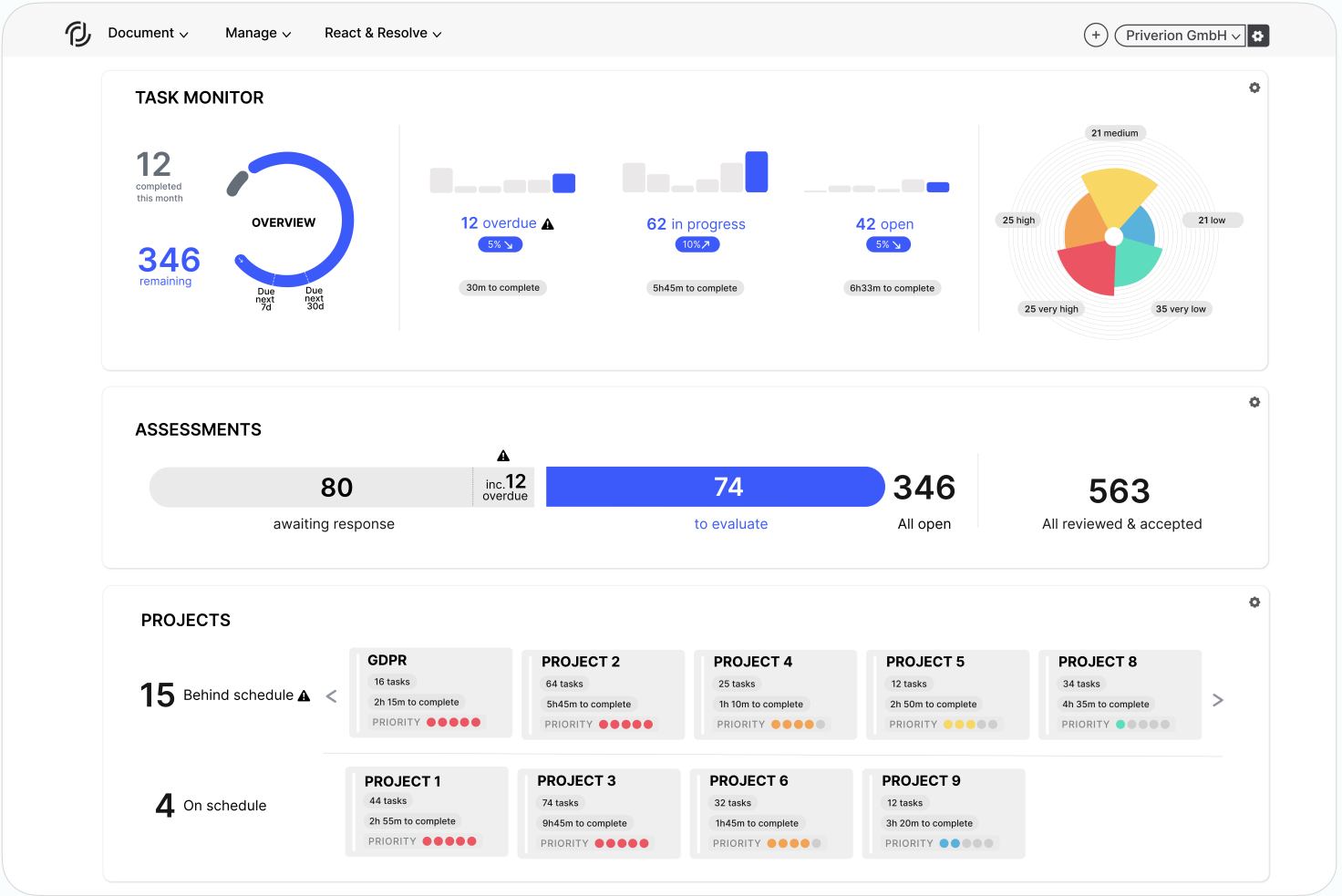
PRIVERION

Eine Plattform.

SEPTEMBER 2023

Eine Plattform.

Datenschutz und InfoSec.



Eine Logik. Drei Schritte.

Mit unseren Datenschutzmodulen erhalten Sie alle notwendigen Elemente der Datenschutz-konformität aufrecht.

Mit unseren InfoSec-Modulen reduzieren Sie InfoSec Risiken und unterstützen Ihr Informationssicherheitsteam.

Eine Logik. Drei Schritte.

Dokumentieren

Ein zentraler Ort, um die Dokumentation Ihres Datenschutz- und Infosec -Programms zu erstellen. Vom Verzeichnis der Verarbeitungsaktivitäten und einer prozessbasierten Risikoansicht bis hin zum InfoSec Asset Verzeichnis stellen Sie sicher, dass Sie alle Risiken abgebildet haben.

Verwalten

Steuern Sie Ihre Datenschutz- und InfoSec-Themen indem Sie Bewertungen und Audits auslösen sowie Risikoberichte auf Basis von Standards oder Vorgaben der Organisationseinheiten erstellen.

Reagieren & lösen

Reagieren Sie auf Vorfälle, prüfen Sie die Meldepflichten oder erstellen Sie Aufgaben und Projekte, um Ihr Datenschutz und Infosec -Programm auf dem Laufenden zu halten. Erstellen Sie Aufgaben um Korrekturmassnahmen umzusetzen.

Schritt eins. Dokumentieren.

- Verzeichnis der Verarbeitungstätigkeiten (ROPA)
- Datenschutz-Folgenabschätzungen (DPIA)
- Berichte & Downloads
- Dokumentation der berechtigten Interessen
- Aufbewahrungs- und Löschfristen
- Automatisierte Entscheidungsfindung & KI
- Technische & organisatorische Massnahmen (TOM)
- Bewertungen (Assessments)
- Lieferanten (Vendors)
- Richtlinien (Policies)
- Datenerhebungspunkte
- Datenschutzportal (Privacy Center)
- Meetings und Aktivitäten

- Meetings und Aktivitäten
- Lieferanten (Vendors)
- Richtlinien (Policies)
- Berichte & Downloads
- Automatisierte Entscheidungsfindung & KI
- Assets Verzeichnis
- Technische & organisatorische Massnahmen (TOM)
- Bewertungen (Assessments)
- Internationale Standards

Schritt zwei. Verwalten.

- Projekte
- Lieferantenrisiken
- Prozessrisiko
- Datenschutzaudit

- Projekte
- Lieferantenrisiken
- Assets Risiko
- Informationssicherheitsaudit

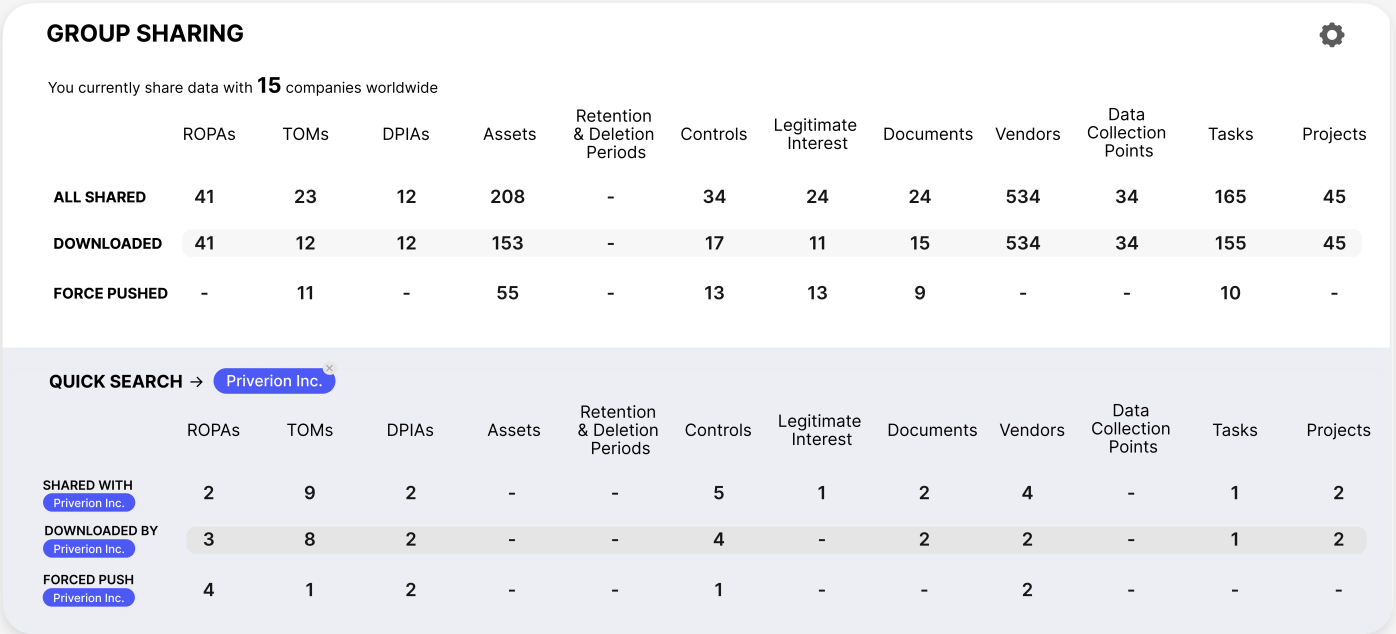
Schritt drei. Reagieren & lösen.

- Aufgaben
- Projekte
- Vorfallmanagement (Incident)
- Anfragen betroffener Personen (DSR)

- Aufgaben
- Projekte
- Vorfallmanagement (Incident)
- Korrekturmassnahmen (Corrective Actions)

Die Funktionen für Gruppengesellschaften unterstützen die Standardisierung von Datenschutz- und InfoSec-Themen. Durch Standardisierung der zentralen Funktionen gewinnen Sie Einblicke in den Reifegrad Ihrer Organisationen sowie der Stellung innerhalb Ihrer Unternehmensgruppe.

Erstellen Sie gemeinsam genutzte Datenverarbeitungen mit einer einzigen Dokumentationsquelle. Jede Organisation kann gemeinsame Dienste herunterladen und deren Dokumentation innerhalb der eigenen Organisation verwenden. Ergänzen Sie die allgemeine Dokumentation um Ihre länderspezifischen Anforderungen.



	ROPAs	TOMs	DPIAs	Assets	Retention & Deletion Periods	Controls	Legitimate Interest	Documents	Vendors	Data Collection Points	Tasks	Projects
ALL SHARED	41	23	12	208	-	34	24	24	534	34	165	45
DOWNLOADED	41	12	12	153	-	17	11	15	534	34	155	45
FORCE PUSHED	-	11	-	55	-	13	13	9	-	-	10	-

	ROPAs	TOMs	DPIAs	Assets	Retention & Deletion Periods	Controls	Legitimate Interest	Documents	Vendors	Data Collection Points	Tasks	Projects
SHARED WITH Priverion Inc.	2	9	2	-	-	5	1	2	4	-	1	2
DOWNLOADED BY Priverion Inc.	3	8	2	-	-	4	-	2	2	-	1	2
FORCED PUSH Priverion Inc.	4	1	2	-	-	1	-	-	2	-	-	-

Highlights

Azure Active Directory

Verbinden Sie Ihr Azure Active Directory und ermöglichen Sie Ihren Mitarbeitern dadurch sofort eine einfachen Zugriff, weisen Sie Aufgaben zu und schaffen Sie Impulse für Ihre Projekte.

Server in der Schweiz oder EU

Wir bieten Server in der Schweiz sowie in Deutschland und an anderen Orten an. Dies umfasst klassische Hyperscaler sowie lokale Anbietern.

DPA Analyzer (in Entwicklung)

Analysieren Sie eine DPA innerhalb einer Minute und erhalten Sie Beratung und Empfehlungen zu Änderungen. Senden Sie Ihr Feedback direkt an den Auftragsverarbeiter, um eine schnelle Umsetzung zu ermöglichen.

Datenschutzportal (in Entwicklung)

Ein Kontaktpunkt für alle Informationen und Anfragen rund um den Datenschutz- und die Informationssicherheit.

Bibliotheken

Aufbewahrung- & Löschfristenbibliothek

Aufbewahrungs- und Löschfristen von über 150 Ländern stehen Ihnen in Kooperation mit unserem Partner Filerskeeper zur Verfügung. Keine langwierige Suche nach Lösch- und Aufbewahrungszeiten in Gesetzen und Vorschriften mehr.

Lieferantenbibliothek (Beta verfügbar)

Keine manuelle Erstellung von Lieferanten mehr. Laden Sie aktualisierte Lieferanten-informationen aus unserer Datenbank und erhalten Sie automatische Aktualisierungen bei Änderungen.

Richtlinienbibliothek (in Entwicklung)

Müssen Sie eine neue Richtlinie (Policy) umsetzen? Laden Sie Vorlagen und Entwürfe aus unserer Bibliothek herunter, um schnell loszulegen.

ROPA-Bibliothek (in Entwicklung)

Die meisten Unternehmen verfügen über Standardprozesse wie HR -Mitarbeiterdateien oder Email-Systeme. Laden Sie diese Verarbeitungstätigkeiten als Vorlagen aus unserer Bibliothek herunter und sparen Sie dadurch Zeit um sich auf komplexe Themen zu konzentrieren.

Modul Index

- Datenschutz Module
- InfoSec Module

D Dokumentieren (Schritt 1)

V Verwalten (Schritt 2)

R Reagieren & lösen (Schritt 3)

D

Aufbewahrungs- und Löschfristen

Eine wichtige Aufgabe der Datenschutz-compliance ist die Aufbewahrung und Löschung von personenbezogenen Daten zu überwachen.
Durch die Erstellung einer organisationsbreiten Aufbewahrungs- und Löschfristen und der Anwendung dieser Fristen auf die relevanten IT Systeme wird die Umsetzung dieser gesetzlichen Voraussetzungen gewährleistet.

D

Automatisierte Entscheidungsfindung & KI

Automatische Entscheidungsfindung und künstliche Intelligenz werden immer wichtiger. Das Erstellen einer soliden Dokumentation zu diesen Technologien und deren Auswirkungen auf die betroffenen Personen ist bei der Einhaltung neuer Vorschriften wie dem AI -Gesetz von größter Bedeutung.

D

Assets Verzeichnis

Dieses Verzeichnis unterstützt den InfoSec Beauftragten und die Risikoeigentümer, bei der Bestimmung der auf Assets (Vermögens-werte) basierenden Risiken. Die Verwendung des szenariobasierten Ansatzes, mittels Schadenshöhen und Eintrittswahrscheinlich-keiten ermöglicht es das Risiko strukturiert zu identifizieren. Erstellen Sie Ihren Risikobe-handlungsplan auf der Grundlage Ihrer Asset Risiken mit wenigen Klicks.

D

Automatisierte Entscheidungsfindung & KI

Es ist zwingende notwendig, dass Sie die Massnahmen zur Informationssicherheit für Ihre automatisierten Entscheidungsprozesse und Technologien für künstliche Intelligenz regelmässig prüfen.
Je mehr Aufmerksamkeit Ihre KI-Technologien erhalten, desto mehr Stakeholder werden die Nachweise über die Einhaltung der Sicherheit und des Datenschutzes einholen.

R

Aufgaben

Erstellen, verwalten und weisen sie Aufgaben Personen in Ihrer Organisation zu. Verfolgen Sie den Fortschritt und erinnern Sie die Benutzer automatisch an Fristen. Bestimmen Sie die Arbeitsaufwand von Aufgaben, um die Arbeitsbelastung Ihres Datenschutzprogramms zu überwachen und Ihre Ressourcen entsprechend zu planen.

R

Anfragen betroffener Personen (DSR)

Verwalten Sie die Anfragen betroffener Personen, erstellen Sie Fälle und verfolgen Sie deren Fortschritt und die Einhaltung der Fristen. Erstellen Sie ein Formular für alle notwendigen Informationen und weisen Sie dynamisch Workflows zu.

V

Assets Risiko

Die meisten internationalen InfoSec Standards nutzen einen Asset (Vermögenswertbasierten) Ansatz um Risiko zu bestimmen. Mithilfe von Risikoszenarien wird die Bedrohung Ihres Assets identifiziert. Basierend auf Ihrem Risikomodell werden die Wahrscheinlichkeiten und Schäden des Risikoszenarios auf das Asset definiert. Mithilfe technischer und organisatorischer Massnahmen können diese Risiken dann kontinuierlich verringert werden.

R

Aufgaben

Erstellen, Verwalten und Zuweisen von Aufgaben im Rahmen der Informations-sicherheit in Ihrer Organisation. Verfolgen Sie den Fortschritt und erinnern Sie die Bearbeiter automatisch an Fristen. Bestimmen Sie die Arbeitsbelastung durch Aufgaben, um den Zeitaufwand Ihres InfoSec-Programms zu bestimmen.

D

Berichte & Downloads

Erstellen Sie individuelle Berichte ohne grossen Aufwand. Möchten Sie einen Bericht Ihrer Verarbeiter mit hohem Risiko oder den offenen Aufgaben erstellen? Mithilfe von Such- und Filterfunktionen können Sie Ihren individuellen Bericht auswählen und erstellen lassen, um Ihre spezifische Frage und Themen zusammenzufassen. Standardisierte Compliance-Berichte ergänzen die einzelnen Berichte.

D

Bewertungen (Assessments)

Die Bewertung von Vorgängen ist eine wichtige Säule Ihres Datenschutzprogramms. Bewertungen können intern zu bestimmten Elementen wie einem ROPA oder extern bei Anbietern durchgeführt werden. Mit unseren Best Practice-Vorlagen oder Ihrer eigenen individuellen Bewertungsmatrix unterstützen wir ihre jährlichen Überprüfungen.

D

Berichte & Downloads

Erstellen Sie individuelle Berichte ohne grossen Aufwand. Möchten Sie einen Bericht der hohen InfoSec Risiken erstellen? Mithilfe von Such- und Filterfunktionen können Sie Ihren individuellen Bericht auswählen und erstellen lassen. Standardisierte Compliance-Berichte ergänzen die einzelnen Berichte.

D

Bewertungen (Assessments)

Die Bewertung des Reifegrads Ihrer Informationssicherheit und die kontinuierliche Aktualisierung kann einen grossen Teil Ihrer Zeit veranschlagen. Die Verwendung eines risikobasierten Ansatzes zur Feststellung des Überprüfungszeitpunkts unterstützt Sie, indem Sie Ihre Ressourcen zielgerichtet einsetzen und Fragen automatisch an die jeweiligen Parteien versenden.

D

Datenschutz-Folgenabschätzungen (DPIA)

Eine DSFA ist erforderlich, um die Verarbeitung personenbezogener Daten mit hohen Risiko zu erfassen, diese zu bewerten und Massnahmen zu definieren. Diese Folgenabschätzungen sind nach vielen Gesetzen erforderlich, wie z. B. der DSGVO oder den bundesstaatlichen Gesetzen in den USA. Wenn Sie planen, sensible oder spezielle Datenkategorien zu verarbeiten, müssen Sie wahrscheinlich eine DSFA durchführen.

D

Datenerhebungspunkte

Um die Informationspflichten zu erfüllen, muss ein Unternehmen alle Schnittstellen erfassen an denen personenbezogene Daten in die Organisation fließen. Diese sogenannten Datenerhebungspunkte sind mit Datenschutz-hinweisen verknüpft und informieren die betroffene Person über die Verarbeitung der Daten. Auf diese Weise können Sie sicher sein, dass Ihre Informationspflichten erfüllt sind.

D Datenschutzportal (Privacy Center)

Das Datenschutzportal ermöglicht es jeder Organisation, ihre Datenschutz- und Infosec-Informationen auf einer zentralen Seite zu veröffentlichen. Dies erhöht die Transparenz und das Vertrauen, da Kunden die Compliance -Dokumentation problemlos überprüfen können. Darüber hinaus werden die Anfragen der betroffenen Personen in standardisierten Best Practice -Formularen durchgeführt.

D Dokumentation der berechtigten Interessen

Als Organisation können Sie Ihre berechtigten Interessen als Grundlage verwenden, um personenbezogene Daten zu verarbeiten. Dafür ist es wichtig, die Interessen der betroffenen Personen zu dokumentieren und diese gegen die der Organisation abzuwägen. Mit dem Modul für berechtigte Interessen können Sie dies auf strukturierte Weise tun und sicherstellen, dass Sie alle erforderlichen Informationen besitzen.

R

Datenschutzaudit

Durch den Überblick über alle Datenschutzthemen, Maßnahmen und Risiken können Sie Ihr aktuelles Datenschutzniveau sofort erfassen und Bereiche identifizieren, in denen weitere Aktionen erforderlich sind.

D

D

Internationale Standards

Internationale Standards wie ISO27001, Cloud Security Standard oder NIST sind die Grundlage für die meisten Infosec-Programme. Mithilfe des Moduls für internationale Standards können Sie alle standardspezifischen Elemente erstellen.

V

Informationssicherheitsaudit

Abhängig von den geltenden Standards sind regelmässige Audits für Informationssicherheit erforderlich. Zum Beispiel die internen Audits nach ISO27001. Unter Verwendung des InfoSec-Prüfungsmoduls können standardspezifische oder individuelle Audits schnell und effizient durchgeführt werden.

R

Korrekturmaßnahmen (Corrective Actions)

Mindern Sie identifizierte Risiken in der Informationssicherheit, indem Korrekturmassnahmen erstellen, um die Wahrscheinlichkeit oder Schadenshöhe zu verringern. Dokumentieren Sie Entscheidungen zu jeder Korrekturmassnahme, welche vom Management getroffen wurden.

D

Lieferanten (Vendors)

Die Datenschutzrisiken in Lieferketten werden immer wichtiger. Um eine korrekte Risikosteuerung zu ermöglichen benötigen sie Einblicke in den Stand des Datenschutzes und der eingesetzten Lieferanten. Veränderungen müssen dort erfasst und zeitnah bearbeitet werden. Unsere Bibliotheken unterstützen Sie zusätzlich durch die Bereitstellung von neuen Informationen.

V

Lieferantenrisiken

Jeder Lieferant erhält eine Bewertung hinsichtlich dessen Risikos. Unter Verwendung verschiedener Risikogruppen kann der Datenschutzbeauftragte zielgerichtete Prüfung steuern und terminieren sowie den notwendigen Fragenkatalog versenden der sich an den Vorgaben der Aufsichtsbehörden orientiert. Aufsichtsbehörden kann auf Anfrage Zugang zur Dokumentation gegeben werden und damit der Auditaufwand und die Dauer der Prüfung reduziert werden.

D

Lieferanten (Vendors)

Alle Daten, die in oder aus Ihrem Unternehmen fliessen, sind ein potenzielles Risiko. Das Verfolgen der Datenflüsse und die Anwendung der richtigen Massnahmen bei Ihren Lieferanten ist für Ihre Informationssicherheit von entscheidender Bedeutung. Von Ihrer externen Anwaltskanzlei bis zu Ihrem externen Entwicklungspartner. Jede Schnittstelle ist wichtig für Ihre Informationssicherheit und sollte regelmässig geprüft werden.

V

Lieferantenrisiken

Abhängig von der Kritikalität Ihres Lieferanten können die Informationssicherheitsbeauftragten Zielreifegrade festlegen und für eine Lieferantenprüfung verwenden.
Mit dem Überblick über das Lieferantenrisiko erhalten die Risikobeauftragten ein direktes Verständnis der Informationssicherheitslandschaft Ihrer Lieferanten.

D

Meetings und Aktivitäten

Das Dokumentieren von Besprechungen und relevanten Aktivitäten ist eine wichtige Aufgabe eines Datenschutzbeauftragten. Da die Beweislast in den meisten Fällen in der Organisation liegt, unterstützt die Aufzeichnung von Aktivitäten in Bezug auf Datenschutz die Abwehr von Ansprüchen. Mit den Modulen für Besprechungen und Aktivitäten können Sie die entsprechende Dokumentation fortlaufend erstellen.

D

Meetings und Aktivitäten

Das Dokumentieren von Meetings und aller relevanten Aktivitäten ist eine wichtige Aufgabe des Informationssicherheitsbeauftragten. Da die Beweislast in den meisten Fällen bei der Organisation liegt, unterstützt Sie diese Aufzeichnungen bei der Abwehr von Ansprüchen. Mit den Modulen für Meetings und Aktivitäten können Sie die entsprechende InfoSec Dokumentation fortlaufend erstellen.

V

Prozessrisiko

Das Verzeichnis der Verarbeitungstätigkeiten erfasst alle Prozesse in Ihrem Unternehmen, die personenbezogene Daten verwenden. Es umfasst alle notwendigen rechtlichen Informationen wie z. B. den Zweck der Verarbeitung sowie die rechtliche Grundlage für die Verarbeitung. Durch intelligente Verknüpfung mit Lösch- und Aufbewahrungsfristen und Ihrer Systemlandschaft wissen Sie immer, welche Lösch- und Aufbewahrungsfristen Anwendung finden.

R

Projekte

Planen Sie ein neues CRM oder die Implementierung eines internationalen Datenschutzstandards? Erstellen Sie ein Projekt und definieren Sie die dafür notwendigen Aufgaben. Führen Sie vor dem Beginn eine GAP Analyse durch, damit Sie wissen, welche Aufgaben erledigt werden müssen und wer diese ausführen wird.

R

Projekte

Regelmässig auftretende Aufgaben können in Projekte gebündelt werden. Jedes Jahr auftretende Prüfprojekte können automatisiert erstellt werden. Mit dieser Funktionalität können Sie Ihre internen Bewertungen auf Autopilot stellen.

D

Richtlinien (Policies)

Die Versionsverfolgung und Kommunikation Ihrer internen Richtlinien ist wichtig für die Implementierung eines effizienten Datenschutzmanagementsystems.
Mit dem Richtlinienmodul können Sie neue Versionen von Dokumenten verfolgen und feststellen, wie gut Ihre Organisation über jede Richtlinie informiert ist.

D

Richtlinien (Policies)

IT-Sicherheitsrichtlinien wie die BYOD-Richtlinie sind wichtige Massnahmen zur Gewährleistung der Informationssicherheit. Mithilfe des Richtlinienmoduls können Sie die Bekanntgabe der Richtlinien innerhalb der Organisation sowie Änderungen und aktualisiert nach Bedarf verfolgen.

D

Technische & organisatorische Massnahmen

Die TOM zeigen auf wie Ihre Organisation rechtliche und regulatorische Anforderungen implementiert hat.
Durch regelmäßige Überprüfungen und eine aktuelle Dokumentation können Sie den Reifegrad Ihrer TOM im Auge behalten.

D

Technische & organisatorische Massnahmen

Nach der Bewertung der finanziellen Risiken für das Unternehmens werden TOM implementiert, um das identifizierte Risiko zu verringern. Die Verknüpfung von TOM mit Risikoszenarien und Überwachung des Implementierungsstatus stellt sicher, dass keine Lücken übersehen werden.

T

D

Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten (ROPA) enthält eine detaillierte Dokumentation aller Prozesse in Ihrem Unternehmen, die personenbezogene Daten verwenden. Es umfasst alle notwendigen rechtlichen Informationen, z. B. den Zweck der Verarbeitung sowie die rechtliche Grundlage für die Verarbeitung. Durch intelligente Verknüpfung mit Lösch- und Aufbewahrungsfristen und Ihrer Systemlandschaft wissen Sie immer, welche Fristen für jedes System gelten und wer verantwortlich ist.

R

Vorfallmanagement (Incident)

Die Behandlung von Vorfällen nach länder-spezifischen Anforderungen ist eine Heraus-forderung. Mithilfe des Vorfall-management können Sie alle erforderlichen Informationen und Benachrichtigungen an einem Ort bündeln. Mit den enthaltenen Workflows sind Sie auf den Ernstfall vorbereitet und können Vorfälle strukturiert prüfen. Dabei unterstützen Sie die Meldeprozesse sollte die Meldung an eine Vielzahl von Aufsichtsbehörden notwendig sein.

D

Vorfallmanagement (Incident)

Vorfälle aufzeichnen, klassifizieren und behandeln. Von der Erstbewertung bis hin zur Berichterstattung und Benachrichtigung an Datenschutzbehörden oder betroffene Personen. Der geführte Prozess unterstützt Informationssicherheitsbeauftragte und Datenschutzbeauftragte bei der Durchführung der erforderlichen Schritte gemäss Best Practices.