Anlage 3

Leistungsbeschreibung

1. Allgemeine Produktbeschreibung

Als „SaaS-Anwendung“ steht der PrivacyPilot seinen Kunden über das Internet zur Nutzung bereit. Das System verhilft den Nutzern, die Anforderungen des Datenschutzrechts, der Informationssicherheit und etwaiger weiterer Standards zu erfüllen. Dabei ermöglicht das System nach Wahl des Kunden, anerkannten Standards (z.B. Standard-Datenschutzmodell der deutschen Aufsichtsbehörden, IT-Grundschutzkompendium des BSI) zu folgen und/oder eigene Standards zur weiteren Verwendung in das System zu integrieren.

2. Funktionalitäten und Produktbestandteile

Die Softwarelösung weist vier Module auf: das Basis-Modul, das Compliance-Modul, das Reporting-Modul sowie das Marktplatz-Modul. Zudem beinhaltet die Software eine Vielzahl spezieller Funktionen sowie einen verwaltenden Bereich für Benutzerdaten.

2.1. Basis-Modul

Das Basis-Modul bietet Funktionalitäten zur zentralen und strukturierten Stammdatenverwaltung von innerhalb der Softwarelösung verwendbaren Datenelementen. Es handelt sich bspw. um Listeneinträge, Sammlungen, technische und organisatorische Maßnahmen (TOM) und Kontakte. Mit Ausnahme der Liste von Ländern sowie den BSI-Gefährdungen können die Datenelemente durch einen berechtigten Nutzer angelegt, verändert oder gelöscht werden, sofern es sich nicht um über den Marktplatz abonnierte Elemente handelt (siehe „Marktplatz-Modul“). Anhand von Verwendungsnachweisen kann in ausgewählten Bereichen nachvollzogen werden, wo innerhalb des Compliance-Moduls die im Basis-Modul verwalteten Daten verwendet werden. Anlässlich des erstmaligen Aufsetzens eines Tenants stimmt der Auftragnehmer gemeinsam mit dem Auftraggeber ab, welche schon auf Auftragnehmerseite vorhandenen Listen, Sammlungen und TOM-Kataloge dem Auftraggeber im Basis-Modul initial – ggfs. über das Marktplatz-Modul – zur Verfügung gestellt werden.

2.1.1. Listenelemente

Das System weist folgende Listenelemente auf:

- BSI-Gefährdungen,
- Ausnahmen (Drittlandtransfer),
- Garantien (Drittlandtransfer),
- Länder,
- Löschereignisse und
- Rollen.

2.1.2. Sammlungen

Im Unterschied zu Listenelementen (s.o.) können Sammlungen nach definierbaren Ordnungskriterien strukturiert werden. Das System weist folgende Sammlungen auf:

- Attribute – Betroffene,
- Attribute – Datenkategorien,
- Attribute – Zwecke,
- AV-Dienstleistungen,
- benutzerdefinierte Risiken,
- Betroffene,
- Betroffenenrechte,
- Datenkategorien,
- Grundsätze,
- Informationsmittel,
- Interne Empfänger,
- Label-Kataloge,
- Quellen,
- Rechtsgrundlagen,
- Schwellwertanalyse,
- Systeme und
- Zwecke.

2.1.3. TOM-Kataloge

Im Bereich „TOM-Kataloge“ können frei definierbare TOM-Kataloge angelegt werden. TOM-Kataloge bestehen aus mindestens einem Ordner sowie einer beliebigen Anzahl darin enthaltener technisch-organisatorischer Maßnahmen. Die technisch-organisatorischen Maßnahmen können nach diversen Merkmalen klassifiziert werden. Neben allgemeinen Angaben (z.B. „spezifisch“) können die TOMs auch nach komplexen Standards beschrieben werden (z.B. SDM, BSI). Zudem kann auch auf die unter „Sammlungen -> Benutzerdefinierte Risiken“ gepflegten Risiken zurückgegriffen werden. Insoweit bietet das System u.a. anklickbare Matrizen an, die einem Farbschema folgen können, etwa zur Festlegung von Potentialen zur Mitigation von Risiken.

2.1.4. Kontakte

Im Bereich „Kontakte“ können Einzelkontakte und Kontaktkategorien angelegt, verändert und gelöscht werden. Den Kontakten lassen sich weitere Kontakte zuordnen (z.B. DSB, Vertreter). Auch können Angaben zu Zwecken, Rollen und bei Drittlandkontakten Ausnahmen und Garantien hinzugespeichert werden.

2.2. Compliance-Modul

Das Compliance-Modul stellt diverse Funktionalitäten zur Erfüllung von Anforderungen allgemein gültiger und/oder nutzerseitig gewählter Standards bereit. Nahezu alle im Compliance-Modul zu pflegenden Informationen stammen aus dem Basis-Modul (s.o.).

Das Compliance-Modul weist ein Dashboard auf, über welches die Nutzer einen Überblick über ihre Organisation und insoweit relevante Bearbeitungsstände erhalten.

Mittels des „Hierarchiebrowsers“ können Nutzer ihre individuelle Organisation unter Einbeziehung einer beliebigen Anzahl von rechtlich selbstständigen Einheiten und internen Bereichen in bis zu 14 hierarchischen Ebenen abbilden. Den Hierarchieeinheiten kann ein Kontakt mit seinen weiteren Kontakten zugewiesen werden. Zudem können die für eine ausgewählte Hierarchieeinheit existierenden Bearbeitungsstände angezeigt werden.

Im System können unterschiedliche, voneinander unabhängige „Master“ gepflegt werden (z.B. „VT-Master“, „Risiko-Master“, „TOM-Master“ und „AV-Master“). Diese können ggfs. miteinander verknüpft und so in einen inhaltlichen Bezug zueinander gebracht werden. Die Master sind einer oder mehreren Hierarchieeinheiten zugeordnet.

2.2.1. VT-Master

Ein VT-Master besteht aus den

- Verarbeitungstätigkeiten

und optional den folgenden, einzelnen Verarbeitungstätigkeiten zugewiesenen Elementen:

- Löschfristen,
- Externe Empfänger/Gemeinsam Verantwortliche,
- Interne Empfänger,
- Quellen,
- Informationspflichten,
- Grundsätze (Prüfung über im Basis-Modul definierte Assessments),
- Rechtsgrundlagen,
- Betroffenenrechte (Prüfung über im Basis-Modul definierte Assessments),
- Schwellwertanalyse (Prüfung über im Basis-Modul definierte Assessments),
- Risiko-Master und
- TOM-Master.

Zudem können Vorlagen und verbundene VT-Master hinzugefügt sowie Kopien eines VT-Masters erstellt werden. Mittels der „Gilt auch für“-Funktion kann ein VT-Master auch mehreren Hierarchieeinheiten zugewiesen werden.

Oben genannte Verarbeitungstätigkeiten sind innerhalb eines Masters einzigartig und bestehen zwingend aus folgenden Elementen:

- System,
- Betroffener,
- Datenkategorie und
- Zweck.

Optional kann sich der Nutzer zu diesen vier Datenelementen zusätzliche im Basis-Modul gepflegte Informationen anzeigen lassen (z.B. Beschreibung, Attribute) und mittels eines Freitextfeldes einen „Kontext“ zur Verarbeitungstätigkeit dokumentieren.

Die definierten Verarbeitungstätigkeiten dienen als Anknüpfungspunkt für alle weiteren oben genannten Elemente, mit der Folge, dass diese immer einen unmittelbaren Bezug zur jeweiligen Verarbeitungstätigkeit haben.

Bei der Bestimmung relevanter Verarbeitungstätigkeiten und der anschließenden Verknüpfung mit den weiteren Elementen wird nahezu ausschließlich auf strukturierte Daten aus dem Basis-Modul zurückgegriffen.

Innerhalb der VT-Master existieren diverse Filtermöglichkeiten, die es dem Nutzer ermöglichen, die Verarbeitungstätigkeiten sowie die damit verknüpften weiteren Elemente zu filtern und somit eine Zielauswahl zu bilden, die separat bearbeitet werden kann. Diese Bearbeitung erfolgt über ein zusätzliches Auswahlfenster, das die Einbeziehung unterschiedlicher Konstellationen von Daten erlaubt. Die dergestalt im Auswahlfenster selektierten Informationen können optional über Massenzuweisungen mit einer Vielzahl unterschiedlicher Verarbeitungstätigkeiten verknüpft werden.

Soweit Vorlagen zum zu bearbeitenden VT-Master hinzugefügt werden, kann im Wege der Erstellung von Verarbeitungstätigkeiten und der Verknüpfung der Datenelemente auf die Vorlagen zugegriffen werden, um einzelne oder ganze Datensätze in den zu bearbeitenden VT-Master zu übernehmen.

Mithilfe von Schiebereglern können innerhalb der VT-Master einzelnen Verarbeitungstätigkeiten ebenso wie den dazugehörigen Kernanforderungen Genehmigungsstati (genehmigt, nicht genehmigt, unbearbeitet) zugewiesen werden.

2.2.2. Risiko-Master

Mittels der Risiko-Master kann für ein beliebiges Szenario, für einen bestimmten VT-Master oder für ausgewählte Verarbeitungstätigkeiten innerhalb eines VT-Masters eine Risikobewertung vorgenommen werden. Das Risikoobjekt, auf welches Bezug genommen wird, kann innerhalb des Basis-Moduls frei definiert und im Wege der Bearbeitung des Risiko-Masters ausgewählt werden (z.B. Gefährdungen des BSI-Grundschutzkompendiums, Gewährleistungsziele des Standard-Datenschutzmodells).

Optional kann der Nutzer eine Risiko-Bewertung gemäß der Methodik des „SDM-Würfels“ des Standard-Datenschutzmodells (SDM) der deutschen Aufsichtsbehörden durchführen. Dabei wird eine interaktive Matrix verwendet, welche eine Spezifizierung des Risikos mittels

Farbindikatoren im Hinblick auf die Ebenen, Verarbeitungsvorgänge und Gewährleistungsziele zulässt. Die Matrix bietet verschiedene Funktionalitäten, um mehrere Risikoszenarien einheitlich zu bewerten.

Darüber hinaus kann eine Risikobewertung im Hinblick auf die Gefährdungen des BSI-Grundschutzkompendiums durchgeführt werden, wobei ebenfalls Farbindikatoren zur Risikobestimmung zugewiesen werden können. Nach dem gleichen Prinzip können beliebig viele weitere Risikobewertungen mit unterschiedlichem Risikoobjekt erfolgen, soweit Letztere im Basis-Modul angelegt wurden.

Optional kann der Nutzer bei der Auswahl der Farbindikatoren hilfsweise auf eine Risiko-Bewertungs-Matrix zurückgreifen. Zudem können die einzelnen Risikobewertungen mit Freitextfeldern kommentiert und erläutert werden. Des weiteren können Kopien eines Risiko-Masters erstellt werden. Mittels der „Gilt auch für“-Funktion kann ein Risiko-Master zudem mehreren Hierarchieeinheiten zugewiesen werden. Anhand von Verwendungsnachweisen kann nachvollzogen werden, in welchen VT-Mastern der jeweilige Risiko-Master Verwendung findet.

2.2.3. TOM-Master

Ein TOM-Master besteht aus einer beliebigen Anzahl technisch-organisatorischer Maßnahmen (TOM), die innerhalb des Basis-Moduls angelegt und gepflegt werden. Soweit innerhalb des Basis-Moduls eine Klassifizierung der TOM hinsichtlich ihres (abstrakten) „Risiko-Mitigations-Potentials“ erfolgt (z.B. gemäß SDM oder BSI-Grundschutzkompendium), werden diese Klassifizierungen in den jeweiligen TOM-Master übernommen.

Der Nutzer kann optional eine zuvor im Basis-Modul vorgenommene (abstrakte) Risiko-Mitigations-Bewertung an die konkreten Gegebenheiten anpassen oder, falls eine Vorklassifizierung aus dem Basis-Modul fehlt, eine Risiko-Mitigations-Bewertung für den geltenden Ist-Zustand neu erstellen. Soweit der Nutzer eine zuvor im Basis-Modul vorgenommene Klassifizierung innerhalb eines TOM-Masters ändert, ist dies innerhalb der Klassifizierungszelle anhand eines kleinen Dreieck-Symbols ersichtlich, das die ursprüngliche Klassifizierung aus dem Basis-Modul anzeigt.

Ähnlich zu den Risiko-Mastern (s.o.) bietet das System für eine Klassifizierung gemäß der Methodik des „SDM-Würfels“ des Standard-Datenschutzmodells eine interaktive Matrix, welche eine Spezifizierung nunmehr des Risiko-Mitigations-Potentials mittels Farbindikatoren im Hinblick auf die Ebenen, Verarbeitungsvorgänge und Gewährleistungsziele zulässt. Die Matrix bietet verschiedene Funktionalitäten, um mehrere Risiko-Mitigations-Potentiale einheitlich zu bewerten.

Darüber hinaus kann eine Risiko-Mitigations-Bewertung im Hinblick auf die Gefährdungen des BSI-Grundschutzkompendiums ebenfalls mittels Farbindikatoren durchgeführt werden. Nach dem gleichen Prinzip können beliebig viele weitere Risiko-Mitigations-Bewertungen mit unterschiedlichem Risikoobjekt erfolgen, soweit Letztere im Basis-Modul angelegt wurden.

Optional kann der Nutzer bei der Auswahl der Farbindikatoren hilfsweise auf eine Risiko-Mitigations-Matrix zurückgreifen. Zudem können Kopien eines TOM-Masters erstellt werden.

Mittels der „Gilt auch für“-Funktion kann ein TOM-Master optional mehreren Hierarchieeinheiten zugewiesen werden. Anhand von Verwendungsnachweisen kann nachvollzogen werden, in welchen VT-Mastern der jeweilige TOM-Master Verwendung findet.

2.2.4. AV-Master

Ein AV-Master besteht aus

- Dienstleistungen

und optional den folgenden, den einzelnen Dienstleistungen zugewiesenen Elementen:

- Verantwortliche und
- TOM-Master.

Zudem können verbundene AV-Master hinzugefügt sowie Kopien eines AV-Masters erstellt werden. Mittels der „Gilt auch für“-Funktion kann ein AV-Master auch mehreren Hierarchieeinheiten zugewiesen werden.

Die definierten Dienstleistungen dienen als Anknüpfungspunkt für alle weiteren oben genannten Elemente, mit der Folge, dass diese immer einen unmittelbaren Bezug zur jeweiligen Dienstleistung haben. Bei der Bestimmung relevanter Dienstleistungen und der anschließenden Verknüpfung mit den weiteren Elementen wird ausschließlich auf strukturierte Daten aus dem Basis-Modul zurückgegriffen.

Innerhalb der AV-Master existieren diverse Filtermöglichkeiten, die es dem Nutzer ermöglichen, die Dienstleistungen ebenso wie die damit verknüpften weiteren Elemente zu filtern und somit eine Zielauswahl zu bilden, die separat bearbeitet werden kann. Diese Bearbeitung erfolgt über ein zusätzliches Auswahlfenster, das die Einbeziehung unterschiedlicher Konstellationen von Daten erlaubt. Die dergestalt im Auswahlfenster selektierten Informationen können optional über Massenzuweisungen mit einer Vielzahl unterschiedlicher Dienstleistungen verknüpft werden.

2.2.5. Folgenabschätzungen

Eine Folgenabschätzung bezieht sich immer auf eine oder mehrere Verarbeitungstätigkeiten eines VT-Masters sowie einen Risiko-Master. Ferner ist ein Prüfstandard auszuwählen. Dieser entspricht zwingend einer der in den Risiko-Mastern und TOM-Mastern angebotenen Klassifizierungen (z.B. SDM, BSI-Grundschutzkompendium).

Ausgehend vom ausgewählten Risiko-Master kann sich der Nutzer zu ausgewählten Zellen innerhalb der jeweiligen Farbmatrix die insoweit relevanten TOMs anzeigen lassen. Da Risiko- und TOM-Master den gleichen Klassifizierungsmethoden folgen, kann das System zu einem nutzerseitig ausgewählten Risikoszenario die TOMs anzeigen, denen hinsichtlich des identischen Risikoszenarios ein Risiko-Mitigations-Potential zugewiesen worden ist. Auf diese Weise erhält der Nutzer eine nach seinen Anforderungen selektierte Übersicht relevanter TOM zu einem ausgewählten Risiko.

Nunmehr kann der Nutzer die aus den Risiko-Mastern stammenden Bewertungen (abstrakte Risiken) anhand einer Bewertung der bestehenden TOMs anpassen. Soweit der Nutzer eine

zuvor im Risiko-Master vorgenommene Klassifizierung innerhalb einer Folgenabschätzung ändert, ist dies innerhalb der Klassifizierungszelle anhand eines kleinen Dreieck-Symbols ersichtlich, das die ursprüngliche Klassifizierung aus dem Risiko-Master anzeigt.

Über die Auswahl „Vorbereiten für Stellungnahme“ kann der Nutzer eine weitere Eingabeseite aufrufen, in der abschließende Angaben gemacht werden können zu:

- Stellungnahmen von Datenschutzbeauftragten,
- Standpunkte von Betroffenen und
- Notwendigkeit und Verhältnismäßigkeit.

2.3. Reporting-Modul

Über das Reporting-Modul sind alle durchgeführten Datenschutzfolgenabschätzungen einsehbar. Zur genaueren Eingrenzung der Ergebnisse können verschiedene Filtermöglichkeiten verwendet werden. Etwa kann über den gesamten Tenant hinweg anhand von im Basis-Modul definierten Elementen ein Reporting individuell zusammengestellt werden.

2.4. Marktplatz-Modul

Das tenantübergreifende Marktplatz-Modul besteht aus einer Vielzahl von Vorlagen, namentlich hinsichtlich des Basis-Moduls aus mehreren Listen, Sammlungen und TOM-Katalogen sowie hinsichtlich des Compliance-Moduls aus mehreren VT-Mastern.

Vorlagen können durch den Nutzer als Kopie oder als Abonnement in den eigenen Tenant übernommen werden. Bei einer Kopie wird die kopierte Vorlage vom Quelldatensatz separiert. Sie kann bei Bedarf individuell überarbeitet und angepasst werden und ist insofern von etwaigen Änderungen im Quelldatensatz abgekoppelt.

Bei einem Abonnement wird die abonnierte Vorlage nicht vom Quelldatensatz separiert. Sie kann nicht individuell überarbeitet und angepasst werden und ist vielmehr an etwaige Änderungen im Quelldatensatz gekoppelt. Der Inhalt einer abonnierten Vorlage wird immer zentral durch den Quelldatensatz bestimmt.

2.5. Spezielle Funktionen

2.5.1. Labeln

Das System bietet die Möglichkeit, einzelnen, ausgewählten Datenelementen (z.B. Datenelemente einer Sammlung im Basis-Modul oder Verarbeitungstätigkeiten innerhalb eines VT-Masters) ein oder mehrere „Label“ hinzuzuspeichern. Diese werden im Basis-Modul zentral verwaltet und können aus unterschiedlichen Quellen stammen, etwa aus Gesetzen, allgemein anerkannten Standards oder auftraggeberseitig definierten Vorgaben. Ähnlich einem Etikett an einer Ware sind die Labels mit ihren jeweiligen Datenelementen verbunden. Auf diese Weise kann Datenelementen eine beliebige Anzahl beschreibender Attribute hinzugegeben werden. Letzteres kann insbesondere hilfreich sein, um Datenelemente zu kategorisieren und sie ggfs. automatisierten Auswertungen zuzuführen.

2.5.2. Filtern

Das System weist eine Vielzahl von Filterfunktionen auf. Diese können die auf der jeweiligen Eingabemaske befindlichen Informationskategorien enthalten und eine entsprechende Selektion ermöglichen. Diese Funktion dient nicht nur der Übersichtlichkeit hinsichtlich der im System vorhandenen Datenelemente, sondern erlaubt es, den gefilterten Datenbestand einer Massenbearbeitung zuzuführen (z.B.: gefilterten Verarbeitungstätigkeiten innerhalb eines VT-Masters werden in einem Bearbeitungsschritt die gleichen Löschfristen hinzugespeichert).

2.5.3. Suche

Das System weist verschiedentlich die Möglichkeit auf, mittels eines Suchfeldes eine Volltextsuche innerhalb des dazugehörigen Informationsbestandes durchzuführen. Dabei reagiert das System unmittelbar auf eingegebene Zeichen- und Buchstabenfolgen und zeigt sämtliche aus dem dazugehörigen Informationsbestand stammende Treffer an.

2.5.4. Export

Das System ermöglicht es, innerhalb des Compliance-Moduls ausgewählte Inhalte der Master im xlsx-Format zu exportieren. Dabei kann der Nutzer über eine Auswahlfunktion festlegen, welche systemseitig vorgegebenen Bereiche exportiert werden sollen. Soweit ein Export große Datenmengen umfasst, wird die entsprechende xlsx-Datei ggfs. asynchron im Hintergrund generiert und dem Nutzer als E-Mail zugesandt.

Innerhalb des Basis-Moduls können Datenelemente wie Sammlungen oder TOM-Kataloge inklusive ihrer Beschreibungen, Attribute und Bewertungen in ein JSON-Format exportiert werden. Soweit ein Export große Datenmengen umfasst, wird die entsprechende JSON-Datei ggfs. asynchron im Hintergrund generiert und dem Nutzer als E-Mail zugesandt.

2.5.5. Indikatoren

Das System weist eine Vielzahl von Indikatoren auf, die Aufschluss über den Status von im System befindlichen Inhalten geben können. So wird etwa durch eine Farbgebung auf dem Dashboard des Compliance-Moduls angezeigt, ob Folgenabschätzungen vorliegen, ggfs. im Bearbeitungsstatus oder abgeschlossen sind sowie ob sie zu einem positiven oder negativen Ergebnis gekommen sind. Verschiedene Zahlenindikatoren, wie bspw. die Anzahl von Verarbeitungstätigkeiten innerhalb eines VT-Masters und den dazu dokumentierten Elementen, weisen auf den gegenwärtigen Bearbeitungsstand des VT-Masters hin.

2.5.6. Notizen und Aufgaben

Über Notizen und Aufgaben können Nutzer zu bestimmten Ansichten des Systems, bspw. innerhalb eines VT-Masters zu Löschfristen oder innerhalb eines Risiko-Masters zu benutzerspezifischen Risiken, Notizen anlegen, mit anderen Nutzern über eine Chatfunktion kommunizieren sowie sich selbst oder anderen Nutzern Aufgaben zuweisen.

Aufgaben werden immer einem konkreten Nutzer mit einer Priorität zugewiesen. Jeder Nutzer kann ihm zugewiesene Aufgaben einsehen und optional ihren Bearbeitungsstand anpassen.

Zudem wird der Nutzer per E-Mail vom System über neue und geänderte Aufgaben informiert, sofern er die entsprechende Funktion der Software aktiviert hat.

Nutzer, welche Aufgaben anderen Nutzern oder sich selbst zugewiesen haben, können diese Aufgaben ebenfalls nebst ihrem jeweiligen Bearbeitungsstand einsehen.

2.5.7. Verwaltung

Nutzer können ihr Profil in der Softwarelösung bearbeiten und Einstellungen zu Passwort oder Mailbenachrichtigungen selbst vornehmen. Die Anlage weiterer Nutzer erfolgt über die zentrale Systemadministration des Auftragnehmers.

3. Sonstiges

Für die Softwarelösung wird ein Handbuch bereitgestellt.

Die Software ist in deutscher sowie in englischer Sprache verfügbar. Für Datenelemente des Basis-Moduls können Inhalte in deutscher sowie in englischer Sprache separat gepflegt werden.