

Kostenlose Vorlage:
Anforderungen an die technischen und organisatorischen
Maßnahmen (TOM) von Auftragsverarbeitern

Bei diesem Dokument handelt es sich um eine kostenlose Vorlage bzw. Checkliste der activeMind AG zu den Themenbereichen Datenschutz und Datensicherheit. Die aktuellste Version finden Sie stets [im Downloadbereich unserer Website](https://www.activemind.de/datenschutz/dokumente/).

Sie können dieses Dokument an die Bedürfnisse in Ihrem Unternehmen anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass die activeMind AG keinerlei Haftung übernimmt.

Hinweis: In einigen unserer Datenschutz-Vorlagen finden Sie Infoboxen dieser Art. Sie geben wichtige Hinweise darauf, wie bestimmte Aspekte zu handhaben sind. Sie können und sollten diese Boxen natürlich aus Ihrem angepassten Dokument entfernen.

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der activeMind AG

Telefon: +49 (0)89 / 91 92 94 – 900
E-Mail: anfrage@activemind.de
Web: <https://www.activemind.de>

Anforderungen an die technischen und organisatorischen Maßnahmen (TOM) von Auftragsverarbeitern

Gesetzliche Grundlagen zu technischen und organisatorischen Maßnahmen

**Art. 32 DSGVO – „Sicherheit der Verarbeitung“**

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten.

Maßstab der Erforderlichkeit bestimmt sich nach dem mit der Datenverarbeitung verbundenen Risiko für den Betroffenen. Zu berücksichtigen sind Eintrittswahrscheinlichkeit und Schwere möglicher physischer, materieller oder immaterieller Schäden des Betroffenen welche durch Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von personenbezogenen Daten eintreten können.

Je höher das Risiko, desto umfangreicher die erforderlichen Maßnahmen.

**Technische und organisatorische Maßnahmen**

Werden personenbezogene Daten verarbeitet, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Diese Maßnahmen schließen unter anderem, aber nicht ausschließlich, folgende Maßnahmen ein:

1. Pseudonymisierung;
2. Verschlüsselung;
3. Gewährleistung der Vertraulichkeit;
4. Gewährleistung der Integrität;
5. Gewährleistung der Verfügbarkeit;
6. Gewährleistung der Belastbarkeit der Systeme;
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall;
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

# Pseudonymisierung

Ziel ist es, Unbefugten eine Identifizierbarkeit von natürlichen Personen zu erschweren. Pseudonymisierung erfolgt dadurch, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen keine Identifizierung der betroffenen Person ermöglichen. Hierbei werden Identifikationsmerkmale einer Person durch ein Kennzeichen ersetzt. Diese zusätzlichen Informationen werden dabei gesondert und sicher aufbewahrt.

**Maßnahmen**

|  |
| --- |
| DatenminimierungPrüfen, ob die Zwecke der Datenverarbeitung auch bei Pseudonymisierung erreicht werden können:* Produktivsystem
* Testsystem
 |

# Verschlüsselung

Verschlüsselung bietet Schutz vor Veränderungen und unbefugter Offenlegung oder unbefugtem Zugang zu den Daten. Das eingesetzte Verschlüsselungsverfahren muss dem Stand der Technik entsprechen.

**Maßnahmen**

|  |  |
| --- | --- |
| Schriftliche Regelungen für die Verschlüsselung  |  |
| Verschlüsselung von Datenträgern* Vertrauliche Datenträger
* Laptopfestplatten
* Mobile Datenträger
 |
| Verschlüsselte Speicherung von Daten* Verwendete Schlüsselalgorithmen
* Verwendete Hash-Funktionen
 |
| Verschlüsselung bei der Übermittlung* Citrix-Verbindung (128 Bit verschlüsselt)
* VPN-Verbindung (IP-Sec)
* E-Mail Versand mit verschlüsselten ZIP-Dateien
* Datenaustausch über https-Verbindung
* Verschlüsselung von Netzwerken
 |
| Zentrale Schlüsselverwaltung |  |
| Sonstiges |  |

# Vertraulichkeit

Ziel ist es, einen sicheren Schutz vor Zugriffen unbefugter Personen auf Datenverarbeitungsanlagen und Verfahren zu gewährleisten.

**Maßnahmen**

|  |
| --- |
| Zutrittskontrolle z. B.:* Berechtigungsausweise
* Elektronische Zutrittscodekarten/Zutrittstransponder
* Zutrittsberechtigungskonzept
* Videoüberwachung
* Alarmanlage
* Schlüsselregelung
* Begleitung von Besucherzutritten durch eigene Mitarbeiter
* Anwesenheitsaufzeichnungen von Besucherzutritten
* Abgestufte Sicherheitsbereiche und kontrollierter Zutritt
* Gesondert gesicherter Zutritt zum Rechenzentrum
* Aufbewahrung der Server in verschlossenen Räumen
* Aufbewahrung der Datenträger unter Verschluss bzw. abgeschlossenen Räumen
 |
| Zugangskontrolle z.B:* Verschluss von Datenverarbeitungsanlagen
* Passwortsicherung von Bildschirmarbeitsplätzen
* Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
* Verwendung von individuellen Passwörtern
* Automatisierte Sperrung von Accounts nach mehrfacher Fehleingabe von Passwörtern
* Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
* Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität
* Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
* Prozess zum Rechteentzug bei Abteilungswechsel von Mitarbeitern
* Prozess zum Rechteentzug bei Austritt von Mitarbeitern
* Verpflichtung zur Vertraulichkeit
* Protokollierung und Auswertung der Systembenutzung
 |
| Zugriffskontrollez.B:* Festlegung der Zugriffsberechtigung, Berechtigungskonzept
* Regelung zur Wiederherstellung von Daten aus Backups
* Regelmäßige Überprüfung von Berechtigungen
* Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
* Regelmäßige Auswertung von Protokollen (Logfiles)
* Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)
* Protokollierung von Dateizugriffen und -löschungen
* Sicherheitssysteme (z.B. Virenscanner, Firewalls, SPAM-Filter)
 |
| Trennungskontrollez.B:* Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)
* Dateiseparierung bei Datenbanken
* Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
* Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)
* Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt
* Funktionstrennung
* Trennung von Entwicklungs-, Test und Produktivsystem
 |
| Sonstiges |  |

# Integrität

Ziel ist es, die Manipulation und Veränderung von Daten zu verhindern.

**Maßnahmen**

|  |
| --- |
| Weitergabekontrolle* Sichere Versandart der Daten zwischen Auftraggeber und Dritten
* Gesicherter Eingang für An- und Ablieferung
* Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle
* Festlegung der Bereiche, in dem sich Datenträger befinden müssen
* Kontrollierte Vernichtung von Datenträgern (Physikalische Zerstörung oder überschreiben)
* Kontrollierte Zerstörung von Papierdokumenten (Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleiter
* Sicherungskopien von Datenträgern, die transportiert werden müssen
* Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege
* Verpackungs- und Versandvorschriften
* Vollständigkeits- und Richtigkeitsprüfung
 |
| Eingabekontrolle* Kennzeichnung erfasster Daten
* Festlegung von Benutzerprofilen
* Differenzierte Benutzerberechtigungen: Lesen/Ändern/Löschen
* Teilzugriff bei Datenbanken
* Organisatorische Festlegung von Eingabezuständigkeiten
* Protokollierung von Eingaben/Löschungen
* Protokollauswertungssystem
* Verpflichtung auf das Datengeheimnis
* Über OS-Standard hinausgehende Log-Konzept
* Dezidierter Logserver
* Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)
* Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke
 |
| Sonstiges |  |

# Verfügbarkeit und Belastbarkeit

Ziel ist die Daten gegen zufällige Zerstörung oder Verlust zu schützen sowie zu gewährleisten, dass die Systeme mit risikobedingten Veränderungen umgehen können und eine Toleranz mit Ausgleichsfähigkeit gegenüber Störungen aufweisen.

**Maßnahmen**

|  |
| --- |
| Verfügbarkeitskontrolle* Datensicherungs- und Backupkonzepte
* Durchführung der Datensicherungs- und Backupkonzepte
* Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
* Brandmeldeanlagen in Serverräumlichkeiten
* Rauchmelder in Serverräumlichkeiten
* Wasserlose Brandbekämpfungssysteme in separaten Räumlichkeiten und Brandabschnitt
* Klimatisierte Serverräumlichkeiten
* Serverräumlichkeiten in separaten Brandabschnitt
* Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt
* Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft
* Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
* CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten
* Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen
* Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)
* Einbeziehung des Einflusses angrenzender baulicher Einrichtungen
* Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)
* USV-Anlage (Unterbrechungsfreie Stromversorgung)
* Stromgenerator
 |
| Widerstandsfähigkeits- und Ausfallsicherheitskontrollez.B.:* Ausweich-Rechenzentren
* Redundante Stromversorgung / USV-Anlage / Stromgeneratoren / Klimatisierung / Brandbekämpfung
* Datenspeicherung auf RAID-Systemen
* Durchführung von Penetrationstests
* Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
* Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.
 |
| Sonstiges |  |

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Ziel ist es, durch regelmäßige Prüfungen und Evaluierungen die Risikoangemessenheit zu bewerten um entsprechende Anpassungsmaßnahmen vorzunehmen. Insbesondere können sich neue Risiken durch die stetige Entwicklung der Technik ergeben.

**Maßnahmen**

|  |
| --- |
| Kontrollverfahren* Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert
* Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
* Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten
* Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
* Es werden datenschutzfreundliche Voreinstellungen gewählt
* Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen
* Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt
* Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).
 |
| Auftragskontrolle* Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
* Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
* Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)
* Vor-Ort-Kontrollen beim Auftragnehmer
* Überprüfung des Datensicherheitskonzepts beim Auftragnehmer
* Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer
* Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.
 |
| Sonstiges |  |

# Auftragsspezifische Zusatzmaßnahmen

Ziel ist es, die besonderen Risiken, die sich aus dem spezifischen Auftrag ergeben können, zu minimieren.

**Maßnahmen**

|  |
| --- |
|  |