audatis Datenschutz und Informationssicherheit | SERVICES

audatis® MANAGER

Anleitung: Beispiel einer DSFA für den Einsatz von Microsoft 365

Für die Umsetzung einer DSFA im Modul „Datenschutz-Folgenabschätzung“

Gültig ab Version 1.26.0

Inhalt

1 Wichtige Vorbemerkungen

Nach unserer Erfahrung ergab sich bei unseren Tests ohne den Einsatz der Beispiel-DSFA ein zeitlicher Aufwand eines datenschutzfachkundigen Teams von ca. 50 Arbeitsstunden bei der erstmaligen Durchführung einer DSFA mit diesem Anwendungsfall. Mit Einsatz des vorliegenden Beispiels reduzierte sich die Durchführung auf ca. 8 Stunden. Sie können damit somit ca. 84 % der Arbeitszeit einsparen.

Die Durchführung einer Datenschutz-Folgenabschätzung auf Basis des Art. 35 DS-GVO ist stets eine auf die individuelle Situation der jeweiligen Organisation gestützte Risikoanalyse. Diese muss die eingesetzten Mittel, die betroffenen Verarbeitungstätigkeiten und die getroffenen technische und organisatorische Maßnahmen einer Organisation in Hinblick auf Risiken für die Rechte- und Freiheiten der betroffenen Personen berücksichtigen.

Daher kann unser Beispiel einer DSFA für den Einsatz von Microsoft 365 nicht ohne Anpassung auf die betroffene Ausgangslage sinnvoll und nachhaltig eingesetzt werden.

Wie bereits im Namen ersichtlich, dient es lediglich einer beispielhaften Durchführung einer DSFA an einer beispielhaften Nutzungssituation, welche immer von den tatsächlichen Gegebenheiten vor Ort abweichen wird.

Sie müssen daher auf Basis des Beispiels immer eine individuelle Anpassung durchführen.

Aus diesem Grund sind gerade die Risikoevaluation und Risikobehandlung etwas sehr Individuelles und werden bei der Übernahme der Beispieldaten einer DSFA grundsätzlich nicht übernommen, sondern müssen entsprechend angepasst werden.

Alle Angaben und Informationen sind ohne Gewähr.

2 Inhalt des DSFA-Pakets

Im Rahmen des Kaufs stellen wir Ihnen neben der Beispielvorlage der DSFA im audatis MANAGER (ohne Risikoanalyse und Risikobehandlung) die folgenden zusätzlichen Anlagen zur Verfügung:

1. Linksammlung von weiterführenden Dokumenten und Stellungnahmen (PDF, 1 Seite)
2. Risiken hinsichtlich der Datenschutzgrundsätze gem. Art. 5 DS-GVO (MS Word, 8 Seiten)
3. Schaubild zur Beschreibung des Prozesses und Daten-Lebenszyklus (PDF, 1 Seite)
4. Einschätzung des Datenschutzbeauftragten und Freigabeverantwortlichen (MS Word, 2 Seiten)
5. Vorlage einer Richtlinie zur Datenaufbewahrung und Löschung als Löschkonzept inkl. Anlagen (MS Word, 8 Seiten)
   - 5.1 Checkliste zu Datenklassen, Dokumenten und Löschfristen (MS Excel, 1 Seite)
   - 5.2 Lösch- und Datenvernichtungsprotokoll (MS Word, 1 Seite)
6. Bericht einer Datenschutz-Folgenabschätzung zum Einsatz von Microsoft 365 (MS Word, 30 Seiten)
7. Lizenzbedingungen zur Nutzung (PDF)

Hinweis: Aus technischen Gründen erhalten Sie die Dokumente parallel zur Rechnungstellung. Diese werden nicht automatisch in der Anwendung bereitgestellt.

3 Vorbereitung zur Durchführung einer DSFA

3.1 Verarbeitungstätigkeiten dokumentieren, verknüpfen und prüfen

Bevor Sie eine DSFA im audatis MANAGER durchführen können, sollten Sie alle davon betroffenen Verarbeitungstätigkeiten im Modul: Verzeichnis der Verarbeitungstätigkeiten beschrieben haben.

Neben den Informationen zur allgemeinen Beschreibung auf dem Reiter: Allgemein müssen Sie für die Verarbeitungstätigkeiten im Rahmen einer Schwellenwertanalyse ein hohes Risiko und somit die Durchführung einer DSFA annehmen. Dies muss auf dem Reiter: Schwellenwert unten beim Punkt S.2 Risikoeinschätzung mit einem aktivierten Haken dokumentiert werden.

Anschließend muss die Verarbeitungstätigkeit geprüft und als „geprüft (OK)“ freigegeben werden.

Weiterhin sollten Sie entsprechende technische und organisatorische Maßnahmen (z.B. Ihrer Organisation sowie des Microsoft Rechenzentrums) im Modul: technische und organisatorische Maßnahmen hinterlegt und mit den betroffenen Verarbeitungstätigkeiten verknüpft haben.

Das Verknüpfen erfolgt in den Verarbeitungstätigkeiten auf dem Reiter: IT, TOM, Grundsätze. Dort können pro Verarbeitungstätigkeit auch die eingesetzten Anwendungen aus dem Microsoft 365 Bereich verknüpft werden.

Hinweis: Als Hilfestellung für die Erstellung von Verarbeitungstätigkeiten bieten wir ein Vorlagenpaket zu Microsoft 365 an, welches die wesentlichen Elemente der Verarbeitung in den Systemen bereits darstellt. Mehr Informationen dazu finden Sie unter:

https://www.audatis-manager.de/funktionen/verzeichnis-verarbeitungstaetigkeiten-vvt/

3.2 Risikomanagement aktivieren

Im nächsten Schritt sollten Sie als Systemadministrator auf der Startseite in der Rubrik Einstellungen das Risikomanagement öffnen und dort ein neues Risikomanagement für die Datenschutz-Folgenabschätzung anlegen, aktivieren und im Bedarfsfall die Kategorien für die Eintrittswahrscheinlichkeit, Schadenshöhe und das Risikoniveau anpassen.

Wir empfehlen zunächst mit der Standardeinstellung zu starten und nur bei Bedarf eine Anpassung an die Organisationsvorgaben durchzuführen.

Damit lassen sich anschließend die Risiken entsprechend des Risikoniveaus behandeln.

3.3 Anwendungen im IT-Inventar

Die von der DSFA betroffenen Anwendungen sollten, wenn noch nicht im Rahmen der Verarbeitungsdokumentation geschehen, im Modul: IT-Inventarisierung angelegt werden.

4 Anlegen einer Datenschutz-Folgenabschätzung

Zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) im audatis MANAGER gehen Sie auf das Modul „Datenschutz-Folgenabschätzung“, welches sich auf der Startseite des audatis MANAGER befindet. Um eine neue DSFA auf Basis des erworbenen Beispiels zur DSFA für Microsoft 365 anzulegen, klicken Sie zunächst auf „Datenschutz-Folgenabschätzung anlegen“.

4.1 Basisdaten

Geben Sie als Erstes eine Bezeichnung für die neue DSFA ein. Hier eignet sich beispielsweise „DSFA bei Nutzung von Microsoft 365 Produkten“.

Im darauffolgenden Punkt wählen Sie die Verarbeitungstätigkeiten aus, welche in die DSFA einbezogen werden sollen. Beachten Sie, dass hierbei ausschließlich Verarbeitungstätigkeiten angezeigt werden, die bereits im Modul „Verzeichnis der Verarbeitungstätigkeiten“ angelegt wurden und deren Schwellenwertbestimmung ergeben hat, dass für diese eine DSFA erforderlich ist.

Es muss mindestens eine Verarbeitungstätigkeit ausgewählt werden.

Zur Vorbereitung der Verarbeitungstätigkeiten siehe auch Kapitel 3.1.

4.2 Rollendefinition

Tragen Sie anschließend ein, wer der Freigabeverantwortliche und wer der Durchführungsverantwortliche sein soll.

Bei dem Freigabeverantwortlichen handelt es sich um die Person, welche den finalen DSFA-Bericht unterzeichnet und letztendlich das Gesamtrisiko der Verarbeitungsvorgänge sowie der DSFA selbst trägt. Je nach Organisationsstruktur kommt hier beispielsweise der Geschäftsführer in Frage.

Der Durchführungsverantwortliche übernimmt die Projektleitung des DSFA-Prozesses. Alle weiteren Beteiligten werden unter dem Punkt „DSFA-Team“ ausgewählt beziehungsweise eingetragen. Bei „Informationsempfänger“ werden sämtliche Personengruppen eingetragen, denen der finale DSFA-Bericht zur Verfügung gestellt wird.

4.3 Maßnahmen- und Projektplan

Wenn Sie die DSFA über unser Modul „Maßnahmen- und Projektplan“ koordinieren möchten, empfiehlt es sich, einen Haken bei „Ja, neues Projekt mit Maßnahmen + Arbeitspaketen für diese DSFA anlegen“ zu setzen. Dann werden die üblichen Schritte zur Durchführung einer DSFA auf Basis der ISO 29134 in den Maßnahmen und Projektplan aufgenommen und direkt den entsprechend ausgewählten Rollen zugewiesen.

4.4 Verwendung der DSFA-Vorlage

Um die erworbene Beispiel-DSFA zu nutzen, wählen Sie unter dem Punkt „DSFA-Vorlage“ „DSFA: Beispiel zum Einsatz von Microsoft 365 (DSFA-Vorlage audatis MANAGER)“ aus.

5 Erläuterung der Umsetzung in den DSFA-Reitern

Im Folgenden werden die einzelnen Reiter und die enthaltenen Einträge der Beispiel-DSFA kurz erläutert, um Ihnen eine Hilfestellung zur Anpassung an Ihren Sachverhalt zu geben.

Wichtig: In unseren Dokumenten und Vorlagen müssen in [eckigen Klammern] dargestellte Texte angepasst werden z.B. [Firma] bzw. geben Hinweise auf anzupassende Stellen: [Bei Bedarf anpassen].

5.1 Allgemein

Dieser Eintrag enthält Ihre in Punkt 1 getätigten Angaben.

Wichtig: Änderungen an der Zuordnung von Verarbeitungstätigkeiten können zur Überschreibung von bereits erstellten Inhalten führen. Hier erfolgt jedoch vorab ein Hinweis.

5.2 Beschreibung

5.2.1 Welche Verarbeitung ist geplant bzw. Gegenstand der DSFA?

Zunächst sind die Verarbeitungen anzugeben, welche den Gegenstand der DSFA bilden.

In unserem Beispiel werden Verarbeitungstätigkeiten, welche in Verbindung mit der Nutzung von Microsoft 365 Anwendungen eine DSFA erfordern, in umfangreichem Maße aufgelistet. Dennoch ist es ratsam, nachzuprüfen, ob alle aufgelisteten Anwendungen tatsächlich von Ihnen in Betrieb genommen werden und die Liste gegebenenfalls anzupassen.

5.2.2 Welche Zwecke werden mit der Verarbeitung verfolgt?

Hier werden sämtliche der oben genannten Verarbeitungszwecke erläutert. Sofern Sie im vorherigen Punkt Anpassungen vorgenommen haben, gehen Sie die hier genannten Zwecke noch einmal durch und nehmen gegebenenfalls weitere Anpassungen vor.

5.2.3 Wer ist Verantwortlicher für die Verarbeitung?

In diesem Punkt sind Angaben zu dem Verantwortlichen für die Verarbeitung personenbezogener Daten mittels Microsoft 365 zu tätigen. In der Regel handelt es sich hierbei um Ihre Organisation, wobei unser Beispiel Ihnen auch im Falle von gemeinsamen Verantwortlichkeiten Hilfestellung gibt.

5.2.4 Welche Auftragsverarbeiter sind an der Verarbeitung beteiligt?

Unter diesem Punkt sind sämtliche Auftragsverarbeiter auszuwählen, die mit den entsprechenden Verarbeitungstätigkeiten in Verbindung stehen. Klicken Sie hierfür auf „Zuordnung bearbeiten“. Da es sich bei Microsoft 365 um cloudbasierte Anwendungen handelt, ist (mindestens) eine Auftragsverarbeitung zwangsläufig gegeben.

Zu beachten ist hier, dass sich nur Auftragsverarbeitungen auswählen lassen, welche Sie bereits in dem Modul „Auftragsverarbeitung (AV)“ angelegt haben.

Falls dies nicht bereits geschehen ist, müssen Sie jedoch nicht erst in das entsprechende Modul wechseln. Tragen Sie in den Filter eine passende Bezeichnung samt Firma und Ort ein. Anschließend erscheint ein „+“ Symbol (s. Abb. 1). Sobald Sie auf dieses geklickt haben, wird ein neuer Eintrag angelegt, den Sie auswählen können.

Dieser wird zugleich im Modul „Auftragsverarbeitung (AV)“ angelegt, sodass Sie diesen im Anschluss ergänzen können.

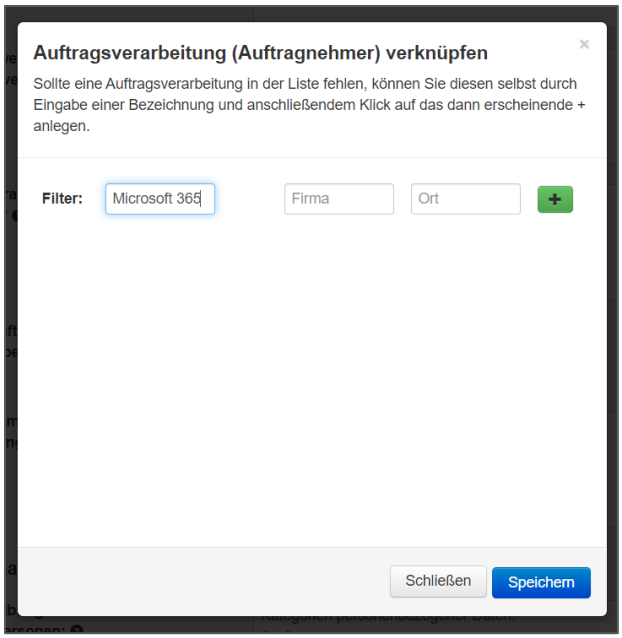

Abbildung 1: Hinzufügen einer Auftragsverarbeitung

5.2.5 Gibt es Gemeinsam Verantwortliche für die Verarbeitung?

Hier wird genauer auf das Vorliegen gemeinsamer Verantwortlichkeiten eingegangen. Sofern diese vorliegen, folgen Sie den in der Vorlage beschriebenen Anweisungen und passen Sie gegebenenfalls die bereits eingetragenen Anwendungsfälle an Ihren Sachverhalt an.

5.2.6 Beschreibung der Daten und betroffenen Personen

Geben Sie hier sämtliche Kategorien personenbezogener Daten sowie die Kategorien betroffener Personen an, welche mit den Verarbeitungstätigkeiten in Verbindung stehen.

In unserem Beispiel werden die jeweiligen Daten umfassend beschrieben. Je nach Organisationsstruktur, lassen sich möglicherweise Anpassungen hinsichtlich der Kategorien betroffener Personen vornehmen.

5.2.7 Beschreibung der Speicher- und Löschfristen

Hier sind die Speicher- und Löschfristen zu beschreiben. Sofern diese bereits in den jeweiligen Verarbeitungstätigkeiten des Moduls „Verzeichnis der Verarbeitungstätigkeiten“ eingetragen wurden, genügt ein Verweis auf dieses Verzeichnis.

Empfehlenswert ist hier zudem das Beifügen eines Löschkonzepts. Sollten Sie über kein Löschkonzept verfügen, empfehlen wir Ihnen unsere Vorlage anzupassen, welche wir Ihnen zusätzlich bereitgestellt haben (s. Anlage 5).

5.2.8 Beschreibung der Empfänger und Zugriffsberechtigten

Nennen Sie hier die zugriffsberechtigten Instanzen sowie die internen und gegebenenfalls externen Empfänger , denen die personenbezogenen Daten im Rahmen der Verarbeitung übermittelt werden. Je nach Organisationsstruktur kann es sinnvoll sein, Anpassungen an den bereits vorhandenen Einträgen vorzunehmen.

5.2.9 Beschreibung des Prozesses und Daten-Lebenszyklus

Hier ist der „Lebenszyklus“, also der Verlauf einer Verarbeitung personenbezogener Daten von der Erfassung bis zur Löschung in Form von einzelnen Prozessen zu beschreiben. Neben einer

umfassenden Beschreibung haben wir Ihnen zudem eine Skizze beigelegt, welche Sie in dem entsprechenden Eintrag hochladen können (s. Anlage 3).

5.2.10 Für die Verarbeitung notwendige Betriebsmittel (u.a. Anwendungen, IT-Systeme, etc.)

Tragen Sie hier die von Ihnen dazugehörigen Anwendungen, IT-Systeme, etc. ein. Unter „Zuordnung bearbeiten“ lassen sich Einträge auswählen, die im Modul „IT-Inventarisierung“ angelegt wurden. Ähnlich wie bei den Auftragsverarbeitungen, lassen sich hier Einträge über die Filterfunktion direkt hinzufügen.

5.2.11 Beschreibung berechtigter Interessen (sofern zutreffend)

Hier sind Ihre „berechtigten Interessen“ für die Verarbeitung durch die verwendeten Microsoft 365 Anwendungen einzutragen. Diese wurden im Rahmen unseres Beispiels umfassend ausformuliert.

5.2.12 Welche Gesetze, Normen und Standards haben Einfluss auf die Verarbeitung?

Tragen Sie hier sämtliche Rechtsnormen, Standards etc. ein, welche Einfluss auf die Verarbeitung haben könnten. Während in unserem Beispiel zahlreiche Normen von Relevanz aufgelistet wurden, könnte es sein, dass Ihre Organisation möglicherweise Normen unterliegt, die hier nicht genannt wurden. Deshalb empfehlen wir Ihnen, wenn nötig, entsprechende Ergänzungen vorzunehmen.

5.3 Anspruchsgruppen

Tragen Sie in diesem Reiter sämtliche Anspruchsgruppen ein, welche in irgendeiner Form an der DSFA mitwirken, beziehungsweise betroffen sein könnten („Anspruchsgruppe anlegen“).

Unser Beispiel enthält sechs eingetragene Anspruchsgruppen, welche abhängig von Ihrer Organisationsstruktur variieren können.

5.3.1 Bezeichnung

Hier wird die von Ihnen gewählte Bezeichnung angezeigt, welche Sie nachträglich ändern können. Zudem ist auszuwählen, ob die entsprechende Anspruchsgruppe selbst personenbezogene Daten verarbeitet oder lediglich von der Verarbeitung personenbezogener Daten betroffen sein kann.

5.3.2 Plan zur Kommunikation, Beratung und Einbindung der Anspruchsgruppe

Hier ist zu dokumentieren, in welchem Ausmaß die Anspruchsgruppe in die DSFA eingebunden wird und welche Rolle diese für die Durchführung der DSFA spielt.

5.3.3 Rückmeldung und Standpunkt der Anspruchsgruppe

Hier ist die Rückmeldung beziehungsweise der Standpunkt der kontaktierten Anspruchsgruppe hinsichtlich der DSFA zu dokumentieren. Auf Wunsch können entsprechende Dokumente hochgeladen werden.

5.3.4 Kontakt zur Anspruchsgruppe

In diesem Feld ist zu dokumentieren, wie der Kontakt zu der Anspruchsgruppe bezüglich der DSFA stattgefunden hat beziehungsweise stattfindet.

5.4 Datenschutzgrundsätze

In diesem Reiter ist einzutragen, ob die Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO im Rahmen der Nutzung von Microsoft 365 Anwendungen jeweils erfüllt werden. Diese Einträge sind möglichst detailliert zu begründen. In unserem Beispiel wird umfassend auf jegliche Punkte

eingegangen, sodass Sie nur noch die Hinweise und Anpassungsplatzhalter in [eckigen Klammern] zu beachten haben.

5.5 Betroffenenrechte

Ähnlich wie bei den Datenschutzgrundsätzen, ist in diesem Reiter einzutragen, ob die jeweiligen Betroffenenrechte (Art. 15-21 DS-GVO) erfüllt werden und es erfolgt eine entsprechende Begründung. In unserem Beispiel wird auf alle Punkte umfassend eingegangen.

Da der Umgang mit Betroffenenanfragen jedoch in jeder Organisation variiert, haben wir Ihnen zu jedem Punkt einen Platzhalter zur Verfügung gestellt, in dem Sie Ihre eigenen Prozesse für entsprechende Betroffenenanfragen beschreiben können.

Die Punkte 5.6 sowie 5.7 dieses Reiters betreffen Formalitäten, welche die Einhaltung der Betroffenenrechte mittelbar oder unmittelbar betreffen. Unser Beispiel enthält zu jedem dieser Punkte jeweils eine umfassende Stellungnahme, die lediglich das Befüllen der Platzhalter zu Ihrem Organisationsnamen erfordert.

5.6 Risikoidentifizierung, Risikoanalyse sowie Risikobehandlung

In den folgenden drei Reitern sind mögliche Risiken in Bezug auf die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit einzutragen. Neben Beispielen für mögliche Risiken mit entsprechender Risikoanalyse und Risikobehandlung in diesen Bereichen, enthält unsere Beispiel-DSFA zudem selbiges für Risiken im Hinblick auf die Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO. Letzteres ist in Anlage 2 zu finden, welches Sie ebenfalls an Ihre Organisation anpassen können.

Risiken, die in einer Organisation auftreten können, sind individuell zu betrachten, weshalb die genannten Beispiele lediglich als Hilfestellung zum Anlegen entsprechender Risiken dienen sollen.

Zu Verständlichkeitszwecken werden die einzutragenden Felder am Beispiel des Risikos „*Unbefugter Zugriff auf den Microsoft 365 Account*“ erläutert.

5.6.1 Risikoidentifizierung

Reiter „Risiko: Vertraulichkeit“ -> „1. Unbefugter Zugriff auf den Microsoft 365 Account“

5.6.1.1 Bezeichnung

Hier ist die Risikobezeichnung zu sehen, welche beim Anlegen des Risikos gewählt wurde.

5.6.1.2 Risikoquelle

Wählen Sie hier aus, von welcher Quelle das Risiko ausgeht. Beispielsweise kann für das Risiko des unbefugten Zugriffs auf den Microsoft Account die Auswahl „Menschliche Quelle (extern): vorsätzliches Handeln“ in Betracht kommen.

5.6.1.3 Aktion

Wählen Sie unter diesem Punkt die Aktion aus, welcher die Risikohandlung am ehesten zuzuordnen ist. Wenn sich jemand unbefugt Zugriff auf das Microsoft Konto eines Mitarbeiters verschafft, könnte es sich beispielsweise um eine Form der Spionage handeln.

5.6.1.4 Betriebsmittel

Wählen Sie hier das Betriebsmittel aus, welches von dem Risiko betroffen ist. Im Falle einer Spionage sowie für weitere Risiken der Kategorie „Vertraulichkeit“, liegt das Betriebsmittel „Informationen“ häufig nahe. Schließlich zielen entsprechende Risiken auf eine unbefugte Informationsbeschaffung ab.

5.6.1.5 Gefährdungsszenario

Beschreiben Sie hier das Szenario, durch welches das Risiko ausgelöst wird. Neben zahlreichen weiteren Beispielen, die in unserem Paket enthalten sind, wird im Folgenden auf das Szenario

eingegangen, bei dem ein Hackerangriff gegen Ihre Organisation erfolgt. Beachten Sie zudem, dass es für ein Risiko mehrere Gefährdungsszenarien geben kann. Aus diesem Grund enthält unsere Beispiel-DSFA zu einigen Risiken mehrere Gefährdungsszenarien.

So kann es empfehlenswert sein, ein Risiko in mehrere Kategorien einzuteilen, die jeweils ähnliche Gefährdungsszenarien beinhalten. Diese einzelnen Unterteilungen legen Sie dann jeweils als eigenes Risiko im audatis MANAGER an.

Dieses Vorgehen erleichtert es Ihnen, eine Risikoanalyse und die Dokumentation der Risikobehandlung im audatis MANAGER durchzuführen.

5.6.2 Risikoanalyse

Die folgenden Punkte werden Ihnen angezeigt, wenn Sie im Modul „Risikomanagement“ ein Risikomanagement mit dem Typen „Datenschutz-Folgenabschätzung“ angelegt haben. Weil die im entsprechenden Modul erstellten Risikomatrizes in jeder Organisation unterschiedlich sein können, werden die dazugehörigen Einträge unseres Beispiels nicht automatisch in die Risikoanalyse übernommen.

Diese sind jedoch in unserem kompletten DSFA-Bericht zu sehen (s. Anlage 6) und wurden farblich markiert. Das Beispiel des Hackerangriffs findet sich in Punkt 6.1 des DSFA-Berichts.

Wichtig: Bekommen Sie den Hinweis, dass kein Risikomanagement aktiviert ist, muss das Risikomanagement vom Typ: Datenschutz-Folgenabschätzung mit entsprechenden Einstellungen im Modul: Risikomanagement vom Systemadministrator aktiviert werden.

In diesem Beispiel haben wir die Standardvorlage unverändert verwendet.

5.6.2.1 Umgesetzte oder geplante Maßnahmen zur Bewältigung des Gefährdungsszenarios

Sollten den Verarbeitungstätigkeiten, welche Sie im Reiter „Allgemein“ im Punkt „Einbeziehung folgender Verarbeitungstätigkeiten:“ ausgewählt haben, technische und organisatorische Maßnahmen (TOMs) zugeordnet worden sein, stehen Ihnen diese zur Auswahl für die Risikobewältigung bereit.

5.6.2.2 Welche Eintrittswahrscheinlichkeit wird hierfür angenommen?

Wählen Sie hier die Eintrittswahrscheinlichkeit für obiges Gefährdungsszenario unter Berücksichtigung der bereits umgesetzten technischen und organisatorischen Maßnahmen aus. Die Auswahlmöglichkeiten wurden zuvor im Modul: Risikomanagement festgelegt.

Begründen Sie zudem Ihre Auswahl. In unserer Beispiel-DSFA wird hierbei auf das Szenario des Hackerangriffs eingegangen (s. Anlage 6). Dabei haben wir die Eintrittswahrscheinlichkeit als „Mittel“ eingestuft. Je nach der IT-Infrastruktur Ihrer Organisation, kann die Eintrittswahrscheinlichkeit höher oder aber geringer ausfallen.

5.6.2.3 Welche Schadensauswirkung ist für die betroffenen Personen zu erwarten?

Bewerten und beschreiben Sie hier das Ausmaß des Schadens im Hinblick auf das Gefährdungsszenario für betroffene Personen. Als Hilfestellung können Sie sich an dem Beispieleintrag aus unserem Vorlagenpaket orientieren (s. Anlage 6). Auch hier haben wir uns für „Mittel“ entschieden.

5.6.2.4 Risikoniveau in der Risikomatrix

Anhand Ihrer Auswahl hinsichtlich der Eintrittswahrscheinlichkeit und Schadensauswirkung, wird das bewertete Risiko grafisch auf der von Ihnen definierten Risikomatrix (Modul: Risikomanagement) dargestellt.

5.6.2.5 Risikoeigentümer

Legen Sie hier eine Person fest, welche für die entsprechende Risikobehandlung verantwortlich ist und im schlimmsten Fall das Risiko trägt.

Hier könnte zum Beispiel der Leiter Ihrer IT-Abteilung in Betracht kommen. Möglicherweise könnte auch der Geschäftsführer Ihrer Organisation als Risikoeigentümer eingeordnet werden.

5.6.3 Risikobehandlung

Reiter „Risikobehandlung“ -> „1. Risiko: Unbefugter Zugriff auf den Microsoft 365 Account“

5.6.3.1 Art der Risikobehandlung

Wählen Sie hier die Art der Risikobehandlung aus. Sie haben die Wahl zwischen Risikoakzeptanz („Das Risiko lässt sich nicht verhindern oder eindämmen, allerdings nehme ich es in Kauf“), Risikoreduktion („Ich senke die Wahrscheinlichkeit des Risikoeintritts“), Risikoübertragung („Ich übertrage das Risiko auf jemanden, der es tragen kann, wie beispielsweise eine Versicherung“) und Risikovermeidung („Ich sorge dafür, dass dieses Risiko nicht eintreten kann“).

Wichtig: Je nach Einstellungen im Modul: Risikomanagement sind die Auswahlmöglichkeiten vorhanden bzw. abhängig vom Risikoniveau definiert. Für das Beispiel des Hackerangriffs kommt eine Maßnahme zur Risikoreduktion in Betracht.

5.6.3.2 Beschreibung

Beschreiben Sie hier, wie Sie das identifizierte Risiko behandeln werden. Orientieren Sie sich hierbei unter anderem an den Beispielen aus Anlage 6.

Sollten Sie bei der Art der Risikobehandlung „Risikoreduktion“ ausgewählt haben, können Sie Maßnahmen zur Risikoreduktion anlegen. Klicken Sie hierfür aus das „+“ Symbol. Diese Maßnahmen werden auch im Maßnahmen- und Projektplan für diese DSFA hinterlegt.

5.6.3.3 Maßnahmen zur Risikoreduktion: Bezeichnung

Geben Sie hier die Bezeichnung für die Maßnahme ein. Orientieren Sie sich hierbei unter anderem an unseren Beispielen (s. Anlage 6). Als Maßnahme zur Risikoreduktion ist in unserem Beispiel das regelmäßige Durchführen von Sicherheitsupdates gelistet.

5.6.3.4 Maßnahmen zur Risikoreduktion: Beschreibung

Beschreiben Sie hier die entsprechende Maßnahme ausführlicher. Auch hierfür haben wir in unserem DSFA-Beispiel die zuvor genannte Maßnahme genauer erläutert (s. Anlage 6).

5.6.3.5 Maßnahmen zur Risikoreduktion: Verantwortlich für die Umsetzung

Geben Sie hier den Fachverantwortlichen für die Umsetzung der Maßnahme an. Auch hier kommt im Beispiel der Leiter der IT-Abteilung in Betracht.

5.6.3.6 Maßnahmen zur Risikoreduktion: Umsetzung bis

Hier können Sie eine Deadline für die Umsetzung der Maßnahme festlegen. Im Falle von regelmäßigen Sicherheitsupdates, kann dieses Feld grundsätzlich leer gelassen werden, da es sich hierbei um einen stetigen Prozess handelt. Es kann jedoch die Einführung einer solchen Maßnahme bis zu einem Stichtag damit dokumentiert werden.

5.6.4 Umsetzung der Risikobehandlung

Nachdem Sie sämtliche Risiken identifiziert und alle dazugehörigen Maßnahmen zur Risikobehandlung festgelegt haben, müssen diese umgesetzt werden.

Nachdem dies geschehen ist, gehen Sie zurück zum Reiter „Risikobehandlung“.

Unter den eingetragenen Maßnahmen zur Risikobehandlung sind zwei Schaltflächen zu sehen. Zum einen die Schaltfläche mit der Bezeichnung „Risikoanalyse nach Risikobehandlung erneut

durchführen“ und zum anderen „Risikoanalyse und Risikobehandlung abschließen“ (s. Abb. 2). Diese beiden Buttons lassen sich jedoch erst anklicken, wenn zu jedem identifizierten Risiko mindestens eine Risikobehandlung angelegt wurde.

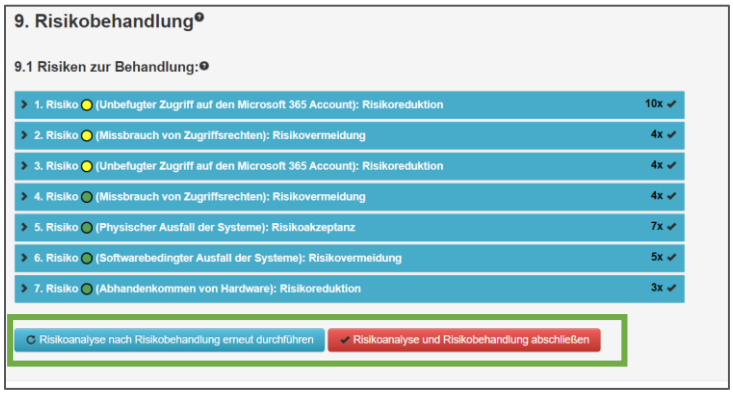

Abbildung 2: Buttons zur Risikobehandlung

5.6.4.1 Risikoanalyse nach Risikobehandlung erneut durchführen

Sofern Sie im Rahmen der Risikoanalyse hohe Risiken definiert haben, welche Sie behandeln müssen, um auf ein geringes oder mittleres Risikoniveau zu kommen, sollten Sie nach erfolgreicher Risikobehandlung, auf „Risikoanalyse nach Risikobehandlung erneut durchführen“ klicken.

Gehen Sie nun die Risiken erneut durch und analysieren die einzelnen Risiken nach der Umsetzung der risikoreduzierenden Maßnahmen erneut. Bewerten Sie die jeweilige Eintrittswahrscheinlichkeit und vergleichen Sie die Werte mit denen, die Sie bei Ihrer vorherigen Risikoanalyse ermittelt haben. Die vorherigen Bewertungen werden Ihnen neben dem Auswahlfeld in Klammern angezeigt (s. Abb. 3).

Abbildung 3: Wiederholen der Risikobehandlung

Im Falle einer „erfolgreichen Risikobehandlung“ müssen die ermittelten Werte geringer geworden sein. Ist dies nicht der Fall, wiederholen Sie die Abläufe so lange, bis die Werte so gering wie möglich und damit aus Sicht des Artikel 35 DS-GVO akzeptabel sind.

5.6.4.2 Risikoanalyse und Risikobehandlung abschließen

Nachdem Sie Ihre Risiken erfolgreich behandelt haben, klicken Sie auf den Button „Risikoanalyse und Risikobehandlung abschließen“.

Nun lassen sich die getätigten Einträge in den Reitern „Risiko: …“ und „Risikobehandlung“ nicht mehr ändern. Wenn Sie diese dennoch ändern beziehungsweise eine erneute Risikobehandlung durchführen möchten, klicken Sie auf den Button „Risikoanalyse und Risikobehandlung entsperren und erneut durchführen“. Dieser erscheint erst, nachdem Sie auf „Risikoanalyse und Risikobehandlung abschließen“ geklickt haben.

5.7 Dateien

Laden Sie hier gegebenenfalls Dokumente hoch, welche aus Ihrer Sicht zum besseren Verständnis der DSFA beitragen. Beispielsweise könnte dies unter anderem ein Löschkonzept sein, für welches wir Ihnen eine Vorlage in den Anlagen 5, 5.1 und 5.2 bereitgestellt haben.

Hinweis: Wenn Sie in der Group-Version des audatis MANAGER arbeiten, werden die initial von Ihnen hochgeladenen Dateien auch auf andere Mandanten übernommen, wenn die DSFA kopiert wird.

6 Prüfung der DSFA durch den Datenschutzbeauftragten

Nachdem sie alle erforderlichen Informationen bearbeitet und sämtliche der beschriebenen Prozesse durchgeführt haben, soll die DSFA zur Prüfung an eine berechtigte Person, wie Ihren Datenschutzbeauftragten (DSB), weitergegeben werden.

Scrollen Sie hierfür (unabhängig von dem ausgewählten Reiter) ganz nach unten und setzen Sie einen Haken bei „Die Daten zu den Datenschutz-Folgenabschätzung sind komplett dokumentiert und können nach dem Speichern an die berechtigten Benutzer zur Überprüfung übermittelt werden.“. Klicken anschließend auf „Datenschutz-Folgenabschätzung speichern“.

Der DSB wird daraufhin per E-Mail benachrichtigt und soll die einzelnen Einträge der DSFA prüfen.

Die Prüfung kann er in dem für ihn erscheinenden Reiter „Prüfung“ in den einzelnen Kategorien 10.- bis 10.6 vornehmen. Sollte er die DSFA als mangelhaft bewertet haben, gehen Sie die Prüfungsschritte des Prüfers durch und verbessern Sie die von ihm bemängelten Punkte.

Geben Sie die DSFA im Anschluss erneut zur Prüfung frei. Wiederholen Sie den Prozess so lange, bis die DSFA als „geprüft (OK)“ eingestuft wurde.

Für das Feld zu „Rat des Datenschutzbeauftragten“ haben wir Ihnen in Anlage 4 unseres Beispiels eine datenschutzrechtliche Bewertung bereitgestellt, an der sich Ihr DSB orientieren oder sie gänzlich übernehmen kann.

7 Freigabe der DSFA durch den Verantwortlichen

Nachdem eine erfolgreiche Prüfung durchgeführt wurde, wird für Sie der Reiter „Freigabe“ sichtbar.

Der Freigebeverantwortliche soll dort nun die entsprechenden Felder ausfüllen.

Wenn Sie sich an unserer Beispiel-DSFA orientieren und Ihre eigene Prüfung (beispielsweise die Risikobewertung) nichts anderes ergeben hat, können Sie einen Haken bei „Der Verantwortliche folgt dem Rat des DSB gem. Ziffer 10.8“ setzen.

Je nach getätigter Bewertung können Sie nun entscheiden, was Sie unter dem Punkt „Nach Durchführung der DSFA bestehen aus Sicht des Verantwortlichen:“ wählen.

In das Feld zu „Stellungnahme des Verantwortlichen“ können Sie den entsprechend vorformulierten Text aus Anlage 4 unseres Beispiels übernehmen.

Geben Sie anschließend das Datum der Freigabe an, wählen Sie gegebenenfalls den Verantwortlichen aus, durch welchen eine Freigabe erfolgt ist und geben Sie bei Bedarf das Datum der nächsten Aktualisierung der DSFA an.

Wählen Sie unter „Ergebnis der Überprüfung“ aus, ob Sie die DSFA freigeben oder nicht.

Damit ist die DSFA komplett und kann als Bericht in der Übersicht heruntergeladen werden. Sollten weiterhin hohe Risiken verbleiben, können Sie diesen Bericht mit Ihren entsprechenden Anlagen bei der Aufsichtsbehörde zur Konsultation einreichen. Dies sollte stets in enger Abstimmung mit Ihrem Datenschutzbeauftragten erfolgen.