**Datenschutzfolgenabschätzung (Art. 35 DS-GVO)**

Verarbeitungstätigkeit: Personalabrechnungs- und Managementsystem

lfd. Nummer: 5010

IT-Anwendung(en): dPersonalmanagement

|  |  |  |
| --- | --- | --- |
| **Prüfpunkte**  | **Ausführungen und Hinweise**  |  |
| **Allgemeines**  |  |
| 1.  | Werden im Verfahren personenbezogene Daten automatisiert verarbeitet?  | Wenn ja, dann weiter bei 2. Wenn nein, keine weitere Überprüfung notwendig     | [x]  ja [ ]  nein  |
| **Erforderlichkeitsprüfung einer Datenschutzfolgenabschätzung („Schwellwertanalyse“)**  |  |
| 2.  | Liegt ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen oder ein Kriterium vor, welche auf die Erforderlichkeit der Durchführung einer DSFA hinweisen?   | Wenn ja, Beschreibung und weiter bei 4. Wenn nein, weiter bei 3.  siehe 5010 - SWA  | [x]  ja [ ]  nein  |
| 3.  | Liegt ein Erforderlichkeitsgrund gemäß den Vorgaben des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein vor [(Art.35 Abs. 4 DS-GVO)](https://dsgvo-gesetz.de/art-35-dsgvo/)?  | Wenn ja, Beschreibung und weiter bei 4. Wenn nein, keine DSFA notwendig.   | [ ]  ja [ ]  nein   |

|  |  |  |
| --- | --- | --- |
| **Vorbereitung**  |  |  |
| 4.  | Wurde ein geeignetes Durchführungsteam erstellt, welches objektiv und zielgerichtet arbeiten kann?  |  Das Team sollte bestehen aus, * Personal mit Erfahrungen und Kompetenzen im Bereich des Datenschutzes, des Risikomanagements und des datenverarbeitungsprogrammspezifischen Prozessmanagements
* Projektverantwortlichen und
* Projektunabhängigen, welche die Objektivität wahren können

    |       [ ]  ja  |
| 5.  | Wurde der Datenschutzbeauftragte der Einrichtung gem. [Art. 35 Abs. 2 DS-GVO](https://dsgvo-gesetz.de/art-35-dsgvo/) beratend hinzugezogen?  | [ ]  ja [ ]  nein, Begründung:   |   |
| 6.  | Wurden die Grundsätze für die Verarbeitung personenbezogener Daten betrachtet [(Art. 5 DS-GVO)](https://dsgvo-gesetz.de/art-5-dsgvo/)?  [x]  Rechtmäßigkeit [x]  Treu und Glauben [x]  Transparenz [x]  Zweckbindung [x]  Datenminimierung [x]  Richtigkeit [x]  Speicherbegrenzung [x]  Integrität u. Vertraulichkeit[x]  Rechenschaftspflicht  | [x]  ja [ ]  nein, Begründung:          |     |
| 7.  | Wurden die Rahmenbedingungen für die Durchführung festgelegt?  | *Häkchen darf nur gesetzt werden, wenn alle Unterpunkte als erledigt markiert wurden!* Erst dann weiter bei 8. |   [ ]  ja  |
| 7.1  | Wurde eine systematische Beschreibung der Verarbeitungstätigkeit mit Zweckbestimmung angefertigt?  | Die Verarbeitungsvorgänge müssen ausführlich und abschließend mit allen Datenflüssen beschrieben werden. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten. [x]  ja [ ]  nein, Begründung: siehe 5010 - DFD  |   |
| 7.2  | Wurden die Verarbeitungsvorgängen in Bezug auf ihren Zweck auf Notwendigkeit bzw. Verhältnismäßigkeit bewertet?  | [x]  ja [ ]  nein, Begründung: siehe 5010 - V |   |
| 7.3  | Wurde ein Rechte- und Rollen-Konzept bzw. Berechtigungskonzept erstellt?  | Rechte, Rollen und Pflichten der beteiligten Akteure müssen festgehalten werden.  [x]  ja [ ]  nein, Begründung: siehe 5010 - R   |     |
| 7.4 | Wurde eine Risikoprüfung mit der Schutzbedarfsfeststellung durchgeführt? | [x]  ja [ ]  nein, Begründung: siehe 5010 - Risiko  |  |
| 7.5 | Wurden die folgenden Datenschutzziele betrachtet? | Die drei unabdingbaren Schutzziele gemäß BSI wurden betrachtet:  [x] die Vertraulichkeit, [x] die Verfügbarkeit [x] die Integrität der Daten.  Darüber hinaus wurden die Gewährleistungsziele nach bestehendem Datenschutzrecht betrachtet: [x]  die Datenminimierung, [x]  die Intervenierbarkeit, [x]  die Transparenz, [x]  die Nichtverkettung.   | [x]  ja [ ]  nein  |

|  |
| --- |
| **Durchführung**  |
| 8.  | Wurden alle möglichen Risikoquellen identifiziert und mit einem Schutzziel (s. Punkt 7.5) versehen?  | Zu Risikoquellen gehören u.a. externe Angreifer, Technikversagen (berücksichtigen, dass Fehler auch erst während des laufenden Betriebs auftreten können) und menschliches Versagen des Anwenders.  siehe 5010 - Risiko   | [x]  ja [ ]  nein     |
| 9.  | Wurde jedes identifizierte Risiko bewertet? | s. Punkt 7.4 Ausführung zu Schutzbedarfsfeststellung Die Bewertung erfolgt unter der Beachtung von Eintrittswahrscheinlichkeit, Höhe und Schwere des Schadens.  siehe 5010 - Risiko  | [x]  ja [ ]  nein  |
| 10. | Wurde der Umgang mit dem jeweiligen Risiko festgelegt? | s. Punkt 7.4 Ausführung zu Umgang mit Risiken  Entscheidet man sich dafür, ein Risiko zu akzeptieren, muss eine verantwortliche Person dies unterzeichnen. Es muss überprüft werden, ob diese Entscheidung wirklich wirksam ist. Es wird die Entscheidung getroffen, alle Restrisiken zu tragen.  siehe 5010 - Risiko | [x]  ja [ ]  nein  |
| 11. | Sind Maßnahmen (Technische und Organisatorische Maßnahmen TOMs) für die Risiken abgeleitet worden? | Maßnahmen können aus bereits eingesetzten Maßnahmen abgeleitet werden. Die Maßnahmen dürfen nicht gegen rechtliche Vorgaben verstoßen und im Rahmen der zugewiesenen Ressourcen ausgewählt werden.  | [ ]  ja [ ]  nein  |
| 11.1 | Gewährleistung der **Vertraulichkeit** (z.B. über Einschränkung bei Zugriffsrechten) | Klicken Sie hier, um Text einzugeben. |  |
| 11.2 | Gewährleistung der **Verfügbarkeit** (z.B. über SSLA mit IT-Dienstleister absicherbar) | Klicken Sie hier, um Text einzugeben. |  |
| 11.3 | Gewährleistung der **Integrität** (z.B. über Berechtigungs- Zugriffskonzepte) | Klicken Sie hier, um Text einzugeben. |  |
| 11.4 | **Datenminimierung** (z.B. es werden nur notwendige Daten erhoben und verarbeitet) | Klicken Sie hier, um Text einzugeben. |  |
| 11.5 | **Intervenierbarkeit** (z.B. durch die Verarbeitung zwingend erforderlicher Daten) | Klicken Sie hier, um Text einzugeben |  |
| 11.6 | **Transparenz** (z.B. durch Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzeptes) | Klicken Sie hier, um Text einzugeben. |  |
| 11.7 | **Nichtverkettung** ( z.B. durch programmtechnische Unterlassung von Schnittstellen) | Klicken Sie hier, um Text einzugeben.  |  |
| 12. | Wurden die Rahmenbedingungen für die Umsetzung festgelegt? | Folgendes sollte festgelegt werden:  * die Verantwortlichen für die Umsetzung,
* der Zeitpunkt bis zur Umsetzung und
* die zur Verfügung stehenden Mittel

 Klicken Sie hier, um Text einzugeben.  | [ ]  ja [ ]  nein  |

|  |
| --- |
| **Umsetzung der Maßnahmen**  |
| 13.  | Konnten alle Maßnahmen umgesetzt werden?  | Wenn ja, weiter bei 16. Wenn nein, weiter bei 14.  Klicken Sie hier, um Text einzugeben.   | [ ]  ja [ ]  nein  |
| 14.  | Wurden alternative Maßnahmen identifiziert und umgesetzt?  | Wenn ja, weiter bei 16. Wenn nein, weiter bei 15.  Klicken Sie hier, um Text einzugeben.   | [ ]  ja [ ]  nein  |
| 15.  | Wurde die Aufsichtsbehörde gem. [Art. 36 DS-GVO](https://dsgvo-gesetz.de/art-36-dsgvo/) konsultiert und nach ihren Empfehlungen gehandelt?  | Bleiben Restrisiken, müssen diese aufgeführt werden.  Klicken Sie hier, um Text einzugeben.  | [ ]  ja [ ]  nein    |
| 16. | Festlegung Zeitraum / Änderungsgrund der DSFA | Klicken Sie hier, um Text einzugeben. |  |