

# HES - RICHTLINIE ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG

## 1. Einführung

Dies ist die Richtlinie zur Datenschutz-Folgenabschätzung (die „**DSFA Richtlinie**“) von HES International B.V. („**HES**“). In dieser DSFA-Richtlinie bezeichnet der Begriff personenbezogene Daten alle Informationen, die sich auf eine identifizierbare lebende Person beziehen. Diese Definition ist sehr weit gefasst und deckt fast alle Informationen (vom Namen einer Person bis hin zu ihrer Handynummer) in dem Maße ab, wie sie sich auf eine identifizierbare lebende Person beziehen. Darüber hinaus umfasst die Verarbeitung das Erheben, Speichern, Analysieren, Verwenden, Offenlegen, Archivieren, Löschen oder jeden anderen Vorgang im Zusammenhang mit personenbezogenen Daten.

## 2. Was ist eine Datenschutz-Folgenabschätzung?

Laut Gesetz ist HES (als Datenverantwortliche) in einer Reihe von Umständen verpflichtet, eine Folgenabschätzung („**DSFA**“) der Auswirkungen und potenziellen Risiken durchzuführen, die ihre geplante Verarbeitung für die betroffenen Personen haben könnte, insbesondere wenn das Unternehmen eine potenziell hoch-riskante Verarbeitung oder Massenverarbeitung personenbezogener Daten durchführt. Die Datenverantwortlichen müssen: (i) die Verarbeitung beschreiben, (ii) wo anwendbar, die Gründe für diese Verarbeitung erläutern, und (iii) die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, zusammen mit den Risiken für die betroffenen Personen beurteilen, die sich aus der Verarbeitung personenbezogener Daten ergeben.

Eine DSFA sollte zu einem frühen Zeitpunkt, und bevor die Verarbeitung erfolgt, effektiv alle Problembereiche identifizieren und anschließend lösen.

Die systematische und vorgeschriebene Durchführung von DSFA bei HES ist integraler Bestandteil ihres Compliance-Programms und zeigt, dass HES alle potenziellen oder tatsächlichen Risiken, die durch die Verarbeitung entstehen können, sorgfältig und ordnungsgemäß abgewogen hat.

Eine DSFA ist ein Schlüsselinstrument, sowohl um die Einhaltung der DSGVO zu gewährleisten, als auch um diese Einhaltung nachzuweisen. Der Rahmen der DSFA ist ein wichtiger Teil der Einhaltung des umfassenderen Grundsatzes der „Rechenschaftspflicht“, der von der DSGVO auferlegt wird.

### 3. Wann ist eine DSFA erforderlich?

Sie (als der betreffende Projektleiter oder sein Delegierter) sollten eine DSFA durchführen: (i) wenn ein neues Informationstechnologiesystem oder eine andere Vorkehrung (technischer oder sonstiger Art), das/die die Verarbeitung personenbezogener Daten einschließt („**Verarbeitungssystem**“) innerhalb oder im Auftrag von HES eingesetzt oder (ii) eine signifikante Änderung an einem bestehenden Verarbeitungssystem durchgeführt werden soll.

Besondere Vorsicht ist geboten, wenn das Verarbeitungssystem zu hohen Risiken für die Privatsphäre der betroffenen Personen führen kann. Zum Beispiel, wenn das Verarbeitungssystem:

- Personen systematisch überwacht;
- personenbezogene Daten in umfassendem Maße verarbeitet;
- neue oder innovative technologische Lösungen verwendet;
- Daten von äußerst persönlicher oder sensibler Natur verarbeitet; oder
- die Beauftragung eines neuen Lieferanten vorsieht.

### 4. Wie ist in diesem Fall vorzugehen?

Sie sollten:

- sicherstellen, dass die Anforderungen dieser DSFA-Richtlinie und die Datenschutzrechte der betroffenen Personen bei der Wahl, dem Entwurf und der Umsetzung der neuen Elemente des neuen oder geänderten Verarbeitungssystems berücksichtigt werden. Insbesondere:
  - (a) sind die personenbezogenen Daten, die von dem Verarbeitungssystem verarbeitet werden sollen, auf ein Minimum zu begrenzen, das für die Geschäftsanforderungen von HES erforderlich ist; und
  - (b) müssen, wo personenbezogene Daten verarbeitet werden sollen und dies angemessen praktikabel und vereinbar mit der Handlungsweise von HES ist, Daten, die eine Identifizierung von betroffenen Personen erlauben, separat von anderen Elementen der betreffenden personenbezogenen Daten aufbewahrt und wirksam geschützt werden, damit die betroffenen Personen nicht identifizierbar sind, außer wenn dies für die Geschäftszwecke von HES notwendig ist; und
- müssen die Anforderungen dieser DSFA-Richtlinie und der HES-Datenschutzrichtlinie für die Verarbeitung personenbezogener Daten durch HES in diesem Verarbeitungssystem und deren Auswirkungen auf die Privatsphäre der betroffenen Personen berücksichtigt werden. Sie sollten sicherstellen, dass das Verarbeitungssystem nach der Umsetzung oder Änderung die Grundsätze dieser DSFA-Richtlinie und der HES-Datenschutzrichtlinie in

allen Aspekten erfüllt und seine Umsetzung nicht zu hohen Risiken für den Datenschutz der betroffenen Personen führt, die nicht begrenzt werden können.

## 5. Sollte eine DSFA ausgeführt werden?

Nach Abwägung der Auswirkungen dieser DSFA-Richtlinie und der HES-Datenschutzrichtlinie für die Verarbeitung personenbezogener Daten durch HES in diesem Verarbeitungssystem und deren Auswirkungen auf die Privatsphäre der betroffenen Personen müssen Sie entscheiden, ob eine DSFA durchgeführt werden sollte.

Wenn Sie sich nicht sicher sind, ob die Grundsätze dieser DSFA-Richtlinie oder der HES-Datenschutzrichtlinie Anwendung finden, oder wenn Sie der Meinung sind, dass die Einführung des neuen oder geänderten Verarbeitungssystems zu hohen Risiken für die Privatsphäre der betroffenen Personen führen kann, sollten Sie dem Compliance-Beauftragten vor Ort eine ausreichend detaillierte Erläuterung des vorgeschlagenen neuen Verarbeitungssystems oder der Umstellung auf ein Verarbeitungssystem zusammen mit einer Zusammenfassung Ihrer Bewertung oder Fragen und Ihrer Begründung zukommen lassen, indem Sie Teil C von Anhang 1 (eine „Erstmitteilung“) ausfüllen.

Nach Erhalt der Erstmitteilung prüft der Compliance-Beauftragte vor Ort, ob eine DSFA erforderlich ist, und informiert Sie über seine Entscheidung. Stellt der Compliance-Beauftragte vor Ort fest, dass eine DSFA erforderlich ist, sollten Sie seine Anweisungen befolgen, einschließlich des Ausfüllens des in Teil D von Anhang 1 beigefügten DSFA-Formulars zur Überprüfung durch den Compliance-Beauftragten vor Ort (das „DSFA-Formular“).

Ein neues Verarbeitungssystem darf nicht innerhalb oder im Namen von HES implementiert werden, und es dürfen keine wesentlichen Änderungen an einem bestehenden Verarbeitungssystem vorgenommen werden, es sei denn, die in den Abschnitten 4 und 5 erwähnte Beurteilung wurde durchgeführt, und Sie:

- haben (i) die Grundsätze dieser DSFA-Richtlinie und der HES-Datenschutzrichtlinie berücksichtigt und sind der Meinung, dass sie in allen Aspekten erfüllt werden und (ii) sind nicht der Meinung, dass die Umsetzung des neuen oder geänderten Verarbeitungssystems zu hohen Risiken für den Datenschutz der betroffenen Personen führt; oder
- Sie haben dem Compliance-Beauftragten vor Ort eine Erstmitteilung geschickt und er hat Sie darüber informiert, dass eine vollständige DSFA nicht erforderlich ist; oder
- Sie haben eine vollständige DSFA auf Anweisung des Compliance-Beauftragten vor Ort durchgeführt, und der Compliance-Beauftragte vor Ort hat Sie darüber informiert, dass das neue oder geänderte Verarbeitungssystem und seine Implementierung erfolgen kann.

## 6. Ihre Verpflichtungen im Rahmen dieser Richtlinie

Wir halten uns an unsere Verpflichtungen zum Datenschutz und zum Schutz der Privatsphäre und nehmen diese sehr ernst. Im Rahmen Ihrer Tätigkeit bei uns sind Sie ebenfalls verpflichtet, dies zu

tun. Die Nichterfüllung dieser Pflichten und/oder die Nichteinhaltung dieser Richtlinie kann ein Disziplinarvergehen darstellen und zur Entlassung führen.

## 7. Fragen

Wenn Sie Fragen zu dieser Richtlinie haben oder Zweifel bezüglich ihrer Anforderungen hegen, wenden Sie sich bitte an den Chief Compliance Officer ([compliance@hesinternational.eu](mailto:compliance@hesinternational.eu)).



# ANHANG 1

## Vorlage des Formulars zur Datenschutz-Folgenabschätzung (Data Privacy Impact Assessment Form)

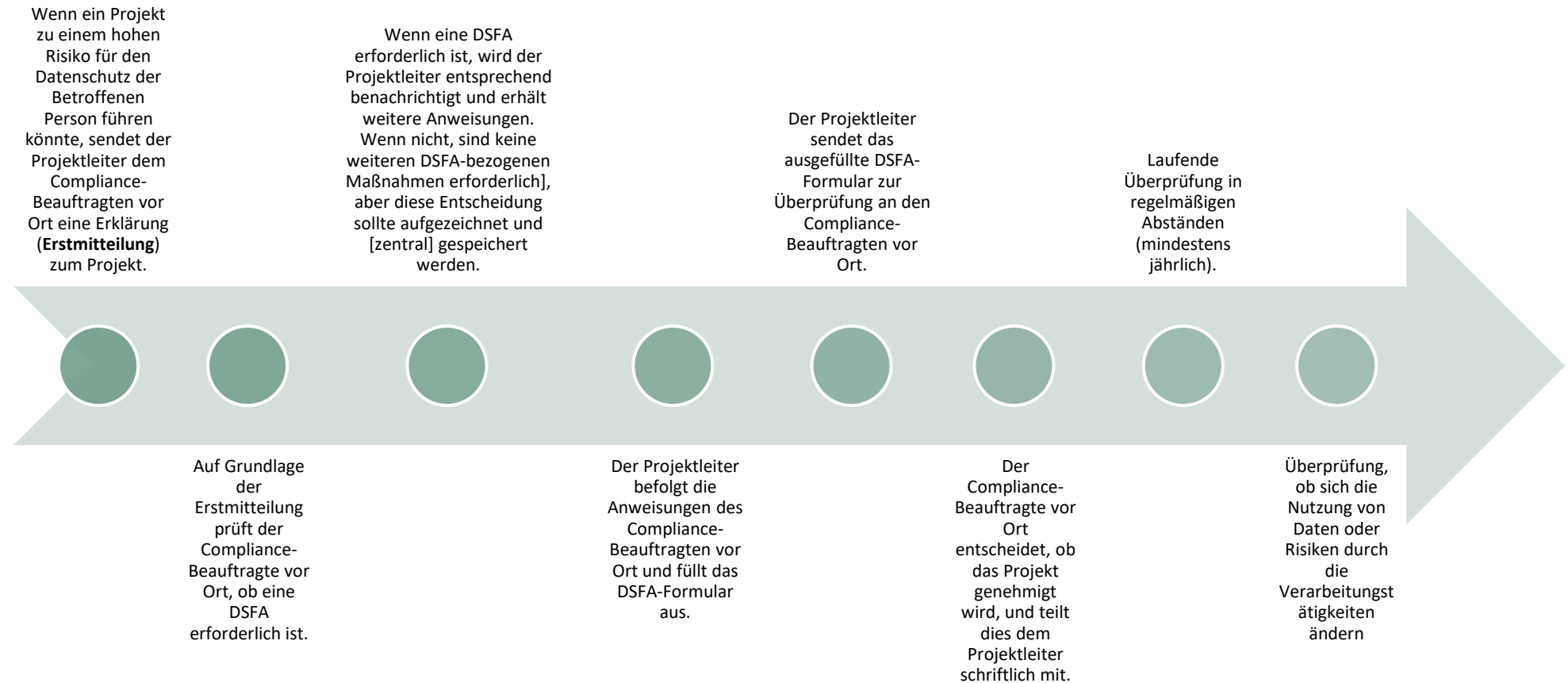
### Teil A: Einführung

Definierte Begriffe, die in diesem Anhang 1 verwendet werden, sind in Teil E (Glossar) im Anhang zu diesem Dokument zu finden.

Teil B enthält ein Übersichtsdiagramm des DSFA-Verfahrens. In Teil C werden einige Fragen gestellt, um die Art des Projekts zu ermitteln und festzustellen, ob eine DSFA erforderlich ist („die **Erstmitteilung**“). Teil D ist das DSFA-Formular und enthält eine Reihe von Fragen zum vorgeschlagenen Projekt und zur vorgeschlagenen Verwendung personenbezogener Daten (das „**DSFA-Formular**“).

*Haftungsausschluss:* Das DSFA-Formular sieht nicht die Situation vor, in der der für die Verarbeitung Verantwortliche die Datenschutzaufsichtsbehörde konsultieren muss. Dies sollte von der **Abteilung Legal** geleitet werden.

## Teil B: Überblick über das DSFA-Verfahren



Teil C: Vorab-Fragen, um festzustellen, ob eine DSFA notwendig ist und wenn ja, wie diese Beurteilung durchgeführt werden soll („Erstmitteilung“)

### Allgemeine Projektinformation

Frage	Antwort
<p>[<b>Relevante HES-Einheit</b>] die das Projekt beantragt/durchführt</p>	
<p>Angaben zum Projektleiter</p>	<p>Name:</p> <p>Rolle:</p> <p>Telefon:</p> <p>E-Mail:</p>
<p>Wird Ihr Projekt die Verarbeitung personenbezogener Daten beinhalten - wenn nein, sind keine weiteren Maßnahmen erforderlich. Bitte senden Sie dieses Formular zur Prüfung und Genehmigung an den Compliance-Beauftragten vor Ort.</p>	
<p>Bitte beschreiben Sie so detailliert wie möglich, inwiefern Ihr Projekt die Verarbeitung personenbezogener Daten umfasst.</p>	
<p>Wird HES personenbezogene Daten als für die Datenverwaltung Verantwortlicher oder als Auftragsverarbeiter verarbeiten? Erklären Sie in beiden Fällen, warum.</p>	
<p>Was ist der Zweck des Projekts?</p>	

Was sind die Vorteile für HES?	
Was sind die potenziellen Vorteile für andere Parteien (einschließlich Kunden von HES und betroffene Personen, soweit zutreffend)?	
Gibt es Dokumente, die für das Projekt relevant sind, wie z. B. ein Projektvorschlag, die für die Zwecke dieser DSFA nützlich sein könnten - z. B. in denen dargelegt wird, wie personenbezogene Daten verwendet werden? Wenn ja, führen Sie sie bitte auf und fügen Sie sie diesem Formular bei.	
Bis zu welchem Datum soll das Projekt durchgeführt werden?	

### Das Projekt und personenbezogene Daten

Frage	Ja/Nein	Datenschutzrisiko
Wird das Projekt das Einholen von personenbezogenen Daten über Einzelpersonen beinhalten?		Niedrig-mittel
Wird das Projekt von Einzelpersonen die Angabe von Informationen über sie selbst verlangen, um den Verarbeitungsdienst anbieten zu können, oder ist dies freiwillig?		Mittel
Wie werden die Personen benachrichtigt/informiert?		Mittel



Werden personenbezogene Daten an die HES-Organisation oder an Dritte weitergegeben oder innerhalb der HES-Organisation oder bei Dritten gespeichert, und zwar auf eine Art und Weise, die bisher noch nicht erfolgt ist?		Mittel
Werden die personenbezogenen Daten für einen neuen oder anderen Zweck verwendet?		Niedrig-mittel
Beinhaltet das Projekt den Einsatz neuer Technologien?		Mittel-Hoch
Führt das Projekt dazu, dass Entscheidungen getroffen oder Maßnahmen gegen Einzelpersonen in einer Weise ergriffen werden, die erhebliche Auswirkungen auf sie haben könnte (z. B. Erstellung von Profilen)?		Hoch
Wird das Projekt automatisierte Entscheidungsprozesse oder das Profiling von Personen beinhalten?		Hoch
Wird das Projekt eine umfangreiche Verarbeitung		Mittel-Hoch

personenbezogener Daten beinhalten?		
Wird das Projekt eine umfangreiche Verarbeitung von Daten über besondere Kategorien oder strafrechtliche Verurteilungen und Straftaten beinhalten?		Hoch
Wird es eine grenzüberschreitende Verarbeitung geben?		Hoch

### Zusammenfassung

Frage	J/N
Erscheint es auf der Grundlage der oben genannten Informationen und Antworten wahrscheinlich, dass die Verarbeitung personenbezogener Daten hohe Risiken für die betroffenen Personen birgt oder eine riskante Verarbeitungstätigkeit darstellt?	
Wenn die Antwort auf die obige Frage "Nein" lautet, erläutern Sie bitte hier die Gründe für diese Schlussfolgerung und senden Sie dieses Formular zur Genehmigung an den Compliance-Beauftragten vor Ort.	
Wenn die Antwort "Ja" lautet, fahren Sie bitte mit dem nächsten Abschnitt fort.	

Teil D: Formular zur Datenschutz-Folgenabschätzung („DSFA-Formular“)

#	Frage	Antwort
Die personenbezogenen Daten		
1.	Welche personenbezogenen Daten werden erhoben? (bitte kreuzen Sie entsprechend J/N an)	Name: J / N Adresse: J / N Geburtsdatum: J / N Rasse oder ethnische Herkunft: J / N Familienstand: J / N Informationen zu Familie und Verwandtschaft: J / N Religion: J / N Gesundheitliche Informationen: J / N Sexuelle Orientierung: J / N Politische Ansichten: J / N Genetische Informationen: J / N Informationen zu strafrechtlichen Verurteilungen: J / N Informationen über körperliche Merkmale (Größe, Gewicht usw.): J / N Kreditkarten-/Bankkontonummer: J / N Eigentumsinformationen (Autos, Häuser, Wohnungen, persönliches Eigentum): J / N Kreditgeschichte: J / N Informationen zu sozialen Netzwerken: J / N Sonstiges (bitte ausführen): J / N
2.	Wie werden die Daten gesammelt?	
3.	Was ist die Verarbeitungsaktivität?	

#	Frage	Antwort
4.	Ist diese Verarbeitung notwendig oder könnte die Aktivität auf eine andere Art und Weise durchgeführt werden?	
5.	Könnte das Projekt trotzdem erfolgreich durchgeführt werden, ohne dass einige oder alle dieser personenbezogenen Daten gesammelt werden?	
6.	Über wen könnten personenbezogene Daten erhoben/verarbeitet werden? (bitte kreuzen Sie entsprechend J/N an)	<p>Angestellte: J / N</p> <p>Nicht-Angestellte: J / N</p> <p>Wenn es sich um Nicht-Angestellte handelt, geben Sie bitte an, um wen es sich handelt (Kunden, Lieferanten, andere Dritte usw.):</p>
7.	Zu welchem spezifischen Zweck werden die personenbezogenen Daten verarbeitet (z. B. für den Betrieb eines neuen, auf die Personalvorsorge abgestimmten Portals)? Beschreiben Sie so detailliert wie möglich, warum die Informationen verarbeitet werden.	
8.	Wie lange werden die personenbezogenen Daten gespeichert?	
Grundlage für die Beurteilung		
9.	Werden die personenbezogenen Daten auf der Grundlage der Einwilligung der Betroffenen Person verarbeitet? Wenn ja, wie wird diese Einwilligung eingeholt?	

#	Frage	Antwort
10.	Werden die personenbezogenen Daten in Erfüllung eines Vertrages mit den betroffenen Personen verarbeitet?	
11.	Werden die personenbezogenen Daten auf der Grundlage eines legitimen Geschäftsinteresses von HES (z. B. interne Personalverwaltung) verarbeitet?	
12.	Werden die personenbezogenen Daten auf der Grundlage einer anderen rechtlichen Begründung verarbeitet (siehe Teil F für ein Verzeichnis der rechtmäßigen Begründungen)?	
Die Informationsflüsse		
13.	Wo werden die personenbezogenen Daten nach der Erhebung bei den betroffenen Personen gespeichert?	
14.	Wer wird Zugang zu den personenbezogenen Daten haben?	
15.	Werden Berichte erstellt, die die Verwendung und Offenlegung der personenbezogenen Daten erfordern?	
16.	Werden die personenbezogenen Daten an eine Nicht-HES-Einheit übertragen? Wenn ja, an welche Einheit und zu welchem Zweck?	
17.	Werden die personenbezogenen Daten in Länder außerhalb des	

#	Frage	Antwort
	Europäischen Wirtschaftsraums übertragen oder von Personen außerhalb des Europäischen Wirtschaftsraums abgerufen?	
18.	Wurde eine Bestandsaufnahme der personenbezogenen Daten durchgeführt?	
19.	<p>Wenn die Antwort auf (18) „Ja“ ist, stellen Sie bitte eine Karte der personenbezogenen Daten zur Verfügung, die die Ströme der an diesem Projekt beteiligten personenbezogenen Daten veranschaulicht.</p> <p>(unter Angabe der Art der persönlichen Daten, der Einheiten, zwischen denen sie ausgetauscht werden, der Standorte dieser Einheiten und der Speicherorte)</p>	
20.	Wie lange werden die personenbezogenen Daten aufbewahrt?	
Anforderungen an die Beratung		
21.	Wen werden Sie intern bezüglich der mit dem Projekt verbundenen Datenschutz- und Sicherheitsrisiken konsultieren?	
22.	Haben Sie den Rat des örtlichen Compliance-Beauftragten, des Chief Compliance Officer oder der Rechtsabteilung eingeholt?	

#	Frage	Antwort
23.	Müssen Betriebsräte oder andere Arbeitnehmergremien zur Beratung herangezogen werden (wenn es um HR-/Arbeitnehmerdaten geht)?	
24.	Müssen bei grenzüberschreitenden Transfers die Daten von einer anderen Rechtsordnung aus abgezeichnet werden?	
25.	Wenn die Fragen (23) oder (24) oben mit „Ja“ beantwortet werden: Haben Sie die entsprechenden Beratungen mit den relevanten Parteien durchgeführt? Bitte bestätigen Sie dies hier und geben Sie an, mit wem und wann die Beratungen durchgeführt wurden.	
Risikoerkennung		
26.	<p>Welche spezifischen Datenschutzprobleme haben Sie auf der Grundlage der obigen Fragen identifiziert, sofern vorhanden? Z. B. das Risiko, dass personenbezogene Daten z. B. von Unbefugten eingesehen werden:</p> <ul style="list-style-type: none"> <li>• Risiko, dass die Sicherheit der Daten kompromittiert wird;</li> <li>• Risiko, dass die Personen gegen die Verarbeitung Einspruch erheben, wenn sie informiert würden;</li> <li>• Risiko, dass die Genauigkeit der Daten nicht gewahrt wird;</li> </ul>	


#	Frage	Antwort
	<ul style="list-style-type: none"> <li>Risiko, dass personenbezogene Daten länger als nötig aufbewahrt werden.</li> </ul>	
27.	Was ist der spezifische Schaden, den solche Risiken für den Einzelnen bedeuten würden (z. B. das Risiko, dass personenbezogene Daten gestohlen werden und die betroffenen Personen dadurch Betrug und Identitätsdiebstahl ausgesetzt sind)?	
28.	Gibt es ein spezifisches Compliance-Risiko?	
29.	Besteht ein breiteres organisatorisches Risiko (z. B. hohe Strafen als Folge des Verstoßes und eine daraus resultierende negative Berichterstattung in den Medien)?	
Schritte und Maßnahmen zur Speicherung, Sicherung und zum Schutz der persönlichen Daten		
30.	Welche Maßnahmen werden in Bezug auf jedes oben identifizierte Risiko ergriffen, um die personenbezogenen Daten zu sichern und zu schützen (z. B. Verschlüsselung, Multi-Faktor-Authentifizierung)?	



#	Frage	Antwort
31.	Wie werden wir in Bezug auf jedes oben identifizierte Risiko die Ausübung der Rechte der Betroffenen Person erleichtern (z. B. das Recht auf Zugang)?	
32.	Wie werden den betroffenen Personen angemessene Informationen über das Projekt und die damit verbundenen Risiken für die Privatsphäre mitgeteilt, falls erforderlich?	
33.	Werden diese Maßnahmen das Risiko insgesamt beseitigen oder lediglich verringern?	
34.	Wird unter Berücksichtigung der identifizierten Risiken und der vorgeschlagenen Lösungen zur Minderung dieser Risiken die endgültige Auswirkung auf die Datenschutzrechte der betroffenen Personen angesichts der Ziele und Vorteile des Projekts als akzeptabel angesehen?	
Einbeziehung von Erkenntnissen und Maßnahmen zur Eliminierung/Minderung identifizierter Risiken		
35.	Wie werden diese Erkenntnisse in das Projekt eingebunden?	

#	Frage	Antwort
36.	Wer wird dafür verantwortlich sein, dass die Ergebnisse richtig eingebunden werden?	
37.	Bis wann?	
38.	Welches Verfahren gilt für betroffene Personen, die ihre Bedenken hinsichtlich ihrer Privatsphäre im Zusammenhang mit dem Projekt äußern möchten?	

### Zusammenfassung

Frage	J/N
Werden die identifizierten Risiken beseitigt, reduziert oder akzeptiert?	
Wenn nicht, darf mit der Bearbeitung erst begonnen werden, wenn die DSFA auf  erweitert wurde und geeignete Maßnahmen ergriffen werden können.	

<b>Abzeichnen und Genehmigung/Ablehnung</b>	
<b>Projektleiter</b>	
Name	
Bezeichnung der Tätigkeit	
Unterschrift	
Datum	
<b>Vertreter des Compliance-Teams (falls benannt)</b>	
Name	
Bezeichnung der Tätigkeit	
Unterschrift	
Datum	

<b>Bestimmung des Compliance-Beauftragten vor Ort</b>	
Name	
Datum	
Antwort	
Erläuterung (sofern zutreffend)	

Unterschrift	
--------------	--



## Teil E

### Glossar

Begriff	Begriffsbestimmung
DSGVO	Die Datenschutz-Grundverordnung, die am 25. Mai 2018 in Kraft getreten ist. Die DSGVO gilt nur für personenbezogene Daten - sie umfasst keine personenbezogenen Daten, die sich auf Unternehmen und andere nicht lebende Personen beziehen.
Verantwortlicher für die Datenverarbeitung:	Das Unternehmen, das die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.
Auftragsverarbeiter:	Das Unternehmen, das personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Compliance Officer vor Ort	Die Person, die innerhalb der HES-Einheit für Datenschutz-Folgenabschätzungen verantwortlich ist.
Personenbezogene Daten	Alle Informationen, die sich auf identifizierbare Personen beziehen. Beispiele für personenbezogene Daten sind:
	A. Name (z. B. vollständiger Name, Mädchenname oder Aliasname);
	B. persönliche Identifikationsnummer (z. B. Sozialversicherungsnummer, Reisepassnummer, Führerscheinnummer und Nummer des Bankkontos oder der Kreditkarte);
	C. Standortdaten (z. B. Postanschrift oder E-Mail-Adresse);
	D. Online-Kennung (z. B. die Adresse des Internet-Protokolls (IP) oder der Medienzugangskontrolle (MAC));
	E. Telefonnummern (einschließlich Handynummern);
F. persönliche Merkmale, einschließlich Fotografien (z. B. des Gesichts), Röntgenbilder, Fingerabdrücke oder andere biometrische Bilder / Vorlagen personenbezogener Daten (z. B. Netzhautabtastung, Stimmensignatur, Gesichtsgeometrie);	

	G. Informationen zur Identifizierung von persönlichem Eigentum (z. B. Kfz-Kennzeichen und damit zusammenhängende Informationen);
	H. Informationen über eine Person, die mit einer der oben genannten Angaben verknüpft oder verknüpfbar sind; (z. B. Geburtsdatum, Geburtsort, Rasse, Religion, Aktivitäten, geographische Indikatoren, Beschäftigungsinformationen, medizinische Informationen, Bildungsinformationen, finanzielle Informationen);
	I. Scheinbar triviale Informationen, wie z. B. die Tatsache, dass eine Person zu einem bestimmten Zeitpunkt eine E-Mail verschickt hat, oder die Tatsache, dass eine Person Angestellter eines HES-Kunden (oder einer anderen Organisation) ist;
	J. Meinungen über eine Person (z. B. Meinungen, die in einer Referenz oder Beurteilung zum Ausdruck kommen).
Verarbeitung:	Fast alle Vorgänge, die im Zusammenhang mit personenbezogenen Daten durchgeführt werden, einschließlich:
	A. Erheben, Speicherung und Aufzeichnung;
	B. Organisation und Ordnung;
	C. Anpassung und Veränderung;
	D. Auslesen, Abfragen und Verwendung;
	E. Offenlegung und Verbreitung;
	F. Abgleich und Verknüpfung; und
	G. Einschränkung, Löschen und Vernichtung.

## Teil F

### Verzeichnis der rechtmäßigen Gründe für die Verarbeitung

- **Die Person, um die es bei den personenbezogenen Daten geht, hat in die Verarbeitung eingewilligt.**
  - Die Einwilligung muss nach eingehender Information ausdrücklich und freiwillig gegeben werden. Eine Person muss auch die Möglichkeit haben, ihre Einwilligung zu widerrufen. Weitere Informationen zur Einwilligung finden Sie in der HES-Datenschutzrichtlinie.
- **Die Verarbeitung ist erforderlich:**
  - im Zusammenhang mit einem Vertrag, den die Person abgeschlossen hat; oder
  - zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen.
- **Die Verarbeitung ist aufgrund einer rechtlichen Verpflichtung erforderlich, die für Sie gilt (mit Ausnahme einer vertraglichen Verpflichtung).**
  - Zum Beispiel müssen die Daten aufbewahrt werden, um behördlichen Anforderungen, Anforderungen an die Finanzberichterstattung oder dem Gesetz zur Bekämpfung von Bestechung und Korruption zu entsprechen.
- **Die Verarbeitung ist notwendig, um „lebenswichtige Interessen“ der Person zu schützen.**
  - Diese Bedingung gilt nur in Situationen, in denen es um Leben oder Tod geht, z. B. wenn die Krankengeschichte einer Person nach einem schweren Verkehrsunfall an ein Krankenhaus weitergegeben wird, das sie behandelt.
- **Die Verarbeitung erfolgt im Einklang mit dem Grundsatz der „berechtigten Interessen“.**
  - Das berechtigte Interesse ist die flexibelste rechtmäßige Grundlage für die Verarbeitung, aber man kann nicht davon ausgehen, dass sie immer die geeignetste ist.
  - Sie ist wahrscheinlich am geeignetsten, wenn Sie die Daten von Personen in einer Weise verwenden, die sie vernünftigerweise erwarten können und die nur minimale Auswirkungen auf die Privatsphäre hat, oder wenn es eine zwingende Rechtfertigung für die Verarbeitung gibt.
  - Der Grundsatz des berechtigten Interesses beruht auf drei Elementen. Es ist hilfreich, sich dies als einen dreiteiligen Test vorzustellen. Dazu müssen Sie: (i) ein berechtigtes Interesse feststellen; (ii) zeigen, dass die Verarbeitung notwendig ist, um es zu erreichen; und (iii) es gegen die Interessen, Rechte und Freiheiten des Einzelnen abwägen.
  - Die berechtigten Interessen können Ihre eigenen Interessen oder die Interessen Dritter sein. Dabei kann es sich um kommerzielle Interessen, individuelle Interessen oder umfassendere gesellschaftliche Vorteile handeln. Die Verarbeitung muss notwendig sein. Wenn Sie das gleiche Ergebnis auf eine angemessene andere, weniger eingreifende Weise erreichen können, gelten die berechtigten Interessen nicht.