Datenschutz durch technische und organisatorische Maßnahmen Amt Marne-Nordsee - TOM - Kurzliste -

Im Amt Marne-Nordsee kommen zahlreiche technische und organisatorische Maßnahmen zum Einsatz. Einige davon gelten für alle Verarbeitungstätigkeiten (z. B. Maßnahmen zur Gebäudesicherheit), andere Maßnahmen werden spezifisch für einzelne Verarbeitungstätigkeiten umgesetzt.

Nachfolgend werden wichtige technische und organisatorische Maßnahmen aufgeführt, die gemäß den Vorgaben von Artikel 32 EU-DSGVO sowie § 40 LDSG SH und verwandten Rechtsgrundlagen umgesetzt werden. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen werden technische und organisatorische Maßnahmen ergriffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Liste umfaßt nur eine **Kurzversion** aller umgesetzten technischen und organisatorischen Maßnahmen. Auf eine Veröffentlichung der konkreten Maßnahmen wurde auf Grund erhöhten Gefahrenpotentials durch Angriffe auf Stellen der öffentlichen Verwaltung verzichtet. Die Gesamtliste ist Bestandteil des Verzeichnisses der Verarbeitungstätigkeiten und wird zyklisch aktualisiert.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

1.1. Zutrittskontrolle

(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

- z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Alarmanlagen, Videoanlagen

1.2. Zugangskontrolle

(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

- z.B.: Kennwörter, automatische Sperrmechanismen, Mehrfaktor-Authentifizierung, Verschlüsselung

1.3. 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.)

- z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen

1.4. Trennungskontrolle

(Sicherstellung der getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten durch technische Vorkehrungen und Prozeßgestaltung)

- z.B. Festlegung von Datenkategorien und Einsatz mandantenfähiger Systeme

1.5. Pseudonymisierung

(Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können)

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

(Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht unautorisiert modifiziert werden können)

2.1. 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.)

- z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

2.2. 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.)

- z.B. Protokollierung und Dokumentenmanagement

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

3.1. Verfügbarkeitskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- z.B.: Backup-Strategie, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

3.2. Belastbarkeit und Wiederherstellung bei technischem Zwischenfall

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- z.B. Backups und redundante Hardwarre

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

4.1. Datenschutzmanagement

(Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM's)

- schriftliche Bestellung eines Datenschutzbeauftragten
- regelmäßige Sensibilisierung der Mitarbeiter zum Thema Datenschutz

4.2. Incident-Response-Management

(Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an die Betroffenen bzw. an die zuständige Aufsichtsbehörde erfolgt.)

- Aufstellung eines internen Incident-Response-Management-Konzepts

4.3. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(Maßnahmen, die gewährleisten, dass den Vorgaben des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) genüge getan wird.)

- z.B. Beteiligung des Datenschutzbeauftragten bei der Konzeption und Auswahl von IT-Systemen und Verarbeitungstätigkeiten

4.4. Auftragskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

- z.B. Dokumentation/Protokollierung

5. Abgeleitete Maßnahmen (Erwägungsgrund 78 EU-DSGVO)

5.1. Datenminimierung

- z.B. nur solche Daten zu erfassen, die zur Zweckerfüllung unbedingt erforderlich sind

5.2. Nichtverkettung und Zweckbindung

- z.B. getrennte Datenhaltung

5.3. Transparenz

- z.B. umfassende Dokumentation und Information über Verarbeitungstätigkeiten

5.4. Intervenierbarkeit

- z.B. Prozesse zur Wahrnehmung von Betroffenenrechten

5.5. Datenträgerkontrolle

- z.B. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern durch technische Vorkehrungen und Prozeßgestaltung

5.6. Speicherkontrolle

- z.B. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

5.7. Benutzerkontrolle

- z.B. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

5.8. Übertragungskontrolle

- z.B. Dokumentation/Protokollierung der Übertragung von personenbezogener Daten mit Hilfe von Einrichtungen zur Datenübertragung

5.9. Transportkontrolle

- z.B. Dokumentation/Protokollierung während der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern

Dokumentinformationen:

Inhalt/Titel:	Datenschutz durch technische und organisatorische Maßnahmen im Amt Marne-Nordsee - Kurzliste“			
Amt/Fachbereich:	Amt-Marne-Nordsee / Datenschutz			
Autor/Ersteller:	GEHE			
Dateiname:	a68d6114f9bf433582125b35df2fb69e.docx			
Bearbeitung:	**Bearbeiter**	**Datum Bearbeitung**	**Datum Freigabe**	**Bemerkung**
	GEHE	01.06.2021		keine
	GEHE	29.06.2021		keine