V2.0/25.11.2024

RESTRICTED TLP:AMBER

Interne Richtlinie

Datenschutz

Version: 2.0

Datum: 25.11.2024

Erstellt von: Sterner

Freigabe von: **XXX**

Inhaltsverzeichnis

1. Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
TT/MM/JJJJ	1.0	Scholz	Erst ab der v1.0 angeben (Erste gültige Fassung)
25/11/2024	2.0	Sterner	Neufassung wesentlicher Teile

2. Definitionen

Anonymisierung	Technisches Verfahren, das auf Personenbezogene Daten angewendet wird, damit Betroffene Personen nicht oder nicht mehr identifiziert werden können.
Auftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Auftragsdatenverarbeitungsvereinbarung (ADV)	Vertragliche Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter, die zumindest die Mindestanforderungen nach Art 28 DSGVO enthält.
Besondere Kategorien personenbezogener Daten	Gemäß Art 9 DSGVO Personenbezogene Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit“ hervorgehen, sowie „genetische Daten, biometrische Informationen zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.“
Betroffene Person	Jede natürliche identifizierte oder identifizierbare Person, die von einer konkreten Verarbeitung Personenbezogener Daten betroffen ist.
Datenschutz-Grundverordnung („DSGVO“)	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Datenschutzkoordinator	Intern benannte und besonders geschulte Person, die den Verantwortlichen (vertreten durch den Geschäftsführer) bei der Einhaltung der Vorgaben nach der DSGVO und lokalem Datenschutzrecht unterstützt. Nicht gleichzusetzen mit der Funktion eines Datenschutzbeauftragten nach Art 37 ff DSGVO.
Personenbezogene Daten	Gemäß Art 4 Z 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen." *Beispiele: U.a. Name, Emailadresse, Geburtsdatum, Sozialversicherungsnummer, Bild- und Tonaufnahmen, Logfiles, aber auch pseudonymisierte / gehashte Informationen.*
Pseudonymisierung	Gemäß Art 4 Z 5 DSGVO „die Verarbeitung Personenbezogener Daten in einer Weise, dass die Personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden."
Verarbeitung Personenbezogener Daten	Gemäß Art 4 /Z 2 DSGVO jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung."
Verarbeitungsverzeichnis („VVZ")	Internes Verzeichnis aller Verarbeitungstätigkeiten, mit dem Mindestinhalt nach Art 30 DSGVO. Nähere Informationen siehe **Punkt 6** dieser Richtlinie.
Verletzung des Schutzes personenbezogener Daten („Data Breach")	Gemäß Art 4 Z 12 DSGVO „die Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden."

Verantwortlicher	Gemäß Art 4 Z 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personenbezogenen Daten entscheidet." *Im Unternehmenskontext typischerweise das Unternehmen in seiner jeweiligen Rechtsform (GmbH oÄ), nicht aber interne Bedarfsträger wie einzelne Abteilungen (HR, IT, etc), da die unternehmerischen Letztentscheidungen immer von der Geschäftsführung getroffen werden.*

3. Geltungsbereich

Bei der hier vorliegenden internen Richtlinie „Datenschutz" handelt es sich um eine für das Gesamtunternehmen verbindliche Vorgabe, um intern ein einheitliches Datenschutzniveau sicherzustellen. Sie enthält neben allgemeinen Vorgaben zum Thema Datenschutz auch eindeutig an bestimmte Adressaten gerichtete Handlungsanweisungen.

Die Richtlinie „Datenschutz" wird daher in ihrer jeweils aktuellen Fassung an alle Mitarbeiter*innen des Gesamtunternehmens zumindest in Form einer elektronischen Kopie ausgehändigt. Die verbindliche Kenntnisnahme als auch die Verpflichtung der Einhaltung der darin enthaltenen Vorgaben sind schriftlich durch jeden Mitarbeiter / jede Mitarbeiterin zu bestätigen. Eine entsprechende Dokumentation erfolgt im Rahmen des Onboardings neuer Mitarbeiter*innen durch den zuständigen HR Ansprechpartner im Personalakt der betreffenden Mitarbeiter*innen.

Festgehalten wird, dass die Einhaltung der in der internen Richtlinie „Datenschutz" getätigten Vorgaben für alle Mitarbeiter*innen verpflichtend ist, die Einhaltung dieser Vorgaben wird durch ein internes Datenschutz-Kontrollmanagement laut **Punkt 11** dieser Richtlinie regelmäßig als auch anlassbezogen geprüft. Ein Verstoß gegen diese Vorgaben kann unter Umständen disziplinar- und arbeitsrechtliche Konsequenzen nach sich ziehen.

Festgehalten wird weiter, dass sich das Hauptquartier des Gesamtunternehmens im Geltungsbereich der DSGVO befindet und deren Regularien daher maßgeblich für das Gesamtunternehmen sind. Weiters ist lokales Datenschutzrecht, im Besonderen für Österreich das Datenschutzgesetz (DSG) in seiner jeweils aktuellen Fassung, beachtlich.

3.1. Verantwortlichkeiten

3.1.1. Verantwortlicher (vertreten durch die Geschäftsführung)

Verantwortlicher im Sinne der DSGVO ist das Gesamtunternehmen, vertreten durch seine nach Außen vertretungsbefugten Geschäftsführer: Diese sind daher verantwortlich, die Richtlinie „Datenschutz" im Gesamtunternehmen zu implementieren und wiederkehrend zu Datenschutz-Themen intern zu kommunizieren sowie eine interne Datenschutz-Kultur zu etablieren („tone from the top").

Weiters ist die Geschäftsführung verantwortlich für die Implementierung eines internen Datenschutz-Kontrollmanagementsystems, um die Effizienz und Effektivität des internen Datenschutzmanagementsystems sicherzustellen. Die Geschäftsführung kann sich in diesem Bereich einer externen Unterstützung (Datenschutzberatung / externer Datenschutzbeauftragter) bedienen, ohne dass jedoch die Verantwortlichkeit auf diesen externen Support übergeht.