**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** |
| **[*Relevante HES-Einheit*]** die das Projekt beantragt/durchführt |  |
| Angaben zum Projektleiter | Name:Rolle:Telefon:E-Mail: |
| 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. |  |
| Bitte beschreiben Sie so detailliert wie möglich, inwiefern Ihr Projekt die Verarbeitung personenbezogener Daten umfasst. |  |
| Wird HES personenbezogene Daten als für die Datenverwaltung Verantwortlicher oder als Auftragsverarbeiter verarbeiten? Erklären Sie in beiden Fällen, warum.  |  |
| Was ist der Zweck des Projekts? |  |
| 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 personenbezogener Daten beinhalten? |  | Mittel-Hoch |
| 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 |
|  | Welche personenbezogenen Daten werden erhoben? (bitte kreuzen Sie entsprechend J/N an) | Name: J / NAdresse: J / NGeburtsdatum: J / NRasse oder ethnische Herkunft: J / NFamilienstand: J / NInformationen zu Familie und Verwandtschaft: J / NReligion: J / NGesundheitliche Informationen: J / NSexuelle Orientierung: J / NPolitische Ansichten: J / NGenetische Informationen: J / NInformationen zu strafrechtlichen Verurteilungen: J / NInformationen über körperliche Merkmale (Größe, Gewicht usw.): J / NKreditkarten-/Bankkontonummer: J / NEigentumsinformationen (Autos, Häuser, Wohnungen, persönliches Eigentum): J / NKreditgeschichte: J / NInformationen zu sozialen Netzwerken: J / NSonstiges (bitte ausführen): J / N |
|  | Wie werden die Daten gesammelt? |  |
|  | Was ist die Verarbeitungsaktivität? |  |
|  | Ist diese Verarbeitung notwendig oder könnte die Aktivität auf eine andere Art und Weise durchgeführt werden? |  |
|  | Könnte das Projekt trotzdem erfolgreich durchgeführt werden, ohne dass einige oder alle dieser personenbezogenen Daten gesammelt werden?  |  |
|  | Über wen könnten personenbezogene Daten erhoben/verarbeitet werden? (bitte kreuzen Sie entsprechend J/N an) | Angestellte: J / NNicht-Angestellte: J / NWenn es sich um Nicht-Angestellte handelt, geben Sie bitte an, um wen es sich handelt (Kunden, Lieferanten, andere Dritte usw.): |
|  | 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. |  |
|  | Wie lange werden die personenbezogenen Daten gespeichert? |  |
| Grundlage für die Beurteilung |
|  | Werden die personenbezogenen Daten auf der Grundlage der Einwilligung der Betroffenen Person verarbeitet? Wenn ja, wie wird diese Einwilligung eingeholt? |  |
|  | Werden die personenbezogenen Daten in Erfüllung eines Vertrages mit den betroffenen Personen verarbeitet? |  |
|  | Werden die personenbezogenen Daten auf der Grundlage eines legitimen Geschäftsinteresses von HES (z. B. interne Personalverwaltung) verarbeitet? |  |
|  | Werden die personenbezogenen Daten auf der Grundlage einer anderen rechtlichen Begründung verarbeitet (siehe Teil F für ein Verzeichnis der rechtmäßigen Begründungen)? |  |
| Die Informationsflüsse |
|  | Wo werden die personenbezogenen Daten nach der Erhebung bei den betroffenen Personen gespeichert? |  |
|  | Wer wird Zugang zu den personenbezogenen Daten haben? |  |
|  | Werden Berichte erstellt, die die Verwendung und Offenlegung der personenbezogenen Daten erfordern? |  |
|  | Werden die personenbezogenen Daten an eine Nicht-HES-Einheit übertragen? Wenn ja, an welche Einheit und zu welchem Zweck? |  |
|  | Werden die personenbezogenen Daten in Länder außerhalb des Europäischen Wirtschaftsraums übertragen oder von Personen außerhalb des Europäischen Wirtschaftsraums abgerufen? |  |
|  | Wurde eine Bestandsaufnahme der personenbezogenen Daten durchgeführt? |  |
|  | 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. (unter Angabe der Art der persönlichen Daten, der Einheiten, zwischen denen sie ausgetauscht werden, der Standorte dieser Einheiten und der Speicherorte) |  |
|  | Wie lange werden die personenbezogenen Daten aufbewahrt? |  |
| Anforderungen an die Beratung |
|  | Wen werden Sie intern bezüglich der mit dem Projekt verbundenen Datenschutz- und Sicherheitsrisiken konsultieren?  |  |
|  | Haben Sie den Rat des örtlichen Compliance-Beauftragten, des Chief Compliance Officer oder der Rechtsabteilung eingeholt?  |  |
|  | Müssen Betriebsräte oder andere Arbeitnehmergremien zur Beratung herangezogen werden (wenn es um HR-/Arbeitnehmerdaten geht)?  |  |
|  | Müssen bei grenzüberschreitenden Transfers die Daten von einer anderen Rechtsordnung aus abgezeichnet werden? |  |
|  | 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  |
|  | 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:* Risiko, dass die Sicherheit der Daten kompromittiert wird;
* Risiko, dass die Personen gegen die Verarbeitung Einspruch erheben, wenn sie informiert würden;
* Risiko, dass die Genauigkeit der Daten nicht gewahrt wird;
* Risiko, dass personenbezogene Daten länger als nötig aufbewahrt werden.
 |  |
|  | 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)? |  |
|  | Gibt es ein spezifisches Compliance-Risiko? |  |
|  | 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 |
|  | 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)? |  |
|  | Wie werden wir in Bezug auf jedes oben identifizierte Risiko die Ausübung der Rechte der Betroffenen Person erleichtern (z. B. das Recht auf Zugang)? |  |
|  | Wie werden den betroffenen Personen angemessene Informationen über das Projekt und die damit verbundenen Risiken für die Privatsphäre mitgeteilt, falls erforderlich? |  |
|  | Werden diese Maßnahmen das Risiko insgesamt beseitigen oder lediglich verringern? |  |
|  | 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 |
|  | Wie werden diese Erkenntnisse in das Projekt eingebunden? |  |
|  | Wer wird dafür verantwortlich sein, dass die Ergebnisse richtig eingebunden werden?  |  |
|  | Bis wann? |  |
|  | 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. |  |

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

|  |
| --- |
| **Bestimmung des Compliance-Beauftragten vor Ort** |
| 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.