Handreichung zur Muster-DSFA

Folgende Handreichung beschreibt den Umgang mit den Dokumenten der Muster-DSFA sowie das beabsichtigte Vorgehen. Während die Pflicht zur Durchführung einer DSFA gem. Art. 35 Abs. 1 DSGVO immer den Verantwortlichen trifft, ist dennoch vorgesehen, dass auch Auftragsverarbeiter insbesondere mit den dazu notwendigen Informationen unterstützen (Art. 28 Abs. 3 lit. f DSGVO). Zur Vereinfachung dieses Prozesses wird daher in den Dokumenten bereits die Perspektive des Verantwortlichen (also der Schulen) eingenommen, der die Verarbeitungen eines Auftragsverarbeiters beschreibt und betrachtet.

Das Vorgehen bei der Risikoanalyse ist am Vorgehensmodell ZAWAS des LfD Niedersachen orientiert. Folgende Dokumente sind anhand dieser Handreichung zu verwenden:

- Vorlage_Verarbeitungstätigkeit.docx
- Vorlage_Risikoanalyse.xlsx
- Ausgewählte BSI-Bausteine.xlsx
- Vorlage_Ergebnismitteilung_Muster-DSFA.pdf

1 Beschreibung der Verarbeitungstätigkeiten

Dokument: Vorlage_Verarbeitungstätigkeit.docx

Anhand der Vorlage sind für alle im Rahmen der Leistungserbringung durchgeführten Verarbeitungstätigkeiten die entsprechenden Verarbeitungsbeschreibungen auf Basis der Vorlage zu erstellen. Typische Verarbeitungsvorgänge sind etwa die Authentifizierung von Usern, die Bereitstellung von Lerninhalten und die Rückmeldung eines Lernstands an die Lehrkraft. Bitte legen Sie für jede Verarbeitungstätigkeit auf Basis der Vorlage ein eigenes Dokument an und nutzen Sie ggf. ein vorhandenes VVT als Grundlage. Alle auszufüllenden Felder sind in der Vorlage grün markiert.

2 Durchführung der Strukturanalyse

Dokument: Vorlage_Verarbeitungstätigkeit.docx

Vor der Durchführung der Risikoanalyse sollten die zu schützenden Objekte (Dienste, Systeme, Daten, Kommunikationsschnittstellen) der Verarbeitungstätigkeiten und deren Beziehung untereinander ermittelt werden. Vorliegend betrifft dies die IT-Systeme des Auftragsverarbeiters sowie deren Anbindung an moin.schule. Soweit vorhanden sollte die schematische Darstellung der Struktur unter Ziffer 9 der Verarbeitungsbeschreibungen eingefügt werden. Alternativ kann auf die schematische Darstellung als Anlage zu den Verarbeitungsbeschreibungen verwiesen werden.

3 Maßnahmenliste

Dokument: Vorlage_Risikoanalyse.xlsx | Ausgewählte BSI-Bausteine.xlsx

Für die Durchführung der Risikoanalyse ist eine strukturierte Dokumentation der **umgesetzten** Maßnahmen notwendige Grundlage. Diese erfolgt im Tabellenblatt UMGESETZTE MAßNAHMEN der Arbeitsmappe Risikoanalyse und sollte auf Basis der technischen und organisatorischen Maßnahmen aus dem Muster-AVV erfolgen.

Zunächst muss für jede Maßnahme eine fortlaufende Maßnahmen ID vergeben werden (Spalte A). Geben Sie außerdem zu jeder dokumentierten Maßnahme eine kurze Beschreibung ab (Spalte C). Weiterhin ist das für die Umsetzung verantwortliche Unternehmen (Spalte D) zu benennen. Jeder Maßnahme sollte außerdem der Maßnahmentyp (organisatorisch oder technisch) und ihre Art (präventiv oder detektiv) zugewiesen werden (Spalte E, F). Bitte dokumentieren Sie in Spalte G den Umsetzungsstatus der jeweiligen Maßnahme.

Für die Risikoanalyse ist es notwendig, jeder Maßnahme die Gefährdungen, gegen die sie wirkt, zuzuordnen. Als Orientierung dazu dient die Zuordnung der Anforderungen aus den IT-Grundschutz-Bausteinen des BSI zu den elementaren Gefährdungen. Im ersten Schritt ist jede Maßnahme, die Sie dokumentieren, einer konkreten Anforderung aus einem BSI-Baustein zuzuordnen. Die als grundsätzlich anwendbar bewerteten Bausteine finden Sie im Dokument Ausgewählte BSI-Bausteine.xlsx. Eine Beschreibungen der Bausteine (je ein Tabellenblatt) sowie die zugehörigen Anforderungsbeschreibungen finden Sie auf der Website des BSI.

Beispiel: Als organisatorische Maßnahme M1 wurde ein Notfallhandbuch erstellt und eingeführt. Diese Maßnahme ist Teil des Bausteins *DER.4 Notfallmanagement* und erfüllt die Anforderung *DER.4.A1 Erstellung eines Notfallhandbuchs*. Der Maßnahme M1 ist also die Anforderung *DER.4.A1* zuzuordnen (Spalte B).

4 Durchführung der Risikoanalyse

Dokument: Vorlage_Risikoanalyse.xlsx | Ausgewählte BSI-Bausteine.xlsx

Im Rahmen der Risikoanalyse sind zunächst die Risiken zu identifizieren, und die jeweiligen Schadenshöhen sowie Eintrittswahrscheinlichkeiten abzuschätzen. Der daraus abgeleitete Risikofaktor bestimmt die möglichen Ergebnisse hinsichtlich der Risikobehandlung.

4.1 Risiken identifizieren

Der erste Schritt der Risikoanalyse ist die Risikoidentifikation im Tabellenblatt RISIKOMATRIX vorzunehmen. Zur Vereinfachung haben wir Risiken, die bei der Art der betrachteten Dienstleistung typischerweise auftreten, bereits modelliert. Risiken ergeben sich aus Gefährdungen[1], die auf das betrachtete IT-System wirken und können eines, mehrere oder alle Schutzziele betreffen.

Sollten für Ihre Leistungserbringung darüberhinausgehende Risiken bestehen, legen Sie bitte weitere Tabelleneinträge an.

Die Spalten der Risikomatrix sind wie folgt zu befüllen:

Spalte A: Fortlaufende Nummer zur Bezeichnung des betrachteten Risikos

Spalte B: Verarbeitungstätigkeiten auf die das modellierte Risiko wirkt (ein oder mehrere VTs)

Spalte C: Betrachtete Gefährdung anhand der elementaren Gefährdungen des BSI

Spalte D: Beschreibung des Risiko bzw. des möglichen Ereignisses, welches selbst einen Schaden für die Betroffenen darstellt bzw. zu einem weiteren Schaden führen kann.

Spalte E: Der Risikoeigentümer kann der Verantwortliche, der Auftragsverarbeiter oder auch ein Subdienstleister sein. Es ist die Organisation, die für die Überwachung und Verwaltung eines bestimmten Risikos verantwortlich und befugt ist.

Spalte F: Risikoverursacher sind die Organisationen/Akteure/Umstände, welche auf den Eintritt des Risikos tatsächlich einwirken können.

Spalte G: Die bisher umgesetzten und auf das betrachtete Risiko wirksamen Maßnahmen sind anhand ihrer Maßnahmen-ID aus dem Tabellenblatt UMGESETZTE MAßNAHMEN zu dokumentieren. Hinsichtlich der Zuordnung von Risiko und wirksamen Maßnahmen wird auf die ausgewählten BSI-Bausteine verwiesen: Jedes Tabellenblatt zeigt die Zuordnung der Anforderungen eines Bausteins zu den elementaren Gefährdungen. Die Zuordnung zu einer BSI Grundschutz Anforderung wurde bereits in der Maßnahmendokumentation vorgenommen (Spalte B des Tabellenblatts umgesetzte Maßnahmen), sodass nun die auf die in jeweils

[1] Die Liste der elementaren Gefährdungen nach dem BSI finden Sie hier.

in Spalte C identifizierte Gefährdung hin die wirksamen Maßnahmen bestimmt werden können.

Beispiel: Die Maßnahme M1 entspricht der Anforderung DER.4.A1. Gemäß der Zuordnungstabelle wirkt diese Maßnahme auf alle Risiken, denen die Gefährdungen G. 0.18, G. 0.27 und G 0.29 zugrunde liegen. Die Maßnahmen ID M1 kann grundsätzlich für alle Risiken dieser Gefährdungen in Spalte G eingetragen werden. Dies sind vorliegend die Risiken Nr. 10, 11, 12, 24 sowie 43 bis 53.

4.2 Schadenshöhe einschätzen

Die Schadenshöhe, welche bei Realisierung des Risikos erwartet wird, ist zu bestimmen. Die Schadenshöhe wird mit einem Wert zwischen 1 und 12 bestimmt und ist wie folgt definiert. Vergleichen Sie hierzu auch das Tabellenblatt RISIKOTABELLE.

1-3 **vernachlässigbar**: Die Schadensauswirkungen sind gering und können vernachlässigt werden.
4-6 **begrenzt**: Die Schadensauswirkungen sind begrenzt und überschaubar.
7-9 **beträchtlich:** Die Schadensauswirkungen können beträchtlich sein.
10-12 **exitenzbedrohend**: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen.

Die Schadenshöhe bei Eintritt des Ereignisses wird dabei hinsichtlich aller sieben einbezogener Schutzziele betrachtet. Diese sind wie folgt definiert.

Spalte H: Verfügbarkeit: Der Zugriff auf personenbezogene Daten sowie ihre Verarbeitung müssen unverzüglich möglich sein. Weiterhin muss eine ordnungsgemäße Verwendung im vorgesehenen Prozess gesichert sein.
Spalte I: Vertraulichkeit: Keine unbefugte Person darf personenbezogene Daten zur Kenntnis nehmen oder nutzen.
Spalte J: Integrität: Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die einen Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet. Es sollen jegliche Veränderungen an den gespeicherten Daten durch unberechtigte Dritte ausgeschlossen oder zumindest so erkennbar gemacht werden, dass sie korrigiert werden können.
Spalte K: Datenminimierung bedeutet, dass die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken ist.
Spalte L: Nichtverkettung: Zu unterschiedlichen Zwecken erhobene personenbezogene Daten dürfen nicht zusammengeführt, d. h. verkettet werden.
Spalte M: Transparenz: Es muss erkennbar sein, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Spalte N: Intervenierbarkeit: Betroffene müssen ihre Rechte an ihren personenbezogenen Daten wahrnehmen können. Konkret bedeutet dies: Die Betroffenen erhalten über ihre gespeicherten Daten Auskunft, sie können Korrekturen vornehmen lassen und sie können ihre personenbezogenen Daten sperren oder löschen lassen. Die Datenverarbeitungsprozesse müssen jeweils so gestaltet sein, dass dies auch möglich ist.

Bitte vergeben Sie für jedes betrachtete Risiko für jedes Schutzziel die entsprechende Schadenshöhe zwischen 1 und 12. Die bereits umgesetzten Maßnahmen (Spalte G) in ihrer Wirkung hinsichtlich einer Verringerung der Schadenshöhe bei Eintritt des Ereignisses sind zu berücksichtigen.

4.3 Eintrittswahrscheinlichkeit einschätzen

Auf Basis der Rahmenbedingungen der Verarbeitung ist nun für jedes Risiko die Eintrittswahrscheinlichkeit zu bestimmen. Die Wahrscheinlichkeit mit der erwartet wird, dass sich das beschriebene Risiko realisiert, kann zwischen 1 und 12 liegen. Vergleichen Sie hierzu auch das Tabellenblatt RISIKOTABELLE.

1-3 **selten**: Das Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
4-6 **mittel**: Das Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
7-9 **häufig:** Das Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
10-12 **sehr häufig**: Das Ereignis tritt mehrmals im Monat ein.

Spalte O: Die Abschätzung der Eintrittswahrscheinlichkeit bezieht sich nicht auf ein konkretes Schutzziel, sondern auf die Wahrscheinlichkeit, mit der sich das betrachtete Risiko realisiert. Umgesetzte Maßnahmen (Spalte G), welche auf eine Verringerung der Eintrittswahrscheinlichkeit hinwirken, sind bei der Betrachtung einzubeziehen.

4.4 Risikofaktor und Ergebnis

Im letzten Schritt der Risikoanalyse ist der Risikofaktor zu betrachten und ein Ergebnis der Risikoanalyse zu bestimmen. Dieser Schritt erfolgt für jedes betrachtete Risiko.

Spalte P: Der Risikofaktor wird von der Tabelle automatisch bestimmt. Wie im Diagramm auf dem Tabellenblatt Risikotabelle ersichtlich wird, ergibt sich der Risikofaktor aus der erwarteten Schadenshöhe und der Eintrittswahrscheinlichkeit. Bei den Risikofaktoren ergibt sich folgende Kategorisierung:

1-4 **grün:** niedriges Risiko
5-11 **gelb**: mittleres Risiko
12-14 **rot:** hohes Risiko

Spalte Q: Hier können Erläuterungen hinsichtlich der Einschätzung der Schadenshöhen sowie der Eintrittswahrscheinlichkeit ausgeführt werden.

Spalte R: Abhängig vom nummerischen Ergebnis der Betrachtung in Form des Risikofaktors (Spalte P) ist das Ergebnis hinsichtlich des bestehenden Restrisikos vorzunehmen. Dazu ist eine geeignete Risikobehandlung zu bestimmen. Ein bestehendes Risiko kann akzeptiert, weiter durch Maßnahmen reduziert, vermieden oder transferiert werden. Restrisiken, welche nicht im gelben oder grünen Bereich liegen, sind nicht akzeptabel.

5 Mitteilung des Ergebnisses an n-21

Dokument: Vorlage_Ergebnismitteilung_Muster-DSFA.pdf

Nach Abschluss der vorgenannten Schritte und Finalisierung der notwendigen Dokumente füllen Sie bitte die Vorlage der Ergebnismitteilung vollständig aus und übermitteln Sie diese per Post an die

Landesinitiative n-21: Schulen in Niedersachsen online e. V.
Schiffgraben 27
30159 Hannover

oder per E-Mail an: dienste@moin.schule.

Die im ersten Schritt erstellten Beschreibungen der Verarbeitungstätigkeiten sind als Anlage beizufügen.

Die Risikoanalyse ist nicht zwingend zu übermitteln. Entsprechend den vertraglichen Vereinbarungen behält sich der Auftraggeber und dessen Datenschutzbeauftragter Kontrollhandlungen im Sinne des Art. 28 Abs. 3 lit. h DSGVO bei dem Auftragnehmer bezüglich der in der Ergebnismitteilung gemachten Angaben sowie der zugrundeliegenden Dokumentation vor.