**Technisch.-organisatorische Maßnahmen nach Art. 32 DSGVO**

Jagdgenossenschaft: Musterhausen

Jagdvorstand: Max Muster

IT-Abteilung: keine

Datenschutzbeauftragter: Herr Datenschutz

Sitz der Genossenschaft: a) Musterstraße 18; 12345 Musterhausen

Weitere Standorte: b) Klicken Sie hier, um Text einzugeben.

 c) Klicken Sie hier, um Text einzugeben.

 d) Klicken Sie hier, um Text einzugeben.

 e) Klicken Sie hier, um Text einzugeben.

 f) Klicken Sie hier, um Text einzugeben.

**Prüfdaten:**

Prüfung am: Klicken Sie hier, um Text einzugeben.

Prüfung durch: Klicken Sie hier, um Text einzugeben.

Geprüfte Orte: Klicken Sie hier, um Text einzugeben.

 Klicken Sie hier, um Text einzugeben.

 Klicken Sie hier, um Text einzugeben.

**Auditinterviews:**

Am: mit: Unterschrift:

Am: mit: Unterschrift:

Am: mit: Unterschrift:

Am: mit: Unterschrift:

Am: mit: Unterschrift:

Am: mit: Unterschrift:

Inhalt

[1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 3](#_Toc520386559)

[1.1 Zutrittskontrolle 3](#_Toc520386560)

[1.2 Zugangskontrolle 4](#_Toc520386561)

[1.3 Zugriffskontrolle 6](#_Toc520386562)

[1.4 Trennungskontrolle 7](#_Toc520386563)

[1.5 Pseudonymisierung/Anonymisierung 8](#_Toc520386564)

[2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 9](#_Toc520386565)

[2.1 Weitergabekontrolle 9](#_Toc520386566)

[2.2 Eingabekontrolle 10](#_Toc520386567)

[3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 10](#_Toc520386568)

[3.1 Verfügbarkeitskontrolle 10](#_Toc520386569)

[3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) 12](#_Toc520386570)

[4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) 12](#_Toc520386571)

[4.1 Datenschutz-Management 12](#_Toc520386572)

[4.2 Incident-Response-Management 13](#_Toc520386573)

[4.3 Datenschutzfreundliche Voreinstellungen – Privacy by Default – (Art. 25 Abs. 2 DS-GVO) 13](#_Toc520386574)

[4.4 Auftragskontrolle 14](#_Toc520386575)

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

## Zutrittskontrolle

Welche der folgenden Maßnahmen trifft zu (Bitte ankreuzen und ggfs. Bemerkungsfeld ausfüllen)

### Technische Maßnahmen:

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Alarmanlage/Einbruchmeldeanlage | Klicken Sie hier, um Text einzugeben. |
| [ ]  | automatisiertes Zutrittskontrollsystem (z.B. Kartenleser, Zahlencode, Transponder-Schließsystem) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Absicherung von Gebäudeschächten, Fenstern u.ä. | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Kameraüberwachung Videoüberwachung der Zugänge zum Unternehmen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Manuelles Schließsystem (Sicherheitsschloss) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Vereinzelungsschleuse | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sicherheitsverfahren für Homeoffice u. bei Reisen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Biometrische Zugangssperren | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Lichtschranken, Bewegungsmelder | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstige - bitte beschreiben | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen:

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Personenkontrolle beim Werkschutz/Pförtner/Empfang | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Protokollierung der Besucher | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schlüsselregelung/Schlüsselbuch | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sorgfältige Auswahl des Sicherheitspersonals | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Tragepflicht von Mitarbeiter- und Gästeausweisen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftlich dokumentierte Sicherheits-Policy (z.B. Verfahren für Zutrittsberechtigungen für Mitarbeiter/innen und Besucher) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Zertifizierungen: ISO27001, ITIL, …) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Regelmäßige Schulungen, Unterrichtungen für IT-Personal  | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstige - bitte beschreiben | Klicken Sie hier, um Text einzugeben. |

## Zugangskontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Benutzer-/Passwortverfahren mit wenigstens 8 Zeichen, drei Zeichenklassen  | kein erzwungener Passwortwechsel  |
| [ ]  | Passwörter laufen nach 3 Monaten ab, die letzten 3 / 5 Passwörter können nicht neu verwendet werden | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Authentifikation mit biometrischen Daten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Automatische Sperrung von Kennungen nach drei (3) Fehlversuchen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Automatische Sperre bei nicht mehr zugangsberechtigten Personen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Public Key Infrastructure (PKI) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Anti-Viren-Software | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Firewalls | Klicken Sie hier, um Text einzugeben. |
| [ ]  | LDAP od. Active Directory (AD) Authentifikation | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Logging aller Zugriffsversuche  | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Mobile Device Management | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von VPN Technologie | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Gehäuseverriegelungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sperren externer Schnittstellen (z.B. USB, Hard- od CD Laufwerke) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verschlüsselung von Datenträgern | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verschlüsselung von Smartphones | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Getrennte Benutzerkonten für Systemadministration und User | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Automatische Beendigung von Web-Sessions nach festgelegter Zeit ohne Benutzerinteraktion | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Die Tätigkeiten der Systemadministration an den IT-Systemen werden protokolliert … | Klicken Sie hier, um Text einzugeben. |
| [ ]  | … diese Protokolldateien werden regelmäßig ausgewertet | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz eines Intrusion Detection Systems | Klicken Sie hier, um Text einzugeben. |

Wie erfolgt der Zugang ins Internet?

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Über eine Sicherheitsinfrastruktur-kette aus Proxy, Virenscanner und Firewall | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Über einen Stand-Alone-Rechner | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Über den Wechsel auf ein anderes Betriebssystem (Dual Boot) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen:

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Benutzerberechtigungen werden vergeben und verwaltet | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Benutzerprofile werden erstellt | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sorgfältige Auswahl des Reinigungspersonals und anderer Dienstleister im Unternehmen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sorgfältige Auswahl des Sicherheitspersonals | Klicken Sie hier, um Text einzugeben. |

## Zugriffskontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Einsatz von Aktenvernichtern | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Ordnungsgemäße Vernichtung von Datenträgern (gem. DIN 32757) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Physische Löschung von Datenträgern vor deren Wiederverwendung |   |
| [ ]  | Protokollierung der Vernichtung von Daten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verschlüsselung von Datenträgern | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verschlüsselung von Smartphones | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Anwendung eines differenzierten, schriftlichen Berechtigungs­konzepts, um die Nutzung von Profilen bzw. Rollen und Transaktionen zu regeln | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Maßnahmen zur Vermeidung unberechtigten Eindringens (Intrusion detection and prevention) | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Die Anzahl der Systemadministratoren ist auf das Notwendigste reduziert | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Es existiert ein Berechtigungskonzept mit geringst-möglichen Zugriffsrechten (only rights required to do the job) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Passwortrichtline inkl. Länge ~~und Wechsel~~ (s.o.) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sichere Aufbewahrung von Datenträgern | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verwaltung der Benutzerrechte durch Systemadministratoren | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Es existieren schriftliche Regelungen zur Nutzung mobiler Datenträger (CD, DVD, USB-Stick, etc.) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Es existieren schriftliche Regelungen zur Vernichtung/Entsorgung von Datenträgern | Klicken Sie hier, um Text einzugeben. |

**Protokollierung von Systemzugriffen durch Benutzer**

|  |  |  |
| --- | --- | --- |
| [ ]  | Alle Systemzugriffe werden protokolliert | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

Diese Protokolle werden wie folgt ausgewertet:

|  |  |  |
| --- | --- | --- |
| [ ]  | Bei Bedarf | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Regelmäßig durch eine manuelle Protokollauswertung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Regelmäßig durch eine automatisierte Protokollauswertung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | sonstiges (bitte nachfolgend erläutern) |  |

## Trennungskontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |  |
| [ ]  | Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |  |
| [ ]  | Trennung von Produktiv- und Testsystem |  |
| [ ]  | Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |  |
| [ ]  | Bei Inanspruchnahme von Cloud-Services: single tenant setup für Applikationen und Daten |  |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Ein Berechtigungskonzept liegt vor | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Datenbankrechte sind definiert | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Eine logische Mandantentrennung wird durchgeführt | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Versehen der Datensätze mit Zweckattributen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Es existieren schriftliche Regelungen zur Funktionstrennung (z.:B. Test/Produktion, Mandantentrennung) | Klicken Sie hier, um Text einzugeben. |

Wie wird sichergestellt, dass Daten nur zum vorgesehenen Zweck verarbeitet und genutzt werden?

|  |  |  |
| --- | --- | --- |
| [ ]  | Es gibt eine Trennung zwischen Entwicklung, Test und Produktion | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Datentrennung durch ein differenziertes Benutzerkonzept | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Die Daten werden nach Mandanten getrennt verarbeitet | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Nicht relevant, weil …  | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

## Pseudonymisierung/Anonymisierung

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.

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis, Beschreibung des Verfahrens: |
| [ ]  | folgende Daten werden pseudonymisiert/anonymisiert: | Klicken Sie hier, um Text einzugeben. |
| [ ]  | * Beschäftigtendaten
 | Klicken Sie hier, um Text einzugeben. |
| [ ]  | * Kundendaten
 | Klicken Sie hier, um Text einzugeben. |
| [ ]  | * Interessentendaten
 | Klicken Sie hier, um Text einzugeben. |
| [ ]  | * Daten von (End)Kunden, die von Kunden zur Verfügung gestellt werden
 | Klicken Sie hier, um Text einzugeben. |
| [ ]  | * User-Namen eigener Beschäftigter
 | Pseudonyme |

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

## Weitergabekontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | VPN-Tunnel | Klicken Sie hier, um Text einzugeben. |
| [ ]  | E-Mail-Verschlüsselungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Daten-Verschlüsselungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verschlüsselung von Speichermedien mobiler Endgeräte (z.B. Laptops) | Klicken Sie hier, um Text einzugeben.  |
| [ ]  | Digitale Signaturen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Protokollierung der Übertragung und Logs | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

Wie werden die Daten beim (physikalischen) Transport geschützt?

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Transport durch Spezialunternehmen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Versand per Einschreiben/Wertpaket | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verwendung gesicherter/verschlossener Transportbehältnisse | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Protokollierung/Dokumentation | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sichere Transportbehälter/-Verpackungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Nicht relevant, weil kein Transport von Datenträgern stattfindet. | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sorgfältige Auswahl von Transportpersonal und -fahrzeugen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Weitergabe von Daten in anonymisierter od. pseudonymisierter Form | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftliche Regelungen zum Versand und zur Übertragung von Daten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftliche Regelungen zur Fernwartung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftliche Regelungen zur Nutzung von Telearbeitsplätzen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftliche Regelungen, dass elektronische Datenträger beim Versand (physikalischer Transport) verschlüsselt sein müssen | Klicken Sie hier, um Text einzugeben. |

## Eingabekontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Protokollierung der Eingabe, Änderung und Löschung von Daten mit Zeitstempel, User-IDs | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | schriftliche Regelungen zur Durchführung einer Eingabekontrolle | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Zufallszugriffe | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Auswertung von Eingabeprotokollen | Klicken Sie hier, um Text einzugeben. |

Wie werden diese Protokolle ausgewertet?

|  |  |  |
| --- | --- | --- |
| [ ]  | Bei Bedarf | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Regelmäßig durch eine manuelle Protokollauswertung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Regelmäßig durch eine automatisierte Protokollauswertung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges – bitte erläutern |  |

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

## Verfügbarkeitskontrolle

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Feuerlöschgeräte in Serverräumen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Feuer- und Rauchmeldeanlagen |  |
| [ ]  | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |  |
| [ ]  | Klimaanlage in Serverräumen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schutzsteckdosenleisten in Serverräumen |  |
| [ ]  | Unterbrechungsfreie Stromversorgung (USV) u/o Notstromgenerator | . |
| [ ]  | Gedoppelte Daten- und Telefonleitungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Gedoppelte Energieleitungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Data Backups werden regelmäßig durchgeführt (mtl. geplante Backups) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Spiegelung von Daten |  |
| [ ]  | Getrennte Aufbewahrung von Produktivdaten und Datensicherungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Stichprobenartige Prüfung von Datensicherungen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Virenscannern auf Arbeitsstationen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Virenscannern auf Servern | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Firewalls zur Absicherung von Netzwerkübergängen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Einsatz von Personal Firewalls auf Arbeitsstationen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sonstiges (bitte nachfolgend erläutern) | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Aufbewahrung der Datensicherung an einem sicheren externen Ort | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Erstellen eines Backup- und Disaster Recovery Konzepts | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Notfallplan/pläne existieren | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Datenwiederherstellungen, regelmäßiges Testen von Disaster-Fällen  | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Die Serverräume befinden sich nicht unterhalb sanitärer Anlagen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | In Hochwassergebieten: Serverräume befinden sich oberhalb der Wassergrenze | Klicken Sie hier, um Text einzugeben. |

## Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Desaster Recovery Maßnahmen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Ausfallrechenzentrum | Klicken Sie hier, um Text einzugeben. |
| [ ]  | gedoppelte Server, räumlich getrennt | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Notfallkonzept | Klicken Sie hier, um Text einzugeben. |
| [ ]  | regelmäßige Notfallübungen | Klicken Sie hier, um Text einzugeben. |

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

## Datenschutz-Management

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | DSMS – Datenschutzmanagement-System | geplant |
| [ ]  | weitere |  |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Sensibilisierung der Mitarbeiter auf Datenschutz | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Informationssystem Abteilungen 🡪 DSB | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Informationssystem DSB 🡪 Abteilung | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Abarbeiten von Maßnahmen nach Projektmanagement-Systematik | Klicken Sie hier, um Text einzugeben. |
| [ ]  | weitere | Klicken Sie hier, um Text einzugeben. |

## Incident-Response-Management

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | es existiert ein IRM-System | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz | Klicken Sie hier, um Text einzugeben. |
| [ ]  | weitere | Klicken Sie hier, um Text einzugeben. |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Notfall-Team bestehend aus:* Geschäftsleitung
* IT-Leitung
* Datenschutzbeauftragter
 | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Notfall-Managementsystem | Klicken Sie hier, um Text einzugeben. |
| [ ]  | weitere | Klicken Sie hier, um Text einzugeben. |

## Datenschutzfreundliche Voreinstellungen – Privacy by Default – (Art. 25 Abs. 2 DS-GVO)

### Technische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Beschäftigtendatenschutz | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Kunden, Interessenten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | weitere: |  |

### Organisatorische Maßnahmen

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | weitere |  |

## Auftragskontrolle

* + 1. **Organisatorische Maßnahmen**

|  |  |  |
| --- | --- | --- |
|  | Maßnahme | Bemerkung/Nachweis: |
| [ ]  | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Schriftliche Weisungen an den Auftragnehmer i.S.d. §11 II BDSG | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Vertragsstrafen bei Verstößen | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Wirksame Kontrollrechte gegenüber dem Auftragnehmer sind vereinbart | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Arbeiten die Aufragnehmer mit Nachweis einer auftragsgemäßen Datenverarbeitung? | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Lieferantenaudits | Klicken Sie hier, um Text einzugeben. |
| [ ]  | Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt | Klicken Sie hier, um Text einzugeben. |

**Prüfungen und Maßnahmen durch den DSB**

|  |  |  |  |
| --- | --- | --- | --- |
| Datum | DSB | Prüfung | Ergebnis, Maßnahmen |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Versionshistorie**

|  |  |  |
| --- | --- | --- |
| **Datum** | **Version** | **Änderung** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
|  |  |

Datum Unterschrift Datenschutzbeauftragter (DSB)

|  |  |
| --- | --- |
|  |  |

Datum Unterschrift – IT-Verantwortliche,