücksichtigt und die Notwendigkeit und Verhältnismäßig der Verarbeitungsvorgänge im Gegensatz zu der Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen geprüft.

Bitte holen Sie bei der Durchführung der DSFA den Rat des Datenschutzbeauftragten ein.

Rat des DSB wurde eingeholt

☐ ja

☐ nein

Folgende **Verantwortliche und Mitarbeiter** waren bei der Durchführung der DSFA beteiligt:

1. Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung

1.1. Systematische, zu Ziffer 3 der Beschreibung der Verarbeitungstätigkeit ergänzende **Beschreibung der geplanten Verarbeitungsvorgänge** inkl. u.a. Empfänger, zugriffsberechtigte Personen, unterstützende Mittel, Speicherfristen (z.B. Systeme, Konfigurationen):

- *Art, Umfang und Umstände der Verarbeitung*
- *Art der personenbezogenen Daten, Empfänger und Speicherfristen*
- *Eingesetzte Datenträger, Wissensträger und/oder Trägermedien (Hardware/Software, Netzwerke, Personen, Papier etc.)*
- *Branche, Rolle des Verantwortlichen und Rolle des Betroffenen*
- *Die eingesetzte Technik muss so konkret beschrieben sein, dass sich die Phasen der Bewertung und der Bewältigung anschließen können*

1.2. Genaue, zu Ziffer 3 der **Beschreibung der Verarbeitungstätigkeit ergänzende Beschreibung der Zwecke der Verarbeitung inkl. der berechtigten Interessen** des verantwortlichen Fachbereichs:

- *Systematische Beschreibung der Zwecke der Verarbeitung, z.B. Abrechnung, Diebstahlschutz, Aufklärung von Straftaten*
- *Systematische Beschreibung der von dem Verantwortlichen verfolgten berechtigten Interessen: rechtlicher, wirtschaftlicher, ideeler oder sonstiger Art (Überschneidungen mit der Beschreibung des Zwecks möglich)*

1.3. Maßgebliche Rechtsgrundlage -> siehe Ziffer III. 9. der Beschreibung der Verarbeitungstätigkeit

2. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

2.1. Genehmigte Verhaltensregeln?

Liegen genehmigte Verhaltensregeln i.S.d. Artikel 40 DSGVO vor, die gem. Artikel 35 Abs. 8 DSGVO zu berücksichtigen sind?

☐ Nein
☐ Ja *-> Welche?*

z.B. CoC Datenschutz

2.2. Notwendigkeit und Verhältnismäßigkeit der Verarbeitung

Konkrete spezifische und legitime Zwecke der Verarbeitung

Einhaltung der Zweckbindung

Berücksichtigung von Betroffenenrechte

2.3. Ausführliche **Beschreibung der hohen Risiken für die betroffenen Personen**

Beschreibung der möglichen physischen, materiellen oder immateriellen Schäden (z.B.: Diskriminierung, Identitätsdiebstahl oder –betrug, finanzieller Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung; grds. wenn sensible Daten (Art. 9 Abs. 1 und 10 DS-GVO) gefährdet sind und zur Verarbeitung öffentlich zugänglich sind oder wenn persönliche Aspekte bewertet werden, um Profile zu erstellen oder zu nutzen[1])

- *Beschreibung der möglichen hohen Risiken und*
- *Bedrohungen aus Sicht der Betroffenen (unbefugter Zugriff, unerwünschte Veränderung von Daten, Verlust von Daten)*

[1] Ausführlichere Beschreibung in Erwägungsgrund 75 der DS-GVO.

2.4. Risikoeinschätzung maßgeblicher Schutzziele:

Wie hoch ist das Risiko für die maßgeblichen Schutzziele?

Risikoeinschätzung, Definition der Datenschutzziele und Maßnahmen zu deren Einhaltung:

Risikoeinschätzung: Gliederung nach Schutzstufenkonzept

- Risiko niedrig*

geringe Verarbeitungshäufigkeit **oder** geringes Missbrauchsinteresse

- Risiko mittel**

hohe Verarbeitungshäufigkeit **oder** hohes Missbrauchsinteresse

- Risiko hoch***

hohe Verarbeitungshäufigkeit **und** hohes Missbrauchsinteresse

Risiko für	niedrig*	mittel**	hoch***	Begründung
Vertraulichkeit				
Integrität				
Verfügbarkeit				
Authentizität				
Transparenz				
Nichtverkettbarkeit				
Datensparsamkeit				

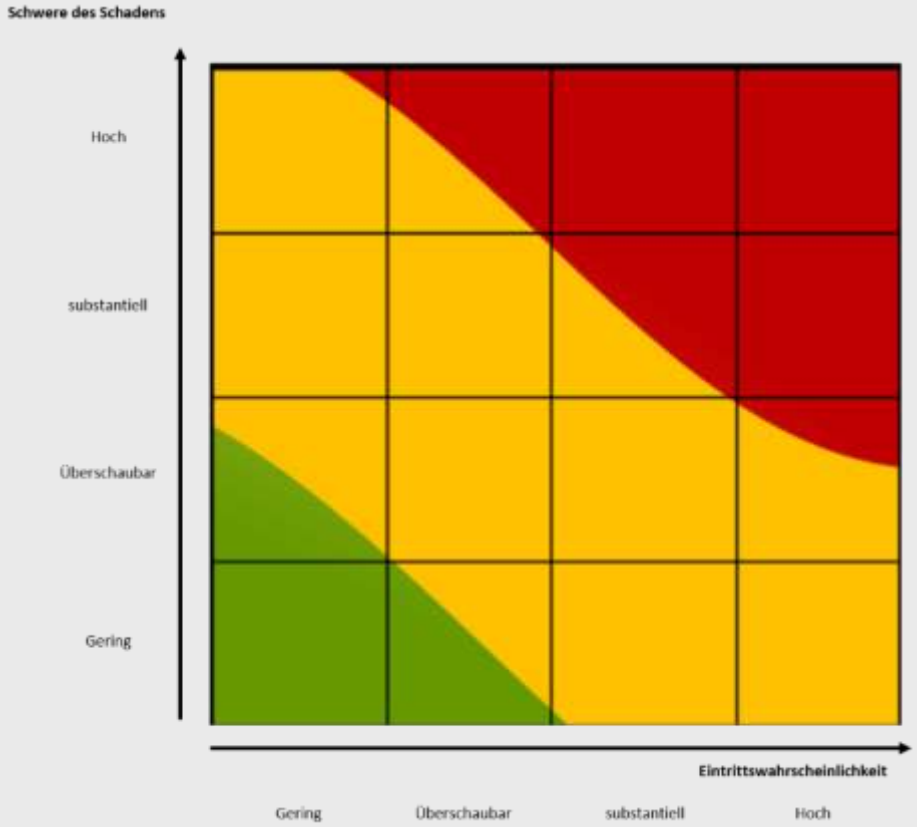
2.5. Welche Angreifer und Risikoquellen kommen in Betracht?

☐ Staatliche Stellen
☐ Unternehmen
☐ Arbeitgeber
☐ Banken
☐ Krankenhäuser
☐ Ärzte

☐ Sonstige

2.6. Risikobewertung für die Rechte und Freiheiten der betroffenen Personen:

Das Risiko bemisst sich als Produkt der Faktoren „Schwere des drohenden Schadens“ und „Eintrittswahrscheinlichkeit“. Für ein hohes Risiko i.S.d. Artikel 35 DSGVO müssen i.d.R. mindestens „wesentliche“ Faktoren in Kombination mit „maximalen“Faktoren aufeinandertreffen.



*Bemessung der **Schwere***

maximal/hoch	Möglicher Eintritt signifikanter, sogar irreversibler Konsequenzen, die nicht überwunden werden können (Vernichtung der wirtschaftlichen Existenz, Arbeitsunfähigkeit, dauerhafte physische oder psychische Konsequenzen, Tod)
wesentlich/substantiell	Möglicher Eintritt signifikanter Konsequenzen, die sich – wenn auch ggf. mit großen Anstrengungen – wieder überwinden lassen (Verlust der Kreditwürdigkeit, Verlust von Eigentum, gesundheitliche Verschlechterung)
begrenzt/überschaubar	Möglicher Eintritt signifikanter Konsequenzen, die sich mit nur geringen Anstrengungen wieder überwinden lassen (Zusatzkosten, Stress, geringe physische Belastungen)
vernächlässigbar/gering	Eintritt allenfalls bloßer Belästigungen, die sich ohne Probleme ertragen lassen (Ärgernisse, kurzer Zeitverlust, etc.)

2.6.1. Schwere des drohendenSchadens:

☐ maximal

☐ wesentlich

☐ begrenzt

☐ überschaubar

*Bemessung der **Eintrittswahrscheinlichkeit***

maximal/hoch	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen sehr leicht möglich (z.B. Aufbewahrung im öffentlich zugänglichen Bereich)
wesentlich/substantiell	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen möglich (z.B. Aufbewahrung im öffentlich zugänglichen Bereich mit leicht umgehbarer Zutrittskontrolle/-beschränkung
begrenzt/überschaubar	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen schwer möglich (z.B. einfache Zugangssicherung)
vernachlässigbar/gering	Realisierung der Bedrohung erscheint aufgrund der gewählten Ressourcen nicht möglich (z.B. doppelte Zugangssicherung)

2.6.2. Eintrittswahrscheinlichkeit:

☐ maximal

☐ wesentlich

☐ begrenzt

☐ überschaubar

Begründung:

Für die Bewertung der Schwere und der Bemessung der Eintrittswahrscheinlichkeit

2.6.3. Ergebnis der Risikobewertung für die Rechte und Freiheiten der betroffenen Person:

☐ hohes Risiko (rot)

☐ Risiko (gelb)

☐ Geringes Risiko (grün)

2.7. **Technische Risikobewertung:**

Die technische Risikobewertung erfolgt obligatorisch in folgender Risikomatrix.
Bitte Binden Sie für die Bewertung die IT-Security/Informationssicherheit mit ein *Link*.
für unten aufgeführte Systeme.

- Online Service (Internet)
- Host-Anwendungen (z.B. Paris, Kompass, Kavis, …)
- Kleinserver-Systeme (z.B. Oracle, etc.)
- …[2]

Das Risiko ergibt sich aus Auswirkung (in Abhängigkeit mit der Klassifikation) und der Wahrscheinlichkeit des Eintritts.

Impact (Auswirkung)							
	Extrem	Extrem	5	Medium	Hight t	High	High
	Signifi-cant	Bedeu-tend	4	Medium	Significant	Significant	High
	Medium	Mittel-mäßig	3	Non or low	Medium	Medium	Significant
	Low	Gering	2	Non or low	Non or low	Medium	Medium
	Insignifi-cant	Zu ver-nach-lässigen	1	Non or low	Non or low	Non or low	Non or low
				1	2	3	4
				Almost impossible	Possible	Likely	Most likely
				Fast unmöglich	Möglich	Wahrschein-lich	Höchst wahrschein-lich
				Probability (Wahr-scheinlichkeit)			

Begründung:

[2] Abhängig vom Unternehmen können / müssen weitere Systeme einer technischen Risikobewertung unterzogen werden.

3. Reduzierung der identifizierten Risiken durch folgende Abhilfemaßnahmen

3.1. **Geeignete Maßnahmen zur Risikoverringerung**:

3.1.1. Vertraulichkeit
- ☐ Berechtigungskonzept
- ☐ Passwortkonzept
- ☐ Verarbeitung gem. Art. 32 Abs. 4 DSGVO
- ☐ Sonstige[3]:

3.1.2. Integrität
- ☐ Hash-Wert Vergleiche vorher/nachher
- ☐ Sonstige[3]:

3.1.3. Verfügbarkeit
- ☐ Sicherheitskonzept
- ☐ Backupkonzept
- ☐ Unterbrechungsfreie Stromversorgung
- ☐ Sonstige[3]:

3.1.4. Authentizität
- ☐ Penetrationstests
- ☐ Löschkonzept
- ☐ Sonstige[3]:

3.1.5. Transparenz
- ☐ Verzeichnis für Verarbeitungstätigkeiten
- ☐ Dokumentation aller Maßnahmen
- ☐ Unterrichtung von Betroffenen (Datenschutzmanagement)
- ☐ Sonstige[3]:

3.1.6. Nichtverkettbarkeit
- ☐ Mandantenfähigkeit
- ☐ Einschränkung von Verarbeitungs- Nutzungs-. und Übermittlungsrechten (Berechtigungskonzept)
- ☐ Sonstige[3]:

3.1.7. Datensparsamkeit
- ☐ Verfahren, bei denen möglichst wenig personenbezogene Daten verarbeitet werden
- ☐ Anonymisierung personenbezogener Daten
- ☐ Pseudonymisierung personenbezogener Daten
- ☐ Speicherdauer der Daten entspricht den gesetzlichen Anforderungen oder ist durch die Verarbeitungstätigkeiten gerechtfertigt
- ☐ Sonstige[3]:

[3] Sonstige Maßnahmen zur Risikoverringerung bitte auf der nächsten unter „**Weitere Abhilfemaßnahmen**“ eintragen.

Die aufgezeigten Maßnahmen der einzelnen Schutzziele sind beispielhaft und nicht abschließend zu verstehen. Soweit weitere Maßnahmen geplant Sind, bitte unter 3.1.8 Sonstige Maßnahmen beschreiben.

3.1.8. Sonstige Maßnahmen

Folgende **weitere, spezifische Abhilfemaßnahmen** sind zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus / zur wirksamen Minimierung der Risiken geplant (z.B. Garantien oder Sicherheitsvorkehrungen, Einsatz datenschutzfreundlicher Technik/Voreinstellungen):

Optional, soweit zur Minimierung des Risikos notwendig

3.2. **Maßnahmen im Sinne der Betroffenen** wurden eingerichtet (z.B. Benachrichtigung, Berichtigung, Auskunftserteilung):

☐ Nein
☐ Ja ->Welche?

Welche?

Abstimmung mit betroffenen Personen / Standpunkt der betroffenen Person bzw. des Vertreters wurde eingeholt:

☐ ja (z.B. Betriebsrat, Kundenbeirat, Kundenumfrage)
☐ nein

3.3. Abschließende Risikobewertung:

Bewertung der Risiken für die betroffenen Personen: Risikoidentifikation, Eintrittswahrscheinlichkeit, Schaden, technisches Risiko, Risiko für die Einhaltung der Betroffenenrecht, etc.

Ergebnis: Sind die Risiken durch die Maßnahmen hinreichend minimiert?

☐ Ja *-> Ende der DSFA*
☐ Nein

Wenn nein:
Mit welchen weiteren, spezifischen Maßnahmen kann das Risiko hinreichend minimiert werden?

Sind die spezifischen Maßnahmen verhältnismäßig (auch unter Berücksichtigung der dadurch entstehenden Zusatzkosten) und können diese implementiert werden?

Werden die spezifischen Maßnahmen umgesetzt?

☐ Ja *-> Ende der DSFA*
☐ Nein

Wenn nein: vorherige Konsultation mit der Aufsichtsbehörde!
Diese erfolgt über den Datenschutzbeauftragten.

3.4 Vorerige Konsultation mit der Aufsichtsbehörde gemäß Art. 36 EU DS-GVO wurde durchgeführt

☐ ja (erforderlich, soweit das Ergebnis der Datenschutzfolgeabschätzung ist, dass die Verarbeitung ein hohes Risiko zur Folge hätte und keine Maßnahmen zur Eindämmung der Risiken

☐ nein

4. Ersteller dieser Beschreibung DSFA

Die fachlichen und technischen Festlegungen aus diesem Formular wurden vom Fachbereich in Abstimmung mit der Technik vorgenommen von:

(Ort, Datum, Name, Vorname, Name der Abteilung)

Bestätigung der Einholung des Rats des Datenschutzbeauftragten:

(Ort, Datum, Name, Vorname, Datenschutzbeauftragter)

Anlage Erläuterungen

Anlage 1: Datenschutzziele

1.1.1. Vertraulichkeit

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass nur befugt auf Verfahren und Daten zugegriffen werden kann.

1.1.2. Integrität

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass Daten aus Verfahren unversehrt, zurechenbar und vollständig bleiben.

1.1.3. Verfügbarkeit

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass Verfahren und Daten zeitgerecht zur Verfügung stehen und diese ordnungsgemäß angewendet werden können.

1.1.4. Authentizität

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass Verfahren ohne Schaden zu nehmen jederzeit unterbrochen und Daten verändert werden können.

1.1.5. Transparenz

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass Verfahren so dokumentiert werden, dass diese jederzeit für die eigene Organisation, Betroffene und Aufsichtsbehörden im Hinblick auf die Schutzmaßnahmen prüffähig sind.

1.1.6. Nichtverkettbarkeit

Verfahren, welche personenbezogene Daten verarbeiten gewährleisten, dass diese klar und systematisch definiert und gegeneinander separiert sind.

1.1.7. Datensparsamkeit

Verfahren, welche personenbezogene Daten verarbeiten, gewährleisten, dass diese einen Bezug zum Verarbeitungszweck haben oder geeignet sind, zur Erreichung des Zwecks beizutragen und die Erhebung auf solche Daten festzulegen, die in diesem Zeitpunkt für die festgelegten Zwecke erforderlich sind.