Kurzfassung der technischen und organisatorischen Maßnahmen des Amtes Marne-Nordsee
- TOM -

Datenschutz durch technische und organisatorische Maßnahmen – TOM

In unserem Amt 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 DSGVO sowie § 40 LDSG 2018 und verwandten Rechtsgrundlagen umgesetzt sind.

Vertraulichkeit

- Zutrittssicherung zu Gebäude und Räumlichkeiten der Amtsgebäude (Transponderschlösser)
- spezifische Zutrittssicherung von IT-Systemräumen (Transponder-/Codeschlösser)
- Zutrittsschutz und Zugangsschutz gegen unbefugte Kenntnisnahme von Datenträgern in den Räumlichkeiten der Amtes (Richtlinie mobile Datenträger, USB-Stick Verbot)
- erhöhte Sicherungsmechanismen für besonders vertrauliche Daten (bei papierbasierten und elektronischen Daten) (Richtlinie für Arbeitsplatz und Umgang mit vertraulichen Daten)
- Zugriffsschutz gegen unbefugte Kenntnisnahme von elektronischen Datenbeständen (insbesondere E-Mails, Dateien, Datenbestände in Datenbanken) (Least Privilege, Need to Know, AD-Rechtevergabe)
- regelmäßige Kontrolle von vergebenen Zugriffsberechtigungen
- Authentisierungs-, Autorisierungs- und Accountingkonzept (Tripple-A)
- Verschlüsselung
    - verschlüsselte Mobilgeräte (Datenträgerverschlüsselung)
    - spezifische Verschlüsselung besonders zu sichernder Daten
    - verschlüsselte Datenübertragung von und zu Webservern
    - standardmäßige Transportverschlüsselung (TLS) von E-Mails

Integrität

- Zutrittsschutz und Zugangsschutz gegen unbefugte Manipulation von IT-Geräten
- Zugriffsschutz gegen unbefugte Manipulation von elektronischen Datenbeständen (VLAN, Kennwortrichtlinie)
- Schutz gegen Schadsoftware (Firewall, AV-Scan Dateien und E-Mails)
- teilautomatisiertes Einspielen von Sicherheitsupdates (Firewall, AV, E-Mailscanner)
- automatisierte asynchrone Datensicherung (dayly, weekly, yearly)

Verfügbarkeit

- Vorhalten von Ersatzhardware (für Clients und Server)
- automatisierte synchrone Datenspiegelung (Clustering Datacores, physisch getrennte Sicherheitszonen)
- Zutrittsschutz und Zugangsschutz gegen unbefugtes Löschen von Datenträgern (Codeschlösser)
- Zugriffsschutz gegen unbefugtes Löschen von elektronischen Datenbeständen (Kennworte, Rechteverwaltung)
- Schutz vor Verlust von elektronischen Datenbeständen und Datenträgern (Backup, RAID, Verschlüsselung)

Belastbarkeit und Wiederherstellung bei technischem Zwischenfall

- redundante Hardware
- Dokumentation und Prozessbeschreibungen für die Wiederherstellung
- regelmäßige synchrone Datenspiegelung mit Wiederherstellungsautomatismen
- regelmäßige Tests der Datensicherung inkl. Wiederherstellungsfunktionen
- automatisierte Meldung auftretender Fehlfunktionen (Zuverlässigkeit)

Datenminimierung

- Festlegung von kurzen Löschfristen zur Umsetzung der Speicherminimierung
- Automatisierung von Löschungsvorgängen
- Aggregation von Daten für statistische Auswertungen (personenbezogene Daten für diesen Zweck nicht mehr benötigt)

Nichtverkettung und Zweckbindung

- getrennte Datenhaltung mit zweckspezifischen Zugriffsrechten bei papierbasierten und elektronische Daten
- zweckspezifische Kennzeichnung von Daten, sofern diese nicht getrennt verarbeitet werden

Transparenz

- umfassende Dokumentation und Information über Verarbeitungstätigkeiten der Amtes
- Information bei der Erhebung mittels Print- und Webformularen
- Dokumentation

Intervenierbarkeit

- Mechanismen zur Änderung und Löschung in Dateisystemen und Datenbanken und E-Mailsystemen
- Prozesse zur Wahrnehmung von Betroffenenrechten

Datenträgerkontrolle

- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern durch technische Vorkehrungen und Prozeßgestaltung (Rechtestruktur und Management)

Speicherkontrolle

- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten durch technische Vorkehrungen und Prozeßgestaltung (Rechtestruktur und Management)

Benutzerkontrolle

- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (siehe Vertraulichkeit) (VPN)

Übertragungskontrolle

- Dokumentation/Protokollierung der Übertragung oder der zur Verfügungstellung von personenbezogener Daten mit Hilfe von Einrichtungen zur Datenübertragung durch technische Vorkehrungen und Prozeßgestaltung (EMS, Archivierung von Daten und E-Mails)

Eingabekontrolle

- automatische Protokollierung, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben wurden oder verändert worden sind (EMS)

Transportkontrolle

- Dokumentation/Protokollierung während der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern zur Aufrechterhaltung von Vertraulichkeit und Integrität der Daten (Richtlinie mobile Datenträger, kein Transport mobiler Datenträger zulässig) (getrennte Fachanwendungen und Rechtestruktur)

Auftragskontrolle

- Dokumentation/Protokollierung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragsverarbeitungsverträge, Audits)

Trennbarkeit

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

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- standardmäßige Beteiligung der bzw. des Datenschutzbeauftragten bei der Konzeption und Auswahl von IT-Systemen und Verarbeitungstätigkeiten
- Verzicht auf Protokollierungen von Datenverarbeitungsvorgängen, soweit dies nicht gesetzlich vorgeschrieben ist, dem Integritätsschutz dient oder aus Sicherheitsgründen erforderlich ist

Datenschutzmanagement

- standardmäßige Beteiligung der bzw. des Datenschutzbeauftragten an Prozessen zu Beschaffungen und Entwicklungen von IT-Systemen und Verarbeitungstätigkeiten (Aufbau notwendiger Prozesse)
- interne Strategien zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der technisch und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Audits, Stichproben, Verwendung PDCA-Zyklus)
- Aufbau und Betrieb eines Datenschutzmanagementsystems (DSMS im Aufbau)

Dokumentinformationen:

Inhalt/Titel:	Datenschutz-Steckbrief/Datenschutzerklärung/Informationen zu Datenverarbeitung: „Datenschutz durch technische und organisatorische Maßnahmen im Amt Marne-Nordsee“			
Amt/Fachbereich:	Amt-Marne-Nordsee / Datenschutz			
Autor/Ersteller:	GEHE			
Dateiname:	datenschutz_technisch-und-organisatorische-massnahmen-bewerbungsverfahren_amt-marne-nordsee.docx			
Bearbeitung:	**Bearbeiter**	**Datum Bearbeitung**	**Datum Freigabe**	**Bemerkung**
	GEHE	19.10.2019		keine
	GEHE	11.08.2020		keine
	GEHE	01.09.2020		keine
	GEHE	10.11.2020		keine
	GEHE	18.01.2021	**X**	