# Technisch-organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

## der Norstat Deutschland GmbH

\\ Version 1.1
\\ Stand der Bearbeitung: 19.10.2021

\\ Erstellt von:
\\ Philipp Kemser • Datenschutzbeauftragter • Norstat Deutschland GmbH

Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Norstat Deutschland GmbH erfüllt diesen Anspruch durch folgende Maßnahmen und führt darüber hinaus regelmäßige Qualitätsüberprüfungen durch, welche nach ISO 20252:2019 zertifiziert sind:

### 1. Vertraulichkeit gem. Art. 32 Abs.1 lit. b DSGVO

#### 1.1 Zutrittskontrolle

- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle am Empfang
- Trennung von Bearbeitungs- und Publikumszonen
- Protokollierung der Besucher

#### 1.2. Zugangskontrolle

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Nutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Einsatz von Intrustion-Detection-Systemen
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

#### 1.3. Zugriffskontrolle

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern der REISSWOLF International AG

### 1.4. Trennungskontrolle

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

- Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten Systemen (mögl. verschlüsselt)
- Interne Anweisung: personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 2.1. Weitergabekontrolle

- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Sicherer Datentransfer über gesicherte Webseite
- Verschlüsselung von E-Mail-Anhängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

### 2.2. Eingabekontrolle

- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind für den Zeitraum der Datenerfassung
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

## 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### 3.1. Verfügbarkeitskontrolle (Sowohl am Standort München als auch im firmeneigenen Rechenzentrum in Larvik, NO)

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte bei Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 4.1. Datenschutz-Management

- Software-Lösungen für Datenschutz-Management im Einsatz
- Interne(r) Datenschutzbeauftragte(r)
  - Philipp Kemser (Standort München)
  - Tone Belsvik (Standort Oslo)
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
- Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
- Jährliche Sensibilisierung der Mitarbeiter
- Dokumentiertes Sicherheitskonzept
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

### 4.2. Incident-Response-Management

- Einsatz von Firewall und regelmäßige Aktualisierung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
- Intrusion Detection System (IDS)
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- Intrusion Prevention System (IPS)
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

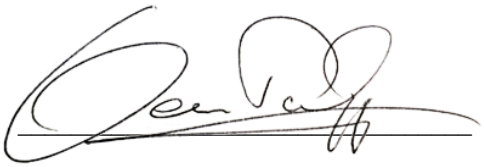
### 4.4. Auftragskontrolle (Outsourcing an Dritte)

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertragsstrafen bei Verstößen

Ausgefüllt für die Organisation durch

Philipp Kemser • Datenschutzbeauftragter • +49 89 5480194 35 • philipp.kemser@norstat.de

München, 19.10.2021



Vom Auftraggeber auszufüllen:

Geprüft am _____ durch _____ Ergebnis(se):

- ☐ Es besteht noch Klärungsbedarf zu _____ .
- ☐ TOM sind für den angestrebten Schutzzweck ausreichend
- ☐ Vereinbarung Auftragsverarbeitung kann geschlossen werden