Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der

Sparkasse LeerWittmund

Mühlenstr. 93

26789 Leer

(Stand : Januar 2019)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- ☒ Zutrittskontrolle
- ☒ Sicherheit bei Türen und Fenstern
- ☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☒ Alarmanlage
- ☒ Videoüberwachung
- ☒ Spezielle Schutzvorkehrungen des Serverraums
- ☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☒ Nicht-reversible Vernichtung von Datenträgern
- ☒ Mitarbeiter- und Berechtigungsausweise
- ☒ Sperrbereiche
- ☒ Besucherregelung (u.a. Abholung am Empfang, Begleitung nach dem Besuch bis zum Ausgang)

b) Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- ☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☒ Autorisierungsprozess für Zugangsberechtigungen
- ☒ Begrenzung der befugten Benutzer
- ☒ Berechtigungskonzept
- ☒ Kennwortverfahren (Vorgaben bzgl. Komplexität und Aktualisierungsintervall)
- ☒ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
- ☒ Protokollierung des Zugangs
- ☒ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität
- ☒ Firewall

c) Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- ☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☒ Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die

Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.

- ☒ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☒ Autorisierungsprozess für Berechtigungen
- ☒ Genehmigungsroutinen
- ☒ Profile/Rollen gemäß Berechtigungskonzept
- ☒ Verschlüsselung bei Geräten, Systemen, Daten, Mail
- ☒ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (Härtung von Systemen wie z.B. Sperrung von Ports an Systemen)
- ☒ „Mobile Device Management-System“ (Sicherheit bei mobilen Geräten)
- ☒ Vier-Augen-Prinzip
- ☒ Funktionstrennung
- ☒ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☒ Nicht-reversible Löschung von Datenträgern

d) Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- ☒ Speicherung von Datensätzen in physikalisch getrennten Datenbanken
- ☒ Verarbeitung auf getrennten Systemen
- ☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☒ Mandantenfähigkeit von IT-Systemen
- ☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☒ Einsatz von Test-, Entwicklungs- und Produktionsumgebung

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Bei der Pseudonymisierung erfolgt 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.

Die Gestaltung und Auswahl von Datenverarbeitungssystemen in unserem Unternehmen richten sich nach dem Ziel aus, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Die Grundsätze der Datenvermeidung bzw. Datensparsamkeit werden dabei beachtet. Insbesondere wird von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☒ Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)
- ☒ Verschlüsselung des Speichermediums von Laptops
- ☒ Gesicherter File Transfer (z.B. sftp)
- ☒ Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- ☒ Verschlüsselung bei Geräten, Systemen, Daten, Mail
- ☒ Physikalische Transportsicherung
- ☒ Verpackungs- und Versandvorschriften
- ☒ Elektronische Signatur

- ☒ Gesichertes WLAN
- ☒ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Rückrufautomatik, Einmal-Passwort)
- ☒ „Mobile Device Management-System“(Sicherheit bei mobilen Geräten)
- ☒ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☒ Protokollierung von Datenübertragung oder Datentransport
- ☒ Protokollierung von lesenden Zugriffen
- ☒ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

b) Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- ☒ Zugriffsrechte
- ☒ Systemseitige Protokollierungen
- ☒ Dokumenten Management System (DMS) mit Änderungshistorie
- ☒ Sicherheits-/Protokollierungssoftware
- ☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☒ Mehraugenprinzip

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- ☒ Sicherheitskonzept für Software- und IT-Anwendungen
- ☒ Back-Up Verfahren
- ☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates
- ☒ Absicherung von IT-Systemen (RAID, Spiegeln, Clustering)
- ☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☒ Brand- und/oder Löschwasserschutz des Serverraums
- ☒ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☒ Klimatisierter Serverraum
- ☒ Virenschutz
- ☒ Firewall
- ☒ Notfallplan
- ☒ Erfolgreiche Notfallübungen

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

a) Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- ☒ Datenschutzleitbild
- ☒ Datenschutz-Richtlinie
- ☒ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit (z.B.: im Unternehmenshandbuch unseres Unternehmens)
- ☒ Bestellung eines Datenschutzbeauftragten
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- ☒ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten

- ☒ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- ☒ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- ☒ Etabilertes Informationssicherheitsmanagement (inkl. Ext. Prüfung/Auditierung der Informationssicherheit)

b) Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- ☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- ☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt. Da sich im zeitlichen Verlauf die Anforderungen bzgl. der Geeignetheit der Maßnahmen ändern können, handelt es sich bei Privacy by Design/Default nicht um einen einmaligen Vorgang, sondern vielmehr um einen fortlaufenden Prozess. Dabei werden zwei Aspekte adressiert. Einerseits wird sowohl bei der Planung, also zum Zeitpunkt der Festlegung der Zwecke und Mittel der Verarbeitung, als auch zum „Zeitpunkt der eigentlichen Verarbeitung“ geeignete Maßnahmen ergriffen („Datenschutz durch Technikgestaltung“). Andererseits wird die Verarbeitung mit „datenschutzfreundliche Voreinstellungen“ durchgeführt. Dabei müssen die getroffenen technischen und organisatorischen Maßnahmen geeignet sein,

- die Datenschutzgrundsätze wirksam umzusetzen und
- die notwendigen Garantien bieten, um den Anforderungen dieser Verordnung zu genügen und
- die Rechte der betroffenen Personen schützen.

d) Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- ☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☒ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☒ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☒ Unabhängige Auditierung der Weisungsgebundenheit
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis (Vertraulichkeitsverpflichtung)
- ☒ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☒ formalisiertes Auftragsmanagement
- ☒ dokumentiertes Verfahren zur Auswahl des Dienstleisters
- ☒ formalisiertes Auftragsmanagement
- ☒ standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister, Dienstleistersteuerung