1. **Technisch-organisatorische Maßnahmen des Archivinhabers**

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen[[1]](#footnote-1).

|  |  |  |
| --- | --- | --- |
| 1. | **Pseudonymisierung**Wie wird die Pseudonymisierung der Daten gewährleistet?Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden. | [ ]  Personenbezogene Daten werden durch Zufallscodes ersetzt[ ]  Data Masking[ ]  Sonstige:       |
| 2. | **Verschlüsselung**Wie wird die Verschlüsselung gewährleistet?Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. | [ ]  Nutzung von kryptografischen Tools[ ]  Data Hashing [ ]  Verschlüsselung von Speichermedien[ ]  Verschlüsselung der Kommunikation [ ]  Sonstige:       |
| 3. | **Fähigkeit der Vertraulichkeit**Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet?Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind. | [ ]  Elektronisches Zutrittskontrollsystem[ ]  Sicherheitstüren und/oder -fenster[ ]  Gitter vor Fenstern und Türen[ ]  Werkschutz, Pförtner[ ]  Alarmanlage[ ]  Videoüberwachung[ ]  Spezielle Schutzvorkehrungen für den Serverraum[ ]  Individueller Log-In und Kennwortverfahren[ ]  Zusätzlicher Log-In für bestimmte Anwendungen[ ]  Automatische Sperrung der Clients (Zeitablauf)[ ]  Verwaltung von Berechtigungen[ ]  Dokumentation von Berechtigungen[ ]  Verschlüsselung von Systemen[ ]  Verschlüsselung der Kommunikation [ ]  Verschlüsselung von Datenträgern[ ]  VPN (Virtual Private Network)[ ]  Gesichertes WLAN[ ]  SSL-Verschlüsselung bei Web-Access |
| 4. | **Fähigkeit der Integrität**Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet?Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. | [ ]  Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern[ ]  Verwendung von Zugriffsrechten[ ]  Systemseitige Protokollierungen[ ]  Funktionelle Verantwortlichkeiten[ ]  Sonstige:       |
| 5. | **Fähigkeit der Verfügbarkeit**Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet?Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können. | [ ]  Back-Up Verfahren[ ]  Spiegeln von Festplatten[ ]  Unterbrechungsfreie Stromversorgung (USV)[ ]  Virenschutz /Firewall[ ]  Notfallplan[ ]  Klimaanlagen[ ]  Brand- und Löschwasserschutz[ ]  Alarmanlage[ ]  Geeignete Archivierungsräumlichkeiten[ ]  Sonstige:       |
| 6. | **Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet?Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist. | [ ]  Penetrationstests[ ]  Sonstige:       |
| 7. | **Wiederherstellbarkeit der Verfügbarkeit und des Zugangs**Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind? | [ ]  Back-Up Verfahren[ ]  Unterbrechungsfreie Stromversorgung (USV)[ ]  Notfallplan[ ]  Vertretungsregelungen[ ]  Sonstige:       |
| 8. | **Verfahren zur regelmäßigen Überprüfung**Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden? | [ ]  Es existiert eine festgelegte Prüfroutine[ ]  Prüfberichte werden evaluiert[ ]  Implementierung von Verbesserungsvorschlägen |
| 9. | **Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können? | [ ]  Individueller Log-In und Kennwortverfahren[ ]  Zusätzlicher Log-In für bestimmte Anwendungen[ ]  Automatische Sperrung der Clients (Zeitablauf)[ ]  Verwaltung von Berechtigungen[ ]  Dokumentation von Berechtigungen[ ]  Verschlüsselung von Systemen[ ]  Sonstige:       |
| 10. | **Verarbeitung personenbezogener Daten nur nach Anweisung**Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden? | [ ]  Mitarbeiter sind zu Verhaltensregeln verpflichtet[ ]  Implementierung unternehmensinterner Datenschutz-Richtlinien[ ]  Verpflichtung der Mitarbeiter auf das Datengeheimnis[ ]  Schulungen aller zugriffsberechtigten Mitarbeiter[ ]  Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag |

1. Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine **allgemeine** Beschreibung darstellen, die es ermöglicht, **vorläufig** zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem gemeinsam Verantwortlichen bei wesentlichen Änderungen und im Übrigen jährlich vorzulegen. [↑](#footnote-ref-1)