Anlage 2 Technische- und organisatorische Maßnahmen (TOM)

Version: 004
Stand: 22.05.2026

Letzte Änderung durch: Andreas Lusch, Peter Ruhtz

Verantwortlicher: Andreas Lusch
Obentrautstr. 32
10963 Berlin

Tel: +49(0)30 92215617
Email: lusch@luxpc.de
Web: www.luxpc.de

Ansprechpartner zur Datensicherheit:

Andreas Lusch
Obentrautstr. 32
10963 Berlin

Tel: +49(0)30 92215617
Email: lusch@luxpc.de
Web: www.luxpc.de

Inhalt

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Zutrittskontrolle

Ziel: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	**Beispiele für Maßnahmen zur Zutrittskontrolle:** ▪ Physikalische Absicherung (Türen, Fenster, Wände etc.), Zutrittskontrollsysteme ▪ Geregelte Schlüsselverwaltung ▪ Beaufsichtigung von Fremdpersonal ▪ Gebäudeüberwachung ▪ Gesicherte Aufbewahrung von Unterlagen und Datenträgern ▪ …
Realisierte Maßnahmen:	

- physikalische Absicherung
  ○ Rollläden bzw. Gitter an Türen und Fenster
  ○ Einbruchmeldeanlage
  ○ Server im abgeschlossenen Stahlschrank
  ○ Manuelles Schließsystem mit Sicherheitsschlössern
  ○ Videoüberwachung des Publikumsbereichs
 	
- organisatorische Absicherung
  ○ geregelte Schlüsselverwaltung
  ○ Beaufsichtigung von Fremdpersonal
  ○ Besucher in Begleitung durch Mitarbeiter
  ○ Sorgfalt bei Auswahl Reinigungsdienste	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Zugangskontrolle

Ziel: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	**Beispiele für Maßnahmen:** ▪ Sichere Authentifizierung ▪ Passwort-Regeln (Länge, Komplexität, Historie, Änderungsfrequenz) ▪ Protokollierung von Benutzeranmeldungen ▪ Maßnahmen bei vergeblichen Anmeldeversuchen ▪ Bildschirmsperren ▪ Eindeutige Benutzerkennungen ▪ …
Realisierte Maßnahmen:	

- Technische Maßnahmen
  - Login mit Benutzername und Passwort
  - Wo möglich Multifaktor Authentifizierung
  - Hardware Firewall
  - Verschlüsselung aller Clients
  - Verschlüsselung aller mobilen Datenträger oder Transport im verschlossenen Transportbehälter
  - Verschlüsselung Smartphones
  - Intrusion Detection System
  - Einsatz VPN bei Remote-Zugriffen
  - Verwalten von Benutzerberechtigungen

- Organisatorische Maßnahmen
  - Anleitung „Manuelle Desktopsperre“
  - Allg. Richtlinie Datenschutz und / oder Sicherheit
  - Zentrale Passwortvergabe
  - Richtlinie „Sicheres Passwort“
  - Richtlinie „Löschen / Vernichten“

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Zugriffskontrolle

Ziel: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung bei der, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	**Beispiele für Maßnahmen:** ▪ Restriktives Berechtigungskonzept ▪ Nachvollziehbare Rechtevergabe (inklusive Administrationsrechte) ▪ Sicherheitsvorkehrungen auf Applikationsebene ▪ Netzsegmentierung ▪ Sichere Netzwerkübergänge ▪ Virenschutzkonzept ▪ …
Realisierte Maßnahmen:	

- Technische Maßnahmen
  ○ Akten Schredder (cross cut)
  ○ Physische Löschung von Datenträgern
  ○ Akten der Kategorie besonders schützenswert befinden sich in abgeschlossenen Schränken
  ○ Trennung zwischen Produktiv- und Gäste bzw. Kundennetzwerk
  ○ Anti-Virus-Software auf allen Servern
  ○ Anti-Virus-Software auf allen Clients
 	
- Organisatorische Maßnahmen
  ○ Einsatz von Berechtigungskonzepten
  ○ Minimale Anzahl an Administratoren
  ○ Verwaltung Benutzerrechte durch Administratoren	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Trennungskontrolle

Ziel: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.	**Beispiele für Maßnahmen:** ▪ physikalische Trennung ▪ logische Mandantentrennung (softwareseitig) ▪ Versehen der Datensätze mit Zweckattributen/ Datenfeldern ▪ Erstellung eines Berechtigungskonzepts ▪ Sandboxing ▪ Trennung von Produktiv- und Testsystem ▪ …
Realisierte Maßnahmen:	
- Technische Maßnahmen o Trennung von Produktiv- und Test-umgebung o Trennung unterschiedlicher Mandanten (Systeme / Datenbanken / Datenträger) o Mandantenfähigkeit relevanter Anwendungen - Organisatorische Maßnahmen o Steuerung über Berechtigungskonzept o Festlegung von Datenbankrechten	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Pseudonymisierung

Ziel: 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.	**Beispiele für Maßnahmen:** ▪ Nutzung von Pseudonymisierung wo möglich (u.a. bei Weitergabe) ▪ geeignete Wahl der Pseudonymisierungsschlüssel ▪ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System ▪ **…**
Realisierte Maßnahmen:	
- Technische Maßnahmen ○ - Organisatorische Maßnahmen ○	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Weitergabekontrolle

Ziel: Es ist zu 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	**Beispiele für Maßnahmen:** ▪ Absicherung der Übermittlung durch Verschlüsselungsverfahren ▪ Überprüfung der Integrität übertragener Daten ▪ Protokollierung der Weitergabe ▪ Abgesicherter Datenträgertransport ▪ Datenschutzkonforme Vernichtung von Datenträgern ▪ **…**
Realisierte Maßnahmen:	
- Technische Maßnahmen ○ Bereitstellung über verschlüsselte Verbindungen wie https, TLS ○ Sichere Transportbehälter ○ Protokollierung der Zugriffe und Abrufe ○ Einsatz von VPN ○ Email-Verschlüsselung - Organisatorische Maßnahmen ○ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen ○ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen ○ Sorgfalt bei Auswahl von Transport, Personal und Fahrzeugen ○ Datenschutzkonforme Vernichtung von Datenträgern	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Eingabekontrolle

Ziel: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	**Beispiele für Maßnahmen:** ▪ Protokollierung von Eingaben in Anwendungen ▪ Benutzerbezogene Protokollierung von Netzwerkaktivitäten ▪ Verwendung von elektronischen Signaturen bei Eingaben/Löschungen/Änderungen ▪ …
Realisierte Maßnahmen:	

- Technische Maßnahmen
  ○ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
  ○ Manuelle oder automatisierte Kontrolle der Protokolle
 	
- Organisatorische Maßnahmen
  ○ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen
  ○ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
  ○ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
  ○ Klare Zuständigkeiten für Löschungen	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Auftragskontrolle (Outsourcing)

Ziel: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	**Beispiele für Maßnahmen:** ▪ Vertragliche Vereinbarungen nach § 11 BDSG ▪ Sorgfältige Auswahl der Unterauftragsdatenverarbeiter ▪ Prozessbeschreibungen zur Umsetzung der Weisungen ▪ …
Realisierte Maßnahmen:	
- Technische Maßnahmen o - Organisatorische Maßnahmen o Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation o Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) o Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung o Schriftliche Weisungen an den Auftragnehmer o Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis o Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei vorliegender Bestellpflicht oder eines Datenschutzverantwortlichen o Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer o Regelung zum Einsatz weiterer Subunternehmer o Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags o Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Verfügbarkeitskontrolle

Ziel: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.	**Beispiele für Maßnahmen:** ▪ RAID ▪ Intrusion Detection ▪ BackUp Konzept ▪ Brandmeldeanlage ▪ USV ▪ Hard- und Software Firewall ▪ …

Realisierte Maßnahmen:

- Technische Maßnahmen
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöscher Serverraum
  - USV – unterbrechungsfreie Stromversorgung
  - Schutzsteckdosenleisten flächendeckend
  - RAID System / Festplattenspiegelung
  - Schattenkopien
  - Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

- Organisatorische Maßnahmen
  - Backup & Recovery-Konzept (ausformuliert)
  - Kontrolle des Sicherungsvorgangs
  - Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
  - Georedundante Aufbewahrung von Sicherungsmedien
  - Keine sanitären Anschlüsse im oder oberhalb des Serverraums
  - Getrennte Partitionen für Betriebssysteme und Daten, wo möglich

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Wiederherstellbarkeit

Ziel: (Art. 32 Abs. 1 lit. c DSGVO)	**Beispiele für Maßnahmen:** ▪ Erstellen eines Notfallplans ▪ Nutzung virtueller Maschinen mit Offsitesicherung ▪ passender Hardware-Service-Vertrag ▪ eigene Ersatzteilbevorratung ▪ Wartungsverträge mit geeigneter Reaktionszeit ▪ …
Realisierte Maßnahmen:	

- Technische Maßnahmen
  ○ Nutzung virtueller Maschinen mit Offsitesicherung
  ○ eigene Ersatzteilbevorratung
 	
- Organisatorische Maßnahmen
  ○ Wartungsverträge mit geeigneter Reaktionszeit
  ○ Existenz eines Notfallplans	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Datenschutz-Management

Ziel:	**Beispiele für Maßnahmen:** ▪ Bestellung eines Datenschutzbeauftragten ▪ Einsatz vom Datenschutzkoordinatoren ▪ Verzeichnis von Verarbeitungstätigkeiten ▪ Datenschutzfolgeabschätzungen ▪ Schulungsmaßnahmen/ Sensibilisierungsmaßnamen mit Nachweis ▪ Verpflichtung auf Vertraulichkeit der Mitarbeiter ▪ …
Realisierte Maßnahmen:	
- Technische Maßnahmen o Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung o Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt o Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO o Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener - Organisatorische Maßnahmen o Interner Datenschutzverantwortlicher o Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet o Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich o Interner Informationssicherheitsbeauftragter o Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Incident-Response-Management (Vorfallreaktionsplan)

Ziel: Mithilfe des Vorfallreaktionsplan sollen Sicherheitsvorfälle entdeckt und angemessene Reaktionen hinterlegt werden, die wiederum zur Limitierung der Auswirkungen führen.	**Beispiele für Maßnahmen:** ▪ Definition von Zuständigkeiten und Verantwortlichkeiten für Vorfälle (z.B. Vorfallteam) ▪ definierter Meldeprozess ▪ definierte Maßnahmen für relevante und denkbare Vorfälle ▪ definierte Eskalationswege ▪ aktuelle Melde- und Kontaktlisten ▪ …

Realisierte Maßnahmen:

- Technische Maßnahmen
  - Einsatz von Firewall und regelmäßige Aktualisierung
  - Einsatz von Spamfilter und regelmäßige Aktualisierung
  - Einsatz von Webfilter und regelmäßige Aktualisierung
  - Einsatz von Virenscanner und regelmäßige Aktualisierung
  - Intrusion Detection System (IDS)
  - Patchmanagement der Betriebssysteme und Programme

- Organisatorische Maßnahmen
  - Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
  - Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
  - Dokumentation von Sicherheitsvorfällen und Datenpannen
  - definierter Meldeprozess

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de

Datenschutzfreundliche Voreinstellungen

Ziel: ist der Grundsatz, wonach eine Organisation (der Verantwortliche) sicherstellt, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden (ohne Eingreifen des Nutzers).	**Beispiele für Maßnahmen:** ▪ Prozess zur Sicherstellung von Privacy by Design bei Änderungen ▪ Prozess zur Sicherstellung von Privacy by Default bei Änderungen ▪ …
Realisierte Maßnahmen:	

- Technische Maßnahmen
  ○ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
 	
- Organisatorische Maßnahmen
  ○ Richtlinie „Datensparsame Grundeinstellung“	

LuxPC ♦ Andreas Lusch ♦ Obentrautstr. 32 ♦ 10963 Berlin
030 / 922 156 17 ♦ www.LuxPC.de ♦ mail@LuxPC.de