Die drei Grundideen hinter der DSGVO

1. Awareness

Das Datenschutzgesetz ist ein Verbotsgesetz, d.h. die Verarbeitung personenbezogener Daten ist grundsätzlich nur erlaubt, wenn eine begründete Ausnahme vom Verbot vorliegt.

2. Transparenz

Welche persönlichen Daten werden
warum, wie, wo und von wem verarbeitet

3. Risikobewertung

Daten sind unterschiedlich sensibel -> Fokus auf Relevanz, damit pragmatische Umsetzung möglich ist

Was ist unser Ansatz zur Umsetzung?

1. Einfach

Die Umsetzung erfolgt durch simples Befüllen einer vorgegebenen Checkliste in einem flexiblen Tool.

2. Klar

Zu den meisten Komponenten wie etwa Filesystem, E-Mail, etc. existieren Vorlagen.

3. Fokussiert

Unser Fokus sind kleine und mittlere Organisationen, alle Templates sind darauf maßgeschneidert.

Was ist generell offen?

Wie der behördliche Auditprozess aussehen wird, da dieser noch nicht definiert ist.

Wie schaut die Umsetzung aus?

1. Basisinformationen und Verantwortungen — 1-3 Tage

a) Adaptieren von 6 Vorlagen: Management Summary, Datenschutzbeauftragter, Anwenderinformation, Datenschutzerklärung, Allgemeine Risikobewertung, Folgeabschätzung
b) Mitarbeiter schulen/informieren
c) Dokumente von den Mitarbeitern unterzeichnen lassen bzw. veröffentlichen

2. Prozesse für betroffene Personen — 2-5 Tage

a) Adaptieren von 7 Vorlagen: Einwilligung Kunden & Lieferanten, Nutzungs-, Lösch-, Berichtigungs-, Verarbeitungseinschränkungs-, und Widerspruchsanfrage
b) Dokumente von den Betroffenen unterzeichnen lassen, bzw. veröffentlichen

3. Verarbeitungsverzeichnis erstellen — 2-10 Tage

a) Befüllen eines Templates pro Applikation (inklusive Filesystem, E-Mail etc.), welche personenbezogenen Daten verarbeitet werden
b) Beschreiben DSGVO-relevanter Anwendungsszenarien pro Applikation

4. Technische und Organisatorische Maßnahmen — 3-10 Tage

a) „Gap – Analyse“ von 13 vordefinierten Bedrohungsszenarien bzgl. technischer und organisatorischer Security. Analyse ob weitere Bedrohungsszenarien vorhanden sind.
b) Operatives „Schließen“ von gefundenen Bedrohungsszenarien

5. Maßnahmen bei Verletzung (data breach) — 1-2 Tage

a) Bewertung/Dokumentation Risiko und Auswirkungen
b) Definition Meldung an Behörde
c) Definition Meldung an Betroffene

Weitere Optionen

1. Technischer Audit / Pentest

Prüfung („freundlicher Hackerangriff“) von einzelnen Applikationen durch einen Spezialisten von Secure Business Austria

2. Organisatorischer Audit / ISO 27001

Prüfung der organisatorischen Sicherheitsrichtlinien durch einen Spezialisten von Secure Business Austria

3. Rechtliche Prüfung von Dokumenten

Prüfung kritischer Dokumente aus der DSGVO-Umsetzung durch einen spezialisierten Rechtsanwalt

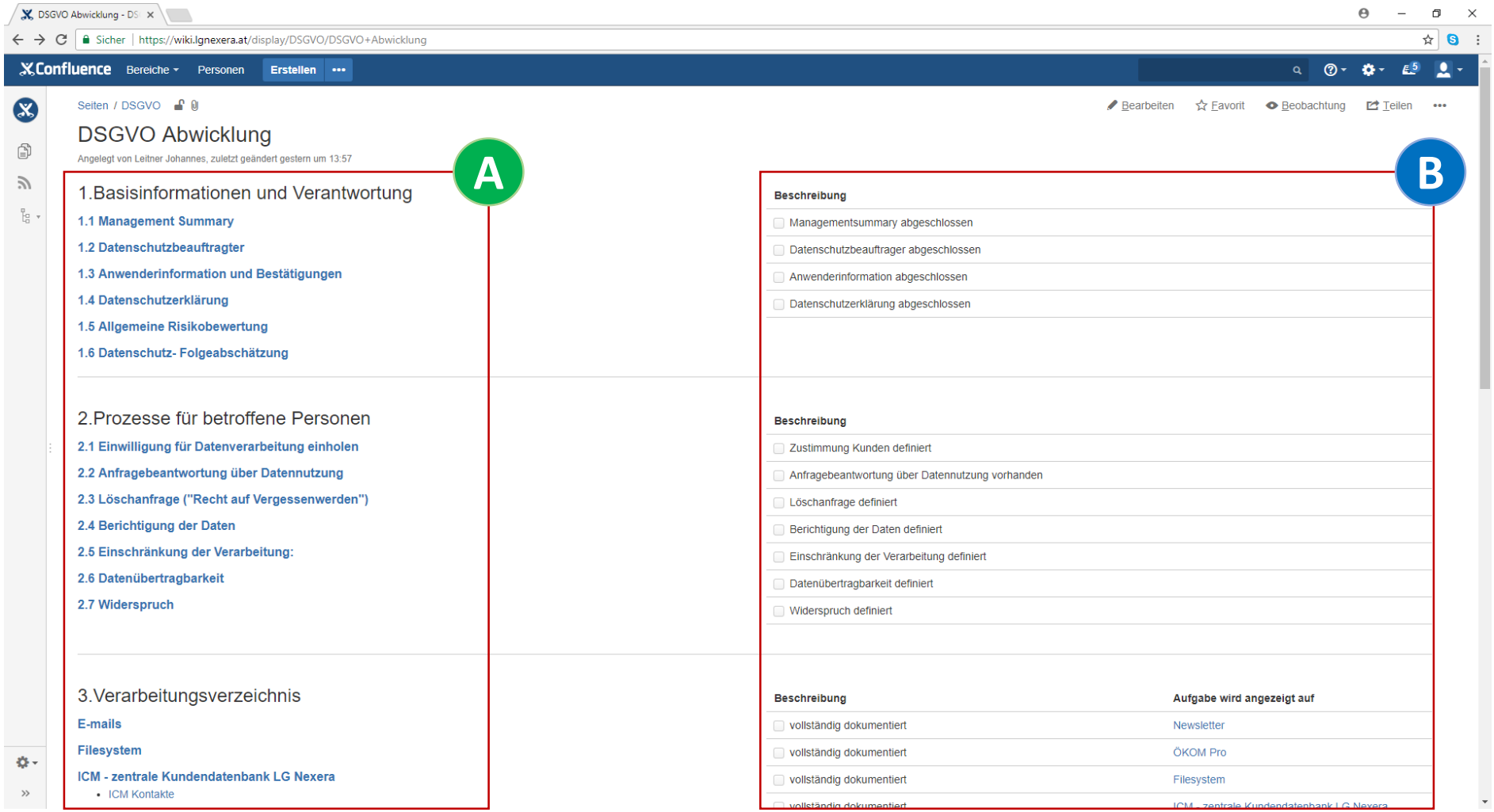
4. Rent a Datenschutzbeauftragter

Sie wollen den Datenschutzbeauftragten nicht selbst stellen, sondern einen externen Profi als Dienstleister engagieren? Reden Sie mit uns!

Thomas Geretschläger

- Ausbildung zum Qualitätsmanager nach ISO/IEC 9001
- Aufbau und Akkreditierung eines Managementsystems nach ISO/IEC 17021 für ISMS Zertifizierungen nach ISO/IEC 27001

Wie schaut das Tool aus? - Übersicht



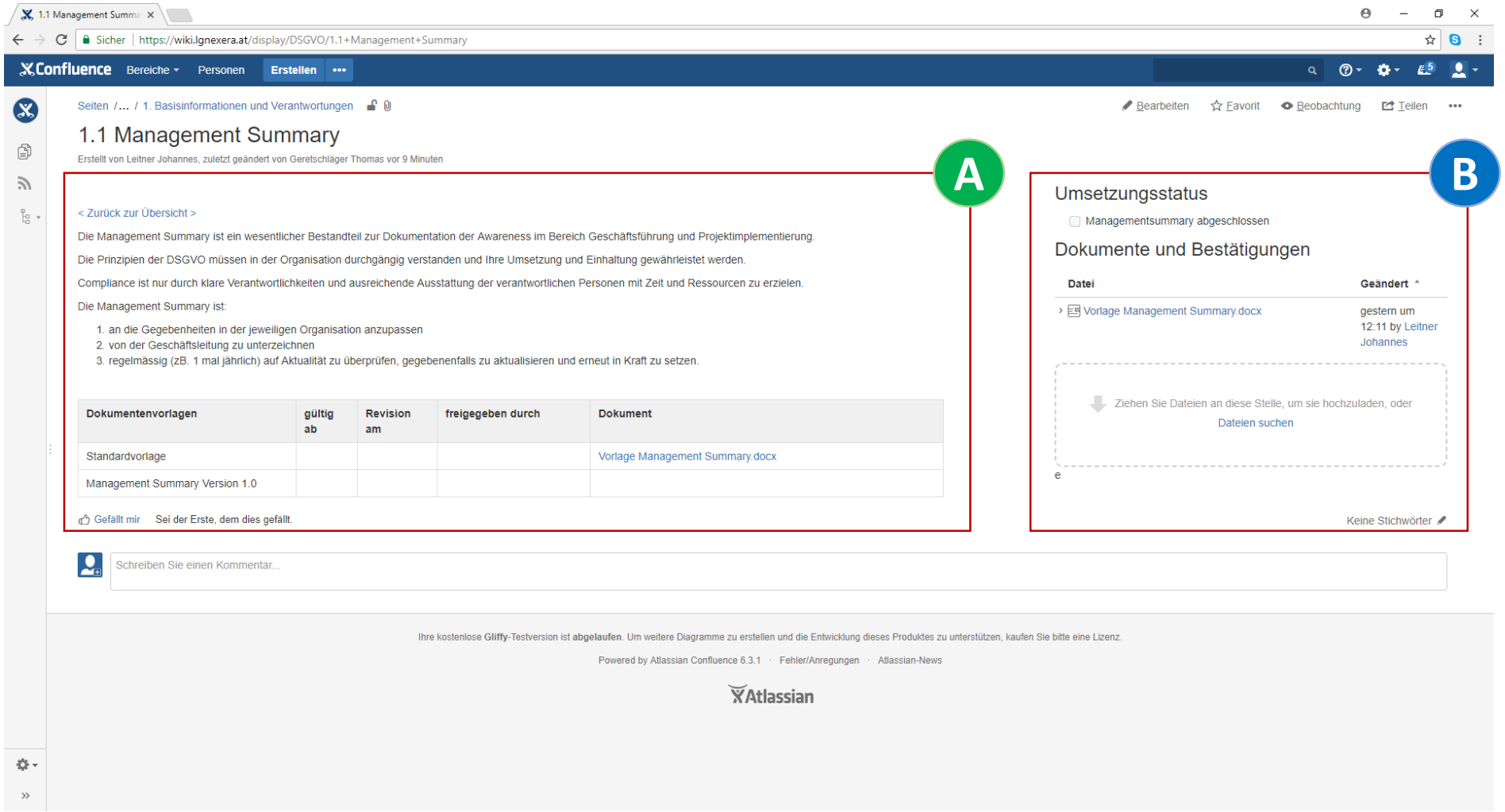
A

Übersichtsliste und Navigation der DSGVO Umsetzungsmaßnahmen

B

Übersicht, welche Schritte, Dokumente und Aufgaben offen sind

Wie schaut das Tool aus? – Dokumente und Bestätigungen



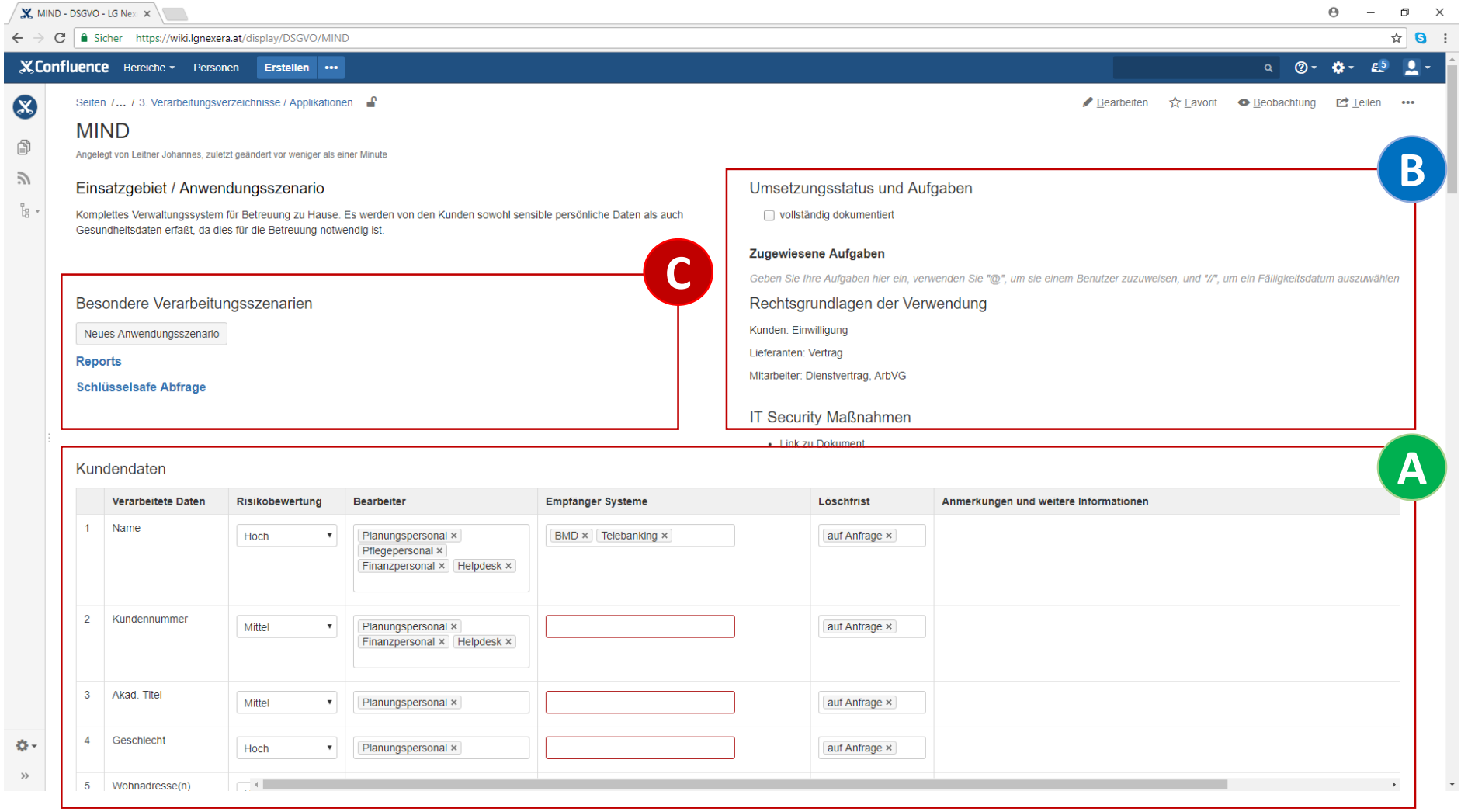
A

Kurze Erklärung, Vorlagen und kundenspezifische Varianten der Dokumente

B

Umsetzungsstatus und integrierte Verwaltung der unterzeichneten Dokumente

Wie schaut das Tool aus? – Verarbeitungsverzeichnis



A

Auflistung aller in der Applikation verarbeiteten persönlichen Daten inklusive Klassifizierung und Dokumentation wohin sie übergeben werden

B

Umsetzungsstatus und weitere Informationen

C

Beschreibung DSGVO-relevanter Arbeitsprozesse in der Applikation inklusive der Schutzmaßnahmen

Umgang mit Filesystem

Szenario für Backup Problematik

Aus Effizienzgründen werden im Rahmen des Backups möglicherweise auch personenbezogene Daten mitgesichert, ohne diese vorher zu löschen. Der Schutz der persönlichen Daten erfolgt jedoch durch den im folgenden definierten **Wiederherstellungsprozess**:

1. Das Wiederherstellen des Backup wird manuell von einem Systemadministrator durchgeführt.
2. Der Datenschutzbeauftragte wird vorher informiert und es werden nur spezifisch angefragte Daten wiederhergestellt.
3. Der Datenschutzbeauftrage prüft bei den wiederhergestellten Daten ob personenbezogene Daten enthalten sind und setzt gegebenfalls die notwendigen Schritte.

Zugriffsrechte aus DSGVO Sicht - Beispiel

Pfad	Abgelegte Personendaten	Risikobewertung	Bearbeiter	Empfänger Systeme	Löschfrist	Anmerkungen und weitere Informationen
Finanzen und Organisation	Mitarbeiterdaten	Mittel	Leitner Johannes, Gornik Gabriele, Poller Florian, Geretschläger Thomas		auf Anfrage ×	
Temp Verzeichnis		Mittel	Alle Mitarbeiter		täglich ×	
Scan Verzeichnis		Mittel	Scanprogramm	ICM ×	täglich ×	
Testverzeichnis	Teilweise Echtdaten von Kunden	Hoch	Gruppe Softwareentwickler		monatlich ×	Wird spätestens monatlich gelöscht.
Restliches Filesystem		Niedrig	Alle Mitarbeiter		auf Anfrage ×	

Besondere Verarbeitungsszenarien

Analog zu den Verarbeitungsverzeichnissen sollten hier sensible Szenarien basierend auf einer Risikoanalyse evaluiert und dokumentiert werden.

Umgang mit E-Mails

Persönliche Postfächer

1. Löschfristen bei Austritt?
2. Zugriff auf weitere Postfächer?
3. Weiterleitungen von anderen Postfächern?

Ein weiterer zentraler Punkt ist die Schulung der Mitarbeiter, welche Information Sie per Mail an wen weiterleiten dürfen; dies ist Teil der Mitarbeiterinformation und Schulung (Punkt 1.3).

Anonyme Postfächer

1. Für welchen Inhalt wird das Postfach benutzt inklusive Risikobewertung?
2. Welche Personen haben Zugriff auf das Postfach?
3. Welche Weiterleitungen sind zu diesem Postfach eingerichtet?
4. Welche EDV-Systeme(=Verarbeitungsverzeichnisse) greifen automatisiert darauf zu?

Verteiler

1. Welche Verteiler gibt es?
2. Wer darf Verteiler einrichten / ändern?
3. Welche Personen/Anonyme Postfächer erhalten die E-Mails?

Anmerkung zum Dokumentationsprozess

Bei Einsatz von Active Directory kann ein Teil der Informationen via spezieller Scripts automatisiert übernommen werden.

Umgang mit Reports in Applikationen

(Die gleiche Problemstellung ergibt sich durch die Möglichkeit, Screenshots von Applikationen anzufertigen)

Zugriffsrechte

1. Sollten im Rahmen der jeweiligen Modulberechtigungen der einzelnen Softwarepakete geregelt sein.
2. Reports mit besonders sensiblen Informationen sollten als Verarbeitungsszenario innerhalb des Verarbeitungsverzeichnisses der Applikation dokumentiert werden.

Speicherung von Reports

1. Information/Sensibilisierung der Mitarbeiter im Rahmen der Schulung bzgl. Speicherung (Punkt 1.3)
2. Definition, auf welchen speziellen Verzeichnissen Reports mit sensiblen Daten gespeichert werden müssen (siehe Verarbeitungsverzeichnis Filesystem), damit die Vorgaben der DSGVO (Zugriff, Löschen etc.) auch in diesem Fall eingehalten werden
3. Information/Sensibilisierung der Mitarbeiter im Rahmen der Schulung bzgl. Weiterleitung (siehe Verarbeitungsverzeichnis E-Mail)

Umgang mit Tests mit Echtdaten

Zugriffsrechte

1. Sollten im Rahmen der jeweiligen Modulberechtigungen der einzelnen Softwarepakete geregelt sein.
2. Reports mit besonders sensiblen Informationen sollten als Verarbeitungsszenario innerhalb des Verarbeitungsverzeichnisses der Applikation dokumentiert werden.

Speicherung von Testdaten

1. Information/Sensibilisierung der Mitarbeiter im Rahmen der Schulung bzgl. Speicherung (Punkt 1.3)
2. Definition, auf welchen speziellen Verzeichnissen die Testdaten mit sensiblen Daten gespeichert werden müssen (siehe Verarbeitungsverzeichnis Filesystem) damit die Vorgaben der DSGVO (Zugriff, Löschen etc.) auch in diesem Fall eingehalten werden.

Summary

Projektablauf

1. Basisinformationen und Verantwortungen	1-3 Tage
2. Prozesse für betroffene Personen	2-5 Tage
3. Verarbeitungsverzeichnis erstellen	2-10 Tage
4. Technische und Organisatorische Maßnahmen	2-10 Tage
5. Maßnahmen bei Verletzung (data breach)	1-2 Tage