Wirksamkeitsprüfung Datenschutz

»Sicherheit der Verarbeitung« aller REISSWOLF Betriebe

Wirksamkeitsprüfung in Form einer Eigenüberwachung zur Umsetzung der Vorgaben der DSGVO

Es ist für REISSWOLF ein elementares Anliegen die datenschutzrechtlichen Anforderungen der DSGVO verordnungskonform umzusetzen.

Nachstehend die Dokumentation über eine interne Prüfung (Eigenüberwachung) der Wirksamkeit der seitens REISSWOLF eingeleiteten Verfahren und Maßnahmen zur Umsetzung der Vorgaben der DSGVO und dem BDSG

Es wurde eine interne Prüfung der Verfahren und Maßnahmen zur Umsetzung der Vorgaben der DSGVO und dem BDSG sowie zur Angemessenheit und Wirksamkeit dieser Verfahren und Maßnahmen vom Dez. 2020 bis Feb. 2021 durchgeführt.

Die Eigenüberwachung soll den auf einen Auftragsverarbeiter (hier: Akten- und Datenvernichter, Digitalisierer, Einlagerungsbetriebe) anwendbaren Wirkungsbereich der DSGVO umfassen, also von der Akten- und Datensammlung bei einer verantwortlichen Stelle über den Transport, die mögliche Einlagerung bis zur Vernichtung in einer Akten-Schredderanlage.

Die Überwachung der Einhaltung der Vorgaben der DSGVO erstreckt sich dabei von der einwandfreien vertraglichen Einbindung verantwortlicher Stellen (Auftragsverarbeitungs-Vertrag) unter Berücksichtigung des Schutzbedarfs und der Herkunft der personenbezogenen Daten (z.B. Berufsgeheimnisträger oder auch Datenträger die dem Bankgeheimnis unterfallen) über die nachweislich gesicherte Verarbeitung (Technisch organisatorische Maßnahmen) bis zum Aufzeichnen der notwendigen Betriebsdaten sowie des übergeordneten Dokumentenmanagementsystems.

Zur Durchführung der Überwachung wurden die sich aus den Artikeln der DSGVO ergebenden Vorgaben als Maßstab angesetzt und die Erfüllung dieser Vorgaben wurde dokumentiert. Die Dokumentation soll die Angemessenheit und Wirksamkeit der ein- bzw. umgesetzten Maßnahmen aufzeigen.

Gegenstand der Prüfung

Das Unternehmen REISSWOLF International AG ist ein Dienstleistungsunternehmen, welches im Auftrag seiner Kunden an verschiedenen Standorten, Akten und Daten einsammelt, digitalisiert, archiviert und vernichtet.

Die Beauftragten für Informationssicherheit und Qualitätsmanagement wurde gebeten eine Überprüfung der Wirksamkeit der Umsetzung der Grundsätze, Verfahren und Maßnahmen nach Vorgabe der DSGVO und dem BDSG in Form einer Eigenüberwachung durchzuführen.

Die Beauftragten führten die Überprüfung anhand mehrerer Vor-Ort-Audits an unterschiedlichen Standorten durch. Das Ergebnis dieser Überprüfung basiert zudem auf zahlreichen Gesprächen mit Mitarbeitern des Hauses REISSWOLF und der Beantwortung eines definierten Anforderungskatalogs durch die zuständigen Fachbereiche. Der Anforderungskatalog konkretisiert die Regelungen der DSGVO und des BDSG im Zusammenhang mit der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und stellt geeignete Kriterien für die Beurteilung der von REISSWOLF getroffenen datenschutzspezifischen Maßnahmen dar.

Die Grundsätze, Verfahren und Maßnahmen des Datenschutzes sind bei REISSWOLF auf die Einhaltung der Anforderungen der DSGVO und des BDSG bei der Verarbeitung personenbezogener Daten ausgerichtet.

Das Zusammenwirken dieser Grundsätze, Verfahren und Maßnahmen wird durch das Datenschutzmanagement bestimmt, das vom Datenschutzumfeld sowie der Datenschutzaufbau- und Ablauforganisation abhängt. Die Ausgestaltung der Verfahren und Maßnahmen des Datenschutzes

Wirksamkeitsprüfung Datenschutz

erfolgt bei REISSWOLF in Abhängigkeit von Art und Umfang der ausgeübten Tätigkeiten: Transportieren, Digitalisieren, Archivieren und Vernichten.

Verarbeitung bezeichnet gemäß Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Reihe von solchen Vorgängen im Zusammenhang mit personenbezogenen Daten. Hierzu gehören bei REISSWOLF gemäß Art. 4 Nr. 2 DSGVO z.B. die Speicherung, das Lagern das Löschen und die Vernichtung der personenbezogenen Daten.

Die Prüfung der Verarbeitungstätigkeiten „Speichern, Lagern, Löschen und Vernichten“ betraf die Tätigkeiten i.S. von Art. 4 Nr. 2 DSGVO und bezog sich auf konkrete Abwicklungen und Vorgänge, die personenbezogene Daten verwenden. Eine isolierte Prüfung der Verarbeitung einzelner Kategorien von personenbezogenen Daten lag nicht im Anwendungsbereich dieser Prüfung.

Ergebnis der Eigenüberwachung

Nach unserer Beurteilung sind die Verfahren und Maßnahmen zur Umsetzung der Anforderungen der DS-GVO und dem BDSG für die Zwecke der Akten- und Datenvernichtung, der Digitalisierung, sowie der Einlagerung geeignet. Die Verfahren und Maßnahmen zur Umsetzung der Anforderungen der DS-GVO und dem BDSG sind in den wichtigen Belangen frei von wesentlichen Fehlern. Sie waren im geprüften Zeitraum hinreichend implementiert und wirksam. Nachstehend ein Auszug.

Glinde, 11.03.2021

Axel Pöhlmann
Datenschutzkoordinator

Wirksamkeitsprüfung Datenschutz

Auszug aus dem Prüfungsumfang

1 DSDVO Anforderung Art 5 Abs. 1, 2, Art. 24 Abs. 1, Art. 29

REISSWOLF stellt mit der Einrichtung eines geeigneten Umfelds und einer geeigneten Aufbau- und Ablauforganisation mit hinreichender Sicherheit die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher.

1.1 Datenschutzziele

Die festgelegten Datenschutzziele lassen sich nachvollziehbar aus der Unternehmensstrategie ableiten, besondere datenschutzrechtliche Faktoren, die sich aus dem Geschäftsmodell ergeben, wurden berücksichtigt und sind dokumentiert.

1.2 Rechtliches, regulatorisches Umfeld

Das in Bezug auf den Datenschutz für REISSWOLF relevante rechtliche und regulatorische Umfeld wurde bei der Festlegung der Datenschutzmaßnahmen berücksichtigt. Es erfolgt eine anlassbezogene sowie regelmäßige Prüfung im Hinblick auf Änderungen des rechtlichen und regulatorischen Umfelds.

1.3 Rahmenwerk zum Umgang mit dem Datenschutz

Die Regelungen sind durch ein Dokumenten-Management nachvollziehbar dokumentiert. Die Regelungen umfassen die nachstehenden Bereiche und sind allen Mitarbeitern zugänglich.

- Datenschutzorganisation
- Stellung und Aufgaben des Datenschutzbeauftragten
- Datenschutzrechtliches Management und Datenschutzfolgenabschätzung
- Zulässigkeit der Verarbeitung personenbezogener Daten
- Datenschutz durch Technikgestaltung
- Verzeichnis von Verarbeitungstätigkeiten
- Technisch organisatorische Maßnahmen
- Löschung von Daten
- Betroffenenrechte
- Datenschutzverletzungen und Meldung
- Auftragsverarbeitung und Zulässigkeit der Übermittlung von Daten
- Übermittlung von Daten in Drittländer
- Sensibilisierung und Kommunikation
- Nachweis- und Rechenschaftspflichten

1.4 Schulungskonzept:

Die Kommunikation der datenschutzrelevanten Grundsätze, Verfahren und Maßnahmen an die beteiligten Mitarbeiter ist durch das Schulungskonzept sichergestellt. Es sorgt dafür, dass die Mitarbeiter ihre Rolle und Bedeutung im jeweiligen Prozess und deren Abhängigkeiten von vor- und nachgelagerten Prozessschritten bzw. Kontrollen kennen.

1.5 Schulungsnachweisführung

Das Unternehmen führt geeignete Nachweise zu regelmäßig durchgeführten Schulungen, zur Teilnahme an den Schulungen und zur Überprüfung des Wissensstands der Mitarbeiter. Die Mitarbeiter haben die Pflicht zur Teilnahme an Datenschutzschulungen (diese schließen auch das Bankgeheimnis ein). Die vollständige Teilnahme wird nachgehalten.

1.6 Gefährdungsanalyse Einhaltung der datenschutzrechtlichen Grundsätze

Die Überwachung der Einhaltung der datenschutzrechtlichen Grundsätze, Verfahren und Maßnahmen erfolgt in Form von internen Audits. Im Verlauf der Audits und bei Bedarf werden Verbesserungsvorschläge erarbeitet. Die angemessene Kommunikation mit dem Datenschutz-Koordinator und der Datenschutzbeauftragten ist sichergestellt.

2 Prozess zum Management von Datenschutzrisiken Art. 32, 35, 24 und 25 Abs. 1 DSGVO

Das Unternehmen stellt mit der Einrichtung eines geeigneten datenschutzrechtlichen Risikomanagements die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben sicher. Die Rechte und Freiheiten von Betroffenen werden angemessen berücksichtigt:

- Identifikation potentieller Risiken
- Bewertung der identifizierten Risiken in Bezug auf die Auswirkungen auf Rechte und Freiheiten von Betroffenen
- Festlegung von Maßnahmen zur Risikobehandlung
- Überwachung der Umsetzung der Maßnahmen zur Risikobehandlung
- Kommunikation der Risiken an alle relevanten Einheiten in der Organisation.

Das Risikomanagement berücksichtigt Risiken für die Rechte und Freiheiten von Betroffenen aus Projekten, Risiken aus dem Regelbetrieb, Risiken im Rahmen von Datenschutzvorfällen, Risiken aus Prozessen für datenschutzfreundliche Technik und Voreinstellungen und Risiken aus Datenschutz-Folgenabschätzungen.

2.1 Prozess zur Datenschutz-Folgenabschätzung

Durch ein zweistufiges Prüfungsverfahren ist sichergestellt, dass für Verarbeitungstätigkeiten mit einem hohen Risiko eine Datenschutz-Folgenabschätzung durchgeführt wird

1. Erforderlichkeitsprüfung: Prüfung, ob ein hohes Risiko für die Rechte und Freiheiten von Betroffenen besteht bzw. die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 DSGVO gegeben ist.
2. Durchführung der Datenschutz-Folgenabschätzung bei voraussichtlich hohem Risiko für die Rechte und Freiheiten von Betroffenen bzw. bei Vorliegen der Voraussetzungen gemäß Art. 35 Abs. 3 DSGVO.

Die Methode zur Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung erfüllt die formalen Anforderungen gemäß Art. 35 DSGVO. Die Ergebnisse der Erforderlichkeitsprüfung und der Datenschutz-Folgenabschätzung werden dokumentiert.

2.2 Technisch organisatorische Maßnahmen auf Basis der Risikobewertung

Es ist ein geregelter Prozess eingerichtet, der sicherstellt, dass auf der Grundlage der Risikobewertung angemessene technische und organisatorische Maßnahmen für Verarbeitungstätigkeiten abgeleitet und dokumentiert werden.

3 Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Die eingerichteten Verfahren und Kontrollen stellen mit hinreichender Sicherheit sicher, dass das Verzeichnis von Verarbeitungstätigkeiten im Unternehmen geführt und gepflegt wird und auf Anfrage bereitgestellt werden kann. Das Unternehmen führt als Auftragsverarbeiter 2 Verzeichnisse: Ein Verzeichnis welches die im eigenen Unternehmen stattfindenden Verarbeitungstätigkeiten beschreibt und eines, welches an öffentliche Stellen auf Anforderung zur Verfügung gestellt werden kann.

3.1 Dokumentationspflicht auf Basis des Verzeichnisses von Verarbeitungstätigkeiten

Das Unternehmen führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO, um seiner Dokumentationspflicht nachzukommen. Das Verzeichnis der Verarbeitungstätigkeiten wird gemäß Art. 30 Abs. 3 DSGVO in schriftlicher Form (elektronisch) geführt.

Das Verzeichnis von Verarbeitungstätigkeiten gibt für jede Verarbeitungstätigkeit Auskunft über.

- den Namen und die Kontaktdaten des Verantwortlichen
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt werden,
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

3.2 Verzeichnis von Verarbeitungstätigkeiten (Auftragsverarbeiter Art. 30 Abs. 2 DSGVO)

REISSWOLF ist als Auftragsverarbeiter tätig und führt ein Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

Das Verzeichnis zu allen Kategorien von den im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung wird gemäß Art. 30 Abs. 3 DSGVO elektronisch geführt.

3.3 Zur Verfügungstellung des Verzeichnisses gemäß Art. 30 Abs. 4 DSGVO

Auf Anfrage der Aufsichtsbehörde ist der Verantwortliche bzw. der Auftragsverarbeiter in der Lage, das Verzeichnis zur Verfügung zu stellen. Diesbezüglich ist vom Unternehmen ein Prozess einschließlich klarer Verantwortlichkeiten definiert. Es erfolgt eine regelmäßige Überprüfung der Vollständigkeit und Richtigkeit des Verzeichnisses durch den Verantwortlichen.

4 Technisch, organisatorische Maßnahmen des Auftragsverarbeiters (Art. 32 DSGVO)

Es sind geeignete technische und organisatorische Maßnahmen eingerichtet, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Hierbei wurden der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die Zwecke der Verarbeitung sowie die

unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt.

Die Maßnahmen umfassen:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen:
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.1 Richtlinien zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

Es sind Richtlinien zur Sicherheit der Verarbeitung vorhanden, die für alle Systeme und Anwendungen gelten, die personenbezogene Daten verarbeiten. Die Richtlinien umfassen klare Vorgaben, Rollen und Verantwortlichkeiten sowie Dokumentationsanforderungen und werden regelmäßig auf Aktualität geprüft.

- Business Continuity und IT-Desaster Recovery
- Zugriffsmanagement
- Kryptographischen Maßnahmen
- Malware und Virenschutz