Technische und Organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO Abs.1 S.2 lit. g

der Organisation:

Statista GmbH
Johannes-Brahms-Platz 1
20355 Hamburg

Stand: July 2022

Organisationen, 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 og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

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

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Alarmanlage	X	Schlüsselregelung / Liste
X	Automatisches Zugangskontrollsystem	X	Empfang / Rezeption / Pförtner
	Biometrische Zugangssperren	X	Besucherbuch / Protokoll der Besucher
X	Chipkarten / Transpondersysteme	X	Mitarbeiter- / Besucherausweise
X	Manuelles Schließsystem	X	Besucher in Begleitung durch Mitarbeiter
X	Sicherheitsschlösser (Serverräume)		Sorgfalt bei Auswahl des Wachpersonals
	Schließsystem mit Codesperre	X	Sorgfalt bei Auswahl Reinigungsdienste
X	Absicherung der Gebäudeschächte		
X	Türen mit Knauf Außenseite		
	Klingelanlage mit Kamera (derzeit deaktiviert)		
	Videoüberwachung der Eingänge		

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen		Organisatorische Maßnahmen	
X	Login mit Benutzername + Passwort	X	Verwalten von Benutzerberechtigungen
	Login mit biometrischen Daten	X	Erstellen von Benutzerprofilen
X	Anti-Viren-Software Server	X	Zentrale Passwortvergabe
X	Anti-Virus-Software Clients	X	Richtlinie „Sicheres Passwort“
X	Anti-Virus-Software mobile Geräte	X	Richtlinie „Löschen / Vernichten“
X	Firewall	X	Richtlinie „Clean desk“ (nicht i.a. Bereichen)

X	Intrusion Detection Systeme	X	Allg. Richtlinie Datenschutz und / oder Sicherheit
	Mobile Device Management	X	Mobile Device Policy
X	Einsatz VPN bei Remote-Zugriffen	X	Anleitung „Manuelle Desktopsperre“
X	Verschlüsselung von Datenträgern		
X	Verschlüsselung Smartphones		
	Gehäuseverriegelung		
X	BIOS Schutz (separates Passwort)		
	Sperre externer Schnittstellen (USB)		
X	Automatische Desktopsperre		
X	Verschlüsselung von Notebooks / Tablet		

Weitere Maßnahmen:

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen		Organisatorische Maßnahmen	
	Aktenschredder (mind. Stufe 3, cross cut)	X	Einsatz Berechtigungskonzepte
X	Externer Aktenvernichter (DIN 32757)	X	Minimale Anzahl an Administratoren
X	Physische Löschung von Datenträgern	X	Datenschutztresor
X	Protokollierung (abhängig vom System)	X	Verwaltung Benutzerrechte durch Administratoren

Weitere Maßnahmen:

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
X	Trennung von Produktiv- und Test-umgebung	X	Steuerung über Berechtigungskonzept
X	Physikalische Trennung (Systeme / Datenbanken / Datenträger)	X	Festlegung von Datenbankrechten
X	Mandantenfähigkeit relevanter Anwendungen	X	Datensätze sind mit Zweckattributen ver-sehen

Weitere Maßnahmen:

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

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

Weitere Maßnahmen:

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

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen		Organisatorische Maßnahmen	
X	E-Mail-Verschlüsselung	X	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
X	Einsatz von VPN	X	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
X	Protokollierung der Zugriffe und Abrufe		Weitergabe in anonymisierter oder pseudonymisierter Form
X	Sichere Transportbehälter (über Fa.Reisswolf)	X	Sorgfalt bei Auswahl von Transport Personal und Fahrzeugen
X	Bereitstellung über verschlüsselte Verbindungen wie sftp, https		Persönliche Übergabe mit Protokoll
X	Nutzung von Signaturverfahren		

Weitere Maßnahmen:

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
X	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	X	Übersicht, mit welchen Programmen welche Daten eingegeben oder gelöscht werden können
X	Manuelle oder automatisierte Kontrolle der Protokolle	X	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
		X	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
		X	Klare Zuständigkeiten für Löschungen (abhängig vom System)

Weitere Maßnahmen:

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder
Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
X	Feuer- und Rauchmeldeanlagen	X	Backup & Recovery-Konzept
X	Feuerlöscher Serverraum	X	Kontrolle des Sicherungsvorgangs
X	Serverraumüberwachung Temperatur und Feuchtigkeit	X	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
X	Serverraum klimatisiert	X	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
X	USV	X	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
X	Schutzsteckdosenleisten Serverraum	X	Existenz eines Notfallplans
X	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.	X	Getrennte Partitionen für Betriebssysteme und Dateien
X	RAID System / Festplattenspiegelung		
X	Videoüberwachung Serverraum		
	Alarmmeldung bei unberechtigtem Zutritt		

Weitere Maßnahmen:

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

Datenschutz-Management

Technische Maßnahmen		Organisatorische Maßnahmen	
X	Software-Lösungen für Datenschutzmanagement im Einsatz	X	Interner Datenschutzbeauftragter
X	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	X	Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	X	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
X	Anderweitiges dokumentiertes Sicherheits-konzept	X	Interner Informationssicherheitsbeauftragter
X	Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	X	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
		X	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
		X	Ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen:

Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen		Organisatorische Maßnahmen					
X	Einsatz von Firewall und regelmäßigen Aktualisierungen	X	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)				
X	Einsatz von Spamfilter und regelmäßige Aktualisierungen	X	Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen				
X	Einsatz von Virenscanner und regelmäßige Aktualisierung	X	Einbindung von Sicherheitsvorfällen und Datenpannen	X	DSB	X	ISB
X	Intrusion Detection System (IDS)	X	Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem				
X	Intrusion Prevention System (IPS)	X	Formaler Prozess von Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen				

Weitere Maßnahmen:

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

Privacy by design / Privacy by default

Technische Maßnahmen		Organisatorische Maßnahmen	
X	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	X	Double Opt-In Verfahren
X	Einfache Ausübung des Widerrufrechts des Betroffenen via tech. Maßnahmen		

Weitere Maßnahmen:

Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
		X	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
		X	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz- und Datensicherheit
		X	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
		X	Schriftliche Weisungen an den Auftragnehmer
		X	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
		X	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
		X	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
			Regelung zum Einsatz weiterer Subunternehmer
		X	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
		X	Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen:

Ausgefüllt für die Organisation durch

Name: Christian Wolf
Funktion: Datenschutzbeauftragter

Rufnummer: +49 40 284 841 679
E-Mail: Christian.Wolf@Statista.com

Hamburg, 29.07.2022

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

Hinweis: Diese Vorlage verwendet durchaus noch Begrifflichkeiten des BDSG a.F. Inhaltlich unterscheiden sich die technischen und organisatorischen Maßnahmen nicht von denen, die in der DSGVO gefordert werden!