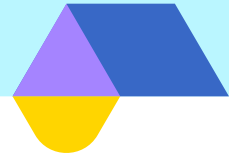


Datenschutz-/Datensicherheitserklärung



Vorbemerkung

Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben gemäß Art. 28, 29 DS-GVO i.V.m. Art. 32 DS-GVO die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Normen des SGB X sowie des BDSG zu erfüllen.

Der Auftraggeber (SBK) ist nach § 80 SGB X i.V.m. Art. 28 DS-GVO für die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit verantwortlich. Hierzu hat sich der Auftraggeber vor Beginn der Datenverarbeitung sowie in regelmäßigen Abständen von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und diese zu dokumentieren.

Ferner ist der Auftraggeber nach § 89 Abs. 4 SGB X berechtigt, die Ausführung des erteilten Auftrages zu prüfen.

Um diesen Anforderungen gerecht zu werden bzw. gegebenenfalls eine Prüfung bei Ihnen vor Ort zu vermeiden, wurde die folgende Erklärung entwickelt, die **Sie uns bitte unabhängig vom Umfang des Auftrages bezogen auf Ihr Unternehmen, vollständig ausgefüllt**, ergänzt um die gewünschten Unterlagen, und unterschrieben wieder an uns **zurücksenden**. Zur korrekten Befüllung der nachstehenden Angaben sind die im Anhang A aufgeführten Anmerkungen und Beispiele heranzuziehen. Der Anhang konkretisiert die erwartete Darstellung und unterstützt bei der Wahl der zutreffenden Perspektive.

Die Datenschutz-/Datensicherheitserklärung ist **auch für Wartungsverträge** abzugeben, vgl. § 80 Abs. 5 SGB X

Die **Mindestanforderungen der SBK sind jeweils kursiv** unter den einzelnen Fragen angegeben. Diese Mindestanforderungen müssen vom Dienstleister spätestens bei Vertragsbeginn erfüllt sein. Für Fragen stehen wir Ihnen gerne zur Verfügung

Hinweis: Bei den angegebenen Antworten sind mehrfache Nennungen möglich. Sollten die vorgedruckten Felder nicht ausreichen, fügen Sie bitte ein extra Blatt bei und vermerken dies bei den jeweiligen Punkten.

Die Erklärung erfolgt für:

Name -----

Anschrift -----

Anzahl der Mitarbeiter -----

DSB -----

Telefonnummer -----

Übersicht

1.	Zutrittskontrolle	3
1.1	Sicherungsmaßnahmen des Gebäudes / des Betriebsgeländes	3
1.2	Sicherungsmaßnahmen innerhalb der Geschäftsräume	4
2.	Zugangskontrolle zu Datenverarbeitungsanlage/n	9
2.1	Datenschutzerklärungen	9
2.2	Arbeitsplatzgestaltung	9
2.3	Identifikation und Authentifikation von Benutzern	9
2.4	Protokollierung der Zugriffe	10
2.5	Single SignOn / Durchreichung des Login-Passwortes	10
2.6	Passwortkonventionen	10
2.7	PEN-Test	11
2.8	Wartungs- und Reparaturarbeiten	12
3.	Zugriffskontrolle	13
3.1	Berechtigungskonzept	13
3.2	Verschlüsselung gespeicherter Personendaten	13
3.3	Kopierschutz für die Arbeitsplätze der Mitarbeiter	13
3.4	Systemadministration/Serverhosting	14
3.5	Ausscheiden von Mitarbeitern	16
4.	Weitergabekontrolle	17
4.1	Übertragung personenbezogener Daten	17
4.2	Datenträger	18
4.3	Datenträgerversand	21
4.4	Fernwartung von Systemen	21
4.5	Papierentsorgung	23
5.	Eingabekontrolle	25
5.1	Protokollierung der Eingabe	25
5.2	Auswertung der Protokolle	25
5.3	Aufbewahrung der Protokollierung	25
6.	Auftragskontrolle von Unterauftragnehmern	26
6.1	Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber	26
6.2	Kontrolle Ihrer Auftragnehmer	26
7.	Verfügbarkeitskontrolle	27
7.1	Betriebsbereitschaft	27
7.2	Auslagerung von Sicherheitskopien	27
7.3	Prüfung der Logdateien der Datensicherung	27
7.4	Wiederherstellung der Daten	27
7.5	Prüfung der Sicherungsmedien	27
7.6	Unterbrechungsfreie Stromversorgung (USV)	28
7.7	Verantwortlichkeit für IT-Sicherheit	28
7.8	Richtlinien zum Datenschutz und zur Datensicherheit	28
7.9	Löschkonzept	32
8.	Trennungsgebot (bezogen auf die in 4.2.1 genannten Datenträger)	33
8.1	Abschottung personenbezogener Daten verschiedener speichernder Stellen gegeneinander	33
8.2	Trennung der DV-Anlagen und Datenträger für besonders sensible Daten	33
9.	Datenschutzbeauftragter	34
9.1	Datenschutzbeauftragter	34
9.2	Automatisierte Verarbeitung personenbezogener Daten	34
9.3	Datenschutz- und Datensicherheitskontrollen	34
9.4	Datenschutzschulungen	34
9.5	Verfahrensverzeichnis	34
9.6	Weiterbildung	35
10.	Anhang A – Anmerkungen und Beispiele für die korrekte Befüllung der Datenschutz- / Datensicherheitserklärung	36
11.	Anhang B - Auftragskontrolle von Unterauftragnehmern	38

1. Zutrittskontrolle

Die Zutrittskontrolle zielt auf den physischen Schutz der technischen Datenverarbeitungseinrichtungen, also die Gebäudesicherheit ab. Dies umfasst bauliche Maßnahmen, wie z.B. bruch sichere Fenster, gesondert gesicherte Räume mit Chipkartenleser etc.

1.1 Sicherungsmaßnahmen des Gebäudes / des Betriebsgeländes

1.1.1 Art des Gebäudes

- | | |
|---|--|
| <input type="checkbox"/> Bürogebäude | <input type="checkbox"/> Büro- und Wohngebäude |
| <input type="checkbox"/> Wohnhaus/Einfamilienhaus | <input type="checkbox"/> |

Unzulässig ist ein Wohnhaus/Einfamilienhaus.

1.1.2 Überwachung des Geländes / Gebäudes außerhalb der Dienststunden

ja nein

- | | | |
|--|--|---|
| <input type="checkbox"/> Wachpersonal: | <input type="checkbox"/> extern | <input type="checkbox"/> intern |
| <input type="checkbox"/> Bewegungsmelder | | |
| <input type="checkbox"/> Videoüberwachung: | <input type="checkbox"/> mit Aufzeichnung | <input type="checkbox"/> ohne Aufzeichnung |
| <input type="checkbox"/> Gebäudealarmanlage mit Verbindung zu: | | |
| | <input type="checkbox"/> Polizei | <input type="checkbox"/> Zentraler Pförtner |
| | <input type="checkbox"/> Feuerwehr | <input type="checkbox"/> Akustischer Alarm |
| | <input type="checkbox"/> Externer Wachdienst | <input type="checkbox"/> |

Ein „Nein“ wird nicht akzeptiert.

1.1.3 Zutrittskontrollsystem (Zugänge in das Gebäude)

Eingang (z.B. Haupteingang)

- | | |
|---|--|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis |
| <input type="checkbox"/> Magnetstreifenkarte | <input type="checkbox"/> Ausweis mit Foto |
| <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit Stellen |

Eingang (z.B. Nebeneingang)

- | | |
|---|--|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis |
| <input type="checkbox"/> Magnetstreifenkarte | <input type="checkbox"/> Ausweis mit Foto |
| <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit Stellen |

- | | | |
|----------------|--|--|
| Eingang | <input type="checkbox"/> Tiefgarage | <input type="checkbox"/> Balkone |
| | <input type="checkbox"/> Keller | <input type="checkbox"/> Dachterrassen |
| | <input type="checkbox"/> Liefer-Rolltore | <input type="checkbox"/> Dachluken |

- | | |
|---|--|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis |
| <input type="checkbox"/> Magnetstreifenkarte | <input type="checkbox"/> Ausweis mit Foto |
| <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit _____ Stellen |

Kein Zutrittskontrollsystem wird grundsätzlich nicht akzeptiert.

Ausnahme: Wenn bei Ziffer 1.1.4 eine besondere Sicherung vorliegt (z.B. Codierte Schlüssell) bzw. bei Ziffer 1.2.2 und 1.2.3 ein Zutrittskontrollsystem.

1.1.4 Schließsystem Gebäude- Eingangstür/en

Eingang _____ (z.B. Haupteingang)

- | | |
|--|--|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem |
| <input type="checkbox"/> Sicherheitsschloss | <input type="checkbox"/> Separater Schließkreis |
| <input type="checkbox"/> Codierte Schlüssell | <input type="checkbox"/> _____ |

Eingang _____ (z.B. Nebeneingang)

- | | |
|--|--|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem |
| <input type="checkbox"/> Sicherheitsschloss | <input type="checkbox"/> Separater Schließkreis |
| <input type="checkbox"/> Codierte Schlüssell | <input type="checkbox"/> _____ |

Eingang

- | |
|--|
| <input type="checkbox"/> Tiefgarage |
| <input type="checkbox"/> Keller |
| <input type="checkbox"/> Liefer-Rolltore |

- | |
|--|
| <input type="checkbox"/> Balkone |
| <input type="checkbox"/> Dachterrassen |
| <input type="checkbox"/> Dachluken |

- | | |
|--|--|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem |
| <input type="checkbox"/> Sicherheitsschloss | <input type="checkbox"/> Separater Schließkreis |
| <input type="checkbox"/> Codierte Schlüssell | <input type="checkbox"/> _____ |

Ein Sicherheitsschloss ist Mindeststandard. Ein einfaches Schloss wird nicht akzeptiert.

1.2 Sicherungsmaßnahmen innerhalb der Geschäftsräume

1.2.1 Haupteingang des Geschäftsbereichs

Geöffnet in der Zeit

- | | |
|-------------------------------------|-----------------------------|
| <input type="checkbox"/> Montag | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Dienstag | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Mittwoch | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Donnerstag | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Freitag | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Samstag | von _____ Uhr bis _____ Uhr |
| <input type="checkbox"/> Sonntag | von _____ Uhr bis _____ Uhr |

Nur Angaben sind einzutragen.

1.2.2 Zutrittskontrollsystem (Zugang zu Geschäftsräumen, Serverräumen, Archivräume, usw.)

Geschäftsräume:

- | | | |
|--|--|---|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis | <input type="checkbox"/> Magnetstreifenkarte |
| <input type="checkbox"/> Ausweis mit Foto | <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit _____ Stellen | |

Serverräume:

- | | | |
|--|--|---|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis | <input type="checkbox"/> Magnetstreifenkarte |
| <input type="checkbox"/> Ausweis mit Foto | <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit _____ Stellen | |

Sonstige Räume -----

- | | | |
|--|--|---|
| <input type="checkbox"/> kein Zutrittskontrollsystem | <input type="checkbox"/> Ausweis | <input type="checkbox"/> Magnetstreifenkarte |
| <input type="checkbox"/> Ausweis mit Foto | <input type="checkbox"/> Magnetstreifenkarte mit Foto | <input type="checkbox"/> Mit PC-Protokollierung |
| <input type="checkbox"/> Karte mit Infrarotleser | <input type="checkbox"/> Codeschloss mit _____ Stellen | |

Kein Zutrittskontrollsystem wird bei Geschäftsräumen und Serverräumen grundsätzlich nicht akzeptiert.

*Ausnahme für Serverräume: Wenn bei Ziffer 1.2.3. **mindestens** ein Sicherheitsschloss vorgesehen ist.*

1.2.3 Schließsysteme der Räumlichkeiten

Geschäftsräume:

- | | | |
|---|--|---|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem | <input type="checkbox"/> Sicherheitsschloss |
| <input type="checkbox"/> Separater Schließkreis | <input type="checkbox"/> Codierte Schlüssel | <input type="checkbox"/> ----- |

Serverräume:

- | | | |
|---|--|---|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem | <input type="checkbox"/> Sicherheitsschloss |
| <input type="checkbox"/> Separater Schließkreis | <input type="checkbox"/> Codierte Schlüssel | <input type="checkbox"/> ----- |

Sonstige Räume -----

- | | | |
|---|--|---|
| <input type="checkbox"/> einfaches Schloss | <input type="checkbox"/> Zentrales Schließsystem | <input type="checkbox"/> Sicherheitsschloss |
| <input type="checkbox"/> Separater Schließkreis | <input type="checkbox"/> Codierte Schlüssel | <input type="checkbox"/> ----- |

Ein Sicherheitsschloss ist der Mindeststandard. Ein einfaches Schloss (außer bei Büroräumen) wird nicht akzeptiert.

1.2.4 Organisatorische Regelungen über Zutrittsberechtigungen

Es bestehen organisatorische Regelungen über Zutrittsberechtigungen zu Geschäftsbereichen

nein

ja, welche

- | | |
|---|---|
| <input type="checkbox"/> Dienstanweisung | <input type="checkbox"/> Zutrittsberechtigungskonzept |
| <input type="checkbox"/> Einweisung der Mitarbeiter | <input type="checkbox"/> ----- |

Eine Dienstanweisung, ein Zutrittsberechtigungskonzept sowie eine Einweisung der Mitarbeiter sind erforderlich.

1.2.5 Verwaltung der Zutrittsmittel

Zutrittsmittel werden sicher verwaltet (Schlüssel usw.)

nein

ja, Regelungen

Regelungen müssen vorliegen.

1.2.6 Zutrittsmitteldokumentation

Es liegt eine Zutrittsmitteldokumentation vor

nein

ja, durch

- ☐ Manuelles Schlüsselbuch/Schlüsselverzeichnis
- ☐ Elektronisches Schlüsselbuch/Schlüsselverzeichnis
- ☐

Ein „Nein“ wird nicht akzeptiert.

1.2.7 Maßnahmen/Regelungen bei Verlust eines Zutrittsmittels

.....

.....

*Meldung zwingend an fest bestimmte Person. Ein Austausch muss erfolgen, wenn dieser nötig ist.
Bei Kartensystemen ist eine automatische Sperrung zu veranlassen.*

1.2.8 Zutritte sonstiger Personen in die Geschäftsräume

Der Zutritt sonstiger Personen zu den Geschäftsräumen wird überwacht

nein

ja, durch

- ☐ Besucherüberwachung (Kunden, Wartungspersonal, Handwerker, usw.) in Form
 - ☐ eines Besucherbuches ☐ von sichtbaren Besucherausweisen
 - ☐ von Begleitung durch Mitarbeiter ☐ von Laufzettel oder Besucherschein
 - ☐ Verpflichtung zum Datenschutz
- ☐ Empfang in den Geschäftsräumen
 - nein ja, von ____ Uhr bis ____ Uhr

Ein „Nein“ wird nicht akzeptiert. Mindestens Besucherbuch inkl. Verpflichtung zum Datenschutz . Eine zusätzliche Begleitung ist sinnvoll.

1.2.9 Reinigung der Geschäftsräume

Geschäftsräume:

- | | |
|---|--|
| <input type="checkbox"/> Eigenes Personal | <input type="checkbox"/> innerhalb der Arbeitszeit |
| <input type="checkbox"/> Externer Dienstleister | <input type="checkbox"/> außerhalb der Arbeitszeit |
| Datenschutzverpflichtung liegt vor | ja nein |

Anmerkungen -----

Serverräume:

- | | |
|---|--|
| <input type="checkbox"/> Eigenes Personal | <input type="checkbox"/> innerhalb der Arbeitszeit |
| <input type="checkbox"/> Externer Dienstleister | <input type="checkbox"/> außerhalb der Arbeitszeit |
| Datenschutzverpflichtung liegt vor | ja nein |

Anmerkungen -----

Sonstige Räume

- | | |
|---|--|
| <input type="checkbox"/> Eigenes Personal | <input type="checkbox"/> innerhalb der Arbeitszeit |
| <input type="checkbox"/> Externer Dienstleister | <input type="checkbox"/> außerhalb der Arbeitszeit |
| Datenschutzverpflichtung liegt vor | ja nein |

Anmerkungen -----

Die Reinigung der Serverräume darf ausschließlich im 4-Augenprinzip erfolgen. Bei auch nur zufälligem Kontakt mit Sozialdaten sind Datenschutzvereinbarungen verpflichtend.

1.2.10 Technik-Unterbringung

	EDV/Serverraum	TK-Anlage	-----
Keller	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Erdgeschoss	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stockwerk 1. Etage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stockwerk 2. Etage oder höher	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sind die Räumlichkeiten für Außenstehende sofort erkennbar	nein	ja	

Nicht akzeptiert wird, wenn die Räumlichkeiten sofort erkennbar sind.

1.2.11 Sicherungsmaßnahmen in den Räumlichkeiten

Geschäftsräume:

Fensterart	Sicherheitsvorkehrungen	
<input type="checkbox"/> ohne Fenster	<input type="checkbox"/> zeitgesteuerte Rollläden	<input type="checkbox"/> Glasbruchmelder
<input type="checkbox"/> normales Fensterglas	<input type="checkbox"/> Außenjalousien	<input type="checkbox"/> Sicherheitsfolie
<input type="checkbox"/> Isolierverglasung	<input type="checkbox"/> Innenjalousien	<input type="checkbox"/> eingeschränktes Öffnen

- ☐ Drahtglas
 ☐ abschließbare Fenstergriffe
 ☐ -----
- ☐ Panzerglas

Serverräume:

Fensterart	Sicherheitsvorkehrungen	
<input type="checkbox"/> ohne Fenster	<input type="checkbox"/> zeitgesteuerte Rollläden	<input type="checkbox"/> Glasbruchmelder
<input type="checkbox"/> normales Fensterglas	<input type="checkbox"/> Außenjalousien	<input type="checkbox"/> Sicherheitsfolie
<input type="checkbox"/> Isolierverglasung	<input type="checkbox"/> Innenjalousien	<input type="checkbox"/> eingeschränktes Öffnen
<input type="checkbox"/> Drahtglas	<input type="checkbox"/> abschließbare Fenstergriffe	<input type="checkbox"/> -----
<input type="checkbox"/> Panzerglas		

Sonstige Räume: -----

Fensterart	Sicherheitsvorkehrungen	
<input type="checkbox"/> ohne Fenster	<input type="checkbox"/> zeitgesteuerte Rollläden	<input type="checkbox"/> Glasbruchmelder
<input type="checkbox"/> normales Fensterglas	<input type="checkbox"/> Außenjalousien	<input type="checkbox"/> Sicherheitsfolie
<input type="checkbox"/> Isolierverglasung	<input type="checkbox"/> Innenjalousien	<input type="checkbox"/> eingeschränktes Öffnen
<input type="checkbox"/> Drahtglas	<input type="checkbox"/> abschließbare Fenstergriffe	<input type="checkbox"/> -----
<input type="checkbox"/> Panzerglas		

Geschäftsräume: Mindeststandard Isolierverglasung, Serverräume: Mindeststandard Panzerverglasung, Sonstige Räume: Mindeststandard Isolierverglasung.

1.2.12 Schilderung von Vorkommnissen bezogen auf die Geschäftsräume der letzten 12 Monate

- ☐ keine Vorkommnisse
 ☐ Einbruch
 ☐ Vandalismus
- ☐ Diebstahl
 ☐ -----

Bei Vorkommnissen, nähere Schilderung des Vorfalles und Ableitungen daraus auf separatem Blatt.

2. Zugangskontrolle zu Datenverarbeitungsanlage/n

Mit der Zugangskontrolle soll die Benutzung der Datenverarbeitungsanlage/n gesichert werden. Zunächst betrifft dies den lokalen Zugangsschutz, wie z.B. passwortgesicherter Zugang auf Betriebssysteme oder chipkartengeschützter Zugang. Bei vernetzten Systemen muss der Zugang zusätzlich gegen Zugriffe über das Netz geschützt werden. Insbesondere bei Anschluss an das Internet sind erhöhte Anforderungen an den Schutz zu stellen. Eine Sicherung hat i.d.R. über Firewall usw. zu erfolgen.

2.1 Verpflichtung zum Datenschutz

Die Mitarbeiter haben eine Verpflichtung zum Datenschutz unterzeichnet:

nein ja, alle Mitarbeiter Anmerkungen _____

Alle Mitarbeiter müssen auf den Datenschutz verpflichtet sein.

2.2 Arbeitsplatzgestaltung

Die eingerichteten Arbeitsplätze sind so gestaltet, dass Externen grundsätzlich kein Einblick (Bildschirm, Drucker, Fax usw.) auf Sozialdaten geboten wird nein ja

Eine regelmäßige Kontrolle wird durchgeführt nein ja, wie oft _____

Ein „Nein“ wird bei der Arbeitsplatzgestaltung nicht akzeptiert.

2.3 Identifikation und Authentifikation von Benutzern

Benutzer werden wie folgt authentifiziert

	Client	Anwendung/Host
User-ID ohne Passwort	<input type="checkbox"/>	<input type="checkbox"/>
User-ID mit Passwort	<input type="checkbox"/>	<input type="checkbox"/>
Magnet-/Chipkarte	<input type="checkbox"/>	<input type="checkbox"/>
-----	<input type="checkbox"/>	<input type="checkbox"/>
keine	<input type="checkbox"/>	<input type="checkbox"/>

User-ID mit Passwort ist der Mindeststandard.

2.4 Protokollierung der Zugriffe

Zugriffe werden wie folgt protokolliert

nein **ja**

Auswertung der Protokolle

nein

ja, durch

wen

wie häufig

Aufbewahrung der Protokolle für

Protokollierung (über System) ist zwingend. Die Auswertung sollte monatlich, nicht nur bei Bedarf erfolgen.

2.5 Single SignOn / Durchreichung des Login-Passwortes

Single SignOn wird angewandt

Client

Anwendung/Host

ja

nein

Anmerkungen

Aus Sicherheitsgründen sollte SingleSignOn bei der Verwendung verschiedener Anwendungen nicht eingesetzt werden. Sollte „JA“ angegeben werden, ist darzulegen, warum dies erforderlich ist.

2.6 Passwortkonventionen

Client

Anwendung/Host

Anzahl/Dauer

Zeichen Mindestlänge

☐☐

.....

Keine Trivialkennworte

☐☐

Klein-/Großbuchstaben

☐☐

Ziffern

☐☐

Sonderzeichen

☐☐

Gültigkeitsdauer

☐☐

.....

Zahl der Generationen

☐☐

.....

keine

☐☐

Die dargestellten Passwortkonventionen werden „erzungen“ durch

☐ Systemeinstellung (technisch)

☐ Passwort-Richtlinie etc. (organisatorisch)

Anmerkungen

*Zeichenlänge muss zwingend größer = 8 Zeichen sein
+ Groß-Kleinschreibung*

+ Sonderzeichen

+ Ziffern

(drei von vier Anforderungen müssen erfüllt sein)

Gültigkeitsdauer nicht länger als 90 Tage.

Zahl der Generationen mind. 3.

Keine Konventionen sind nicht zulässig. Passwortkonventionen müssen durch mindestens eine Voraussetzung erzwungen werden.

2.6.1 Einhaltung und Kontrolle der Passwortkonventionen

Anwendung

☐ Sperrung bei wiederholter

Fehleingabe nein ja, nach dem ___ Versuch

☐ Regelmäßige Kontrollen

der Konventionen nein ja, durch wen wie häufig

Sperrung nach 3. Versuch ist zwingend, Kontrollen erforderlich. Eine monatliche Kontrolle ist zwingend.

2.6.2 Software zur Verwaltung der Passwörter

Es wird eine Software zur Verwaltung der Passwörter eingesetzt (z. B. Freeware „Password Safe“):

nein ja, welche

Wenn ja, die Software wird gegen unbefugte Zugriffe von Innen bzw. Außen wie folgt abgesichert

Software zur Passwortverwaltung sollte nicht eingesetzt werden, da diese ein Sicherheitsrisiko darstellt. Wenn ja ist die besondere Sicherung der Software darzustellen.

2.7 PEN-Test

Die Sicherheitseinstellungen werden durch Hacker-/Penetrationstests überprüft:

nein ja, wie häufig

☐ intern ☐ extern, durch

Anmerkungen

PEN-Tests müssen regelmäßig (mindestens jährlich intern od. extern) durchgeführt werden.

2.8 Wartungs- und Reparaturarbeiten

nein ja

Wartungs- bzw. Reparaturarbeiten werden von Externen durchgeführt

Es sind Verantwortliche für die Beauftragung von Wartungs-/Reparaturarbeiten benannt

Von Externen durchgeführte Wartungs- und

Reparaturarbeiten werden durch fachkundige Mitarbeiter beaufsichtigt

Nach Abschluss der Arbeiten wird überprüft, ob der Wartungsauftrag vollständig und erfolgreich ausgeführt wurde

Nach Abschluss der Arbeiten werden in den betroffenen Bereichen die Passwörter geändert

Nach Abschluss der Arbeiten werden Computer-Viren-Checks durchgeführt

Die durchgeführten Wartungsarbeiten werden dokumentiert (Umfang, Ergebnisse, Zeitpunkt, evtl. Name des Technikers)

Es wird protokolliert, ob dem Techniker Zutritts-, Zugangs- und Zugriffsrechte eingeräumt wurden (Beginn, Ende, Bereich)

Es liegt ein Fristenplan für Wartungsarbeiten vor

Bei IT-Systemen, die außer Haus gegeben werden, werden alle sensitiven Daten, die sich auf Datenträgern befinden vorher physikalisch gelöscht

Die mit der Reparatur beauftragten Unternehmen werden auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen verpflichtet

Die externe Wartungsarbeit wird protokolliert (IT-Systeme, Komponenten, Beginn und Ende, Rückgabe der Geräte, welches Unternehmen)

Bis auf den ersten Punkt müssen alle Punkte mit "JA" beantwortet werden.

Ausnahme: Ein „Nein“ bei „Fristenplan für Wartungsarbeiten“ wird akzeptiert.

3. Zugriffskontrolle

Mit der Zugriffskontrolle ist die Berechtigung zum Zugriff auf die jeweiligen Daten gemeint. Nur die Person, die den Zugriff auf personenbezogene Daten für ihre jeweilige Tätigkeit benötigt, darf die Zugriffsrechte erhalten. Es ist zu gewährleisten, dass die Nutzungsberechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

3.1 Berechtigungskonzept

Ein Berechtigungskonzept ist

nicht vorhanden	vorhanden für (ggf. als Anlage beifügen)		
	Filesystem	nein	ja
	Mailsystem	nein	ja
	Anwendung	nein	ja
		nein	ja

Ein Berechtigungskonzept für Filesystem, Mailsystem und Anwendungen muss zwingend vorliegen.

3.2 Verschlüsselung gespeicherter Personendaten

Es erfolgt eine Verschlüsselung gespeicherter Personendaten

nein ja, Verfahren

Ein Verschlüsselungsverfahren sollte bei Bedarf eingesetzt werden.

Wenn ja, genaue Bezeichnung des Kryptographieverfahrens.

3.3 Kopierschutz für die Arbeitsplätze der Mitarbeiter

Die Arbeitsplätze der Mitarbeiter sind wie folgt gesichert:

	vorhanden		deaktiviert	
	nein	ja	nein	ja
USB-Anschluss				
CD/DVD/Blue-Ray-Brenner				
Download-Funktion				
Schnittstellen zu Bluetooth				
Wireless				

☐ Begrenzung von Mailinganhängen auf _____ MB

☐

Anmerkungen

Es besteht ein Verbot für die Mitarbeiter in Bezug auf die:

nein ja

Mitnahme von privaten Datenträgern in allgemeine Räume mit DV-Anlagen (z.B. Arbeitsplatz)

Mitnahme von privaten Datenträgern in Räume des Rechenzentrums

Es besteht eine Dienstanweisung zum Verbot, Daten für private Zwecke aus dem Unternehmen zu transferieren:

Die Mitarbeiter werden über die verbindlich einzuhaltende Dienstanweisung aufgeklärt

Es ist wie folgt sichergestellt, dass Daten nicht unbefugt das Haus verlassen können:

USB-Anschluss, CD/DVD/Blue-Ray-Brenner, Bluetooth bzw. Wireless sind zu deaktivieren. Eine Begrenzung der Mailanhänge auf X-MB muss erfolgen. Wenn keine Deaktivierung vorgenommen wird bzw. keine Verbote ausgesprochen werden, benötigen wir auf separatem Blatt eine Darstellung, warum eine Deaktivierung nicht vorgenommen wird und wie dem Risiko des unberechtigten Datenabflusses begegnet wird.

3.4 Systemadministration/Serverhosting

3.4.1 Systemadministration

☐ intern ☐ extern, durch -----

Intern und extern wird akzeptiert. Bei extern muss der Vertrag hierzu beigelegt werden.

3.4.2 Serverhosting

☐ intern ☐ extern, durch -----

Intern und extern wird akzeptiert. Bei extern muss der Vertrag hierzu beigelegt werden.

3.4.3 Administrationskonzept

nein ja

Abgestufte Rechte nein ja

Art der Differenzierung

<input type="checkbox"/> Systemadministration	<input type="checkbox"/> Datenbankadministration Einrichtung
<input type="checkbox"/> Vergabe Benutzerberechtigungen	<input type="checkbox"/> Benutzerberechtigungen

Ein Administrationskonzept muss vorliegen. Abgestufte Rechte sind nicht zwingend erforderlich.

3.4.4 Identifizierung und Authentifizierung des/der Administrators/en

	Client	Anwendung/Host
User-ID ohne Passwort	<input type="checkbox"/>	<input type="checkbox"/>
User-ID mit Passwort	<input type="checkbox"/>	<input type="checkbox"/>
Magnet- / Chipkarte	<input type="checkbox"/>	<input type="checkbox"/>
-----	<input type="checkbox"/>	<input type="checkbox"/>
keine	<input type="checkbox"/>	<input type="checkbox"/>

Mindestens User-ID mit Passwort.

3.4.5 Differenzierung zwischen User- und Administrationstätigkeit

nein ja, in Form

Differenzierung wird für erforderlich gehalten (Geringe Berechtigungen + Admin-Account).

3.4.6 Vier-Augen-Prinzip

nein ja, in Form

- | | | |
|---|--------------------------------------|--|
| <input type="checkbox"/> doppeltes Passwort für | <input type="checkbox"/> alle Admin. | <input type="checkbox"/> besondere Admin |
| <input type="checkbox"/> geteiltes Passwort für | <input type="checkbox"/> alle Admin. | <input type="checkbox"/> besondere Admin |
| <input type="checkbox"/> visuelle Kontrolle für | <input type="checkbox"/> alle Admin. | <input type="checkbox"/> besondere Admin |

☐ besondere Administratoren für: -----

4-Augenprinzip ist zwingend. Doppeltes oder geteiltes Passwort ist nicht für alle Administratoren zwingend.

3.4.7 Protokollierung der Administrationstätigkeit

Es erfolgt eine Protokollierung der Administrationstätigkeit

nein ja

Auswertung der Protokolle

nein ja, durch wen ----- wie häufig -----

Protokollierung (über System) ist zwingend. Die Auswertung sollte monatlich nicht nur bei Bedarf durch eine übergeordnete Stelle (z.B. IT-Sicherheitsbeauftragten) erfolgen.

3.5 Ausscheiden von Mitarbeitern

Folgende Aktivitäten erfolgen bei Ausscheiden von Mitarbeitern

nein ja

Einem ausscheidenden Mitarbeiter werden sämtliche eingerichteten Zugriffsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht.

Externe Zugangsberechtigungen via Datenübertragungseinrichtungen werden entzogen bzw. gelöscht.

Von einem ausscheidenden Mitarbeiter werden sämtliche Unterlagen, ausgehändigte Schlüssel, Ausweise sowie ausgeliehene IT-Geräte zurückgefordert.

Ausgeschiedenen Mitarbeitern wird der unkontrollierte Zutritt zum Gebäude verwehrt, insbesondere zu Räumen mit IT-Systemen.

Sämtliche mit Sicherheitsaufgaben betrauten Stellen werden über das Ausscheiden eines Mitarbeiters unterrichtet, insbesondere Pförtnerdienste, Administratoren und IT-Sicherheitsmanagement.

Ein „Nein“ wird nicht akzeptiert.

4. Weitergabekontrolle

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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

4.1 Übertragung personenbezogener Daten

4.1.1 Art und Weise der Übertragung

Schutz	nein	ja	wie
<input type="checkbox"/> Modem/ Telefonnetz			-----
<input type="checkbox"/> Fax			-----
<input type="checkbox"/> Internet (inkl. E-Mail Versand)			-----
<input type="checkbox"/> Standleitung			-----
<input type="checkbox"/> -----			-----

Datenübertragung muss immer verschlüsselt erfolgen entweder VPN oder PGP bzw. analoges Verfahren. Prüfung muss durch IT vorgenommen werden.

4.1.2 Zweck und Empfänger der Übertragung

Klärung, ob die genannten Zwecke der Übertragung für den Auftrag der SBK zwingend sind und mit dem geschlossenen Vertrag/zu schließenden Vertrag übereinstimmen oder ggf. entfallen könnten.

4.1.3 Identifizierung und Authentifizierung der Beteiligten

nein

ja

- | | |
|--|-------------------------------------|
| <input type="checkbox"/> Benutzerkennung | <input type="checkbox"/> Zertifikat |
| <input type="checkbox"/> Automatischer Rückruf | <input type="checkbox"/> Passwort |
| <input type="checkbox"/> ----- | |

Ein „Nein“ wird nicht akzeptiert.

4.1.4 Verschlüsselung der übertragenen Daten

nein ja, Verfahren _____ Verschlüsselte Daten _____

Ein „Nein“ wird nicht akzeptiert. Verschlüsselung sollte dem aktuellen Standard der elektronischen Signatur entsprechen oder VPN mit Serverzertifikat sein.

4.1.5 Protokollierung der Übertragung

nein ja, Art/Umfang der Daten _____

Ein „Nein“ wird nicht akzeptiert. Art der Daten, der Verschlüsselung, Datum, Uhrzeit, Wer.

4.1.6 Auswertung der Protokolle

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. Auswertung regelmäßig, mindestens monatlich.

4.1.7 Daten werden außerhalb des Europäischen Wirtschaftsraum übertragen

nein ja

Ein "Ja" wird grundsätzlich nicht akzeptiert. Wenn ein "Ja" angegeben wird, ist § 80 Abs. 2 SGB X und ggf. § 393 SGB V einzuhalten.

4.2 Datenträger

4.2.1 Einsatz von folgenden Datenträgern

☐ Festplatten ☐ USB Flash Drive ☐ USB Festplatten ☐ CD-Rom/DVD/Blu-Ray
☐ Papier ☐ Magnetbänder ☐ Cloud Speicher, Anbieter: _____

Sind die Datenträger verschlüsselt

nein ja, mit welchem Verfahren _____

Keine Vorgaben.

4.2.2 Schriftliche Regelungen über den Einsatz von Datenträgern inkl. Anfertigung von Datenträgerkopien

nein ja, bitte beifügen

Schriftliche Regelungen sind zwingend. Regelung muss Berechtigungskonzept, sowie Maßnahmen zur Lagerung und Schutz vor unberechtigten Zugriff enthalten. Weiterhin muss die Erstellung und Verwendung protokolliert werden, sowie die Vernichtung (siehe auch Ziffer 4.2.10).

4.2.3 Aufbewahrung von Datenträgern

- | | | |
|---|---|---|
| <input type="checkbox"/> Unverschlossen | <input type="checkbox"/> Robotersystem | <input type="checkbox"/> Schrank |
| <input type="checkbox"/> Archiv | <input type="checkbox"/> Sicherheitsbereich | <input type="checkbox"/> Sicherheitsschrank |
| <input type="checkbox"/> Revisionssicheres Archiv | <input type="checkbox"/> _____ | |

Aufbewahrung unverschlossen oder im Schrank oder nur im Archiv ist nicht zulässig.

4.2.4 Zugangsberechtigter Personenkreis zu Datenträgern

Eine Begrenzung auf wenige Mitarbeiter für die erforderlichen Aufgaben wird akzeptiert.

4.2.5 Datenträgerbestandskontrolle

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. Die Kontrolle ist mindestens wöchentlich durchzuführen.

4.2.6 Protokollierung des Entfernens von Datenträgern

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. Bei Häufigkeit ist die Angabe "Bei Anfall" in Ordnung.

4.2.7 Auswertung der Protokolle über das Entfernen von Datenträgern

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. Auswertung muss mindestens monatlich erfolgen.

Bei Bedarf ist nicht zulässig.

4.2.8 Anfertigung von Datenträgerkopien (Art/Umfang/Häufigkeit von Sicherungen)

- | | |
|---|--|
| <input type="checkbox"/> Vollsicherung | <input type="checkbox"/> Programmsicherung |
| <input type="checkbox"/> Änderungssicherung | <input type="checkbox"/> _____ |

Für folgende Server/Anwendungen _____

- | | | |
|--|---------------------------------------|------------------------------------|
| <input type="checkbox"/> täglich | <input type="checkbox"/> wöchentlich | <input type="checkbox"/> monatlich |
| <input type="checkbox"/> quartalsweise | <input type="checkbox"/> halbjährlich | <input type="checkbox"/> jährlich |
| <input type="checkbox"/> _____ | | |

Dauer der Aufbewahrung _____

Alle angegebenen Sicherungsmöglichkeiten sind zwingend. Diese sollten täglich, wöchentlich, monatlich erfolgen. Längerfristige Sicherungen werden nicht akzeptiert. Aufbewahrung länger als 1 Monat für Kundendaten erscheint nicht notwendig, in der Zeit wird eine Kontrolle durch die SBK erfolgen. Ausnahme: Eine längere Aufbewahrung ist ausschließlich zulässig, sofern die maßgebenden Aufbewahrungsfristen dies festlegen!

4.2.9 Externe Auslagerung von Datenträgern

nein ja, bei _____

Liegt hierzu eine schriftliche Auftragsvergabe vor nein ja

Zwingend räumlich getrennte Aufbewahrung (z.B. auch feuerfester Tresor). Schriftliche organisatorische Regelungen sind zwingend.

4.2.10 Regelungen über die Vernichtung von Datenträgern/Festplatten usw.

nein ja, folgende Regelungen (z. B. Anzahl der Löschvorgänge, Einhaltung DIN Norm 66399)

Ein „Nein“ wird nicht akzeptiert. Zertifikat/Entsorgungsprotokoll für Löschung muss durch den Vernichter vorliegen. Die Vernichtung muss nach DIN Norm 66399 mindestens auf Schutzklasse 3 und Sicherheitsstufe 4 erfolgen.

4.2.11 Protokollierung der Vernichtung von Datenträgern/Festplatten usw.

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. "Bei Anfall/bei Bedarf" wird bei der Angabe der Häufigkeit anerkannt.

4.2.12 Auswertung der Protokolle über Vernichtung von Datenträgern/Festplatten usw.

nein ja, durch wen _____ wie häufig _____

Ein „Nein“ wird nicht akzeptiert. Die Auswertung monatlich ist zwingend.

4.2.13 Externe Vernichtung von Datenträgern/Festplatten usw.

nein ja, bei _____

Liegt hierzu eine schriftliche Auftragsvergabe vor nein ja

Ist der Dienstleister zertifiziert nein ja

Ein „Nein“ wird nicht akzeptiert. Bei "Ja" muss es sich um einen zertifizierten Anbieter handeln.

4.3 Datenträgerversand

4.3.1 Datenträgertransport

Es findet ein Datenträgertransport statt (gilt auch für Sicherungskopien)

nein ja

Ein Datentransport ist unausweichlich, da verlangt wird, dass Sicherungen räumlich getrennt aufbewahrt werden.

4.3.2 Art des Transports

☐ Selbstabholung ☐ Bote/Kurier ☐ Firmeneigener Fahrdienst
☐ Fester Taxifahrer ☐ Postversand ☐ -----

Eine sichere Form ist zu wählen, wobei die Selbstabholung bzw. der firmeneigene Fahrdienst am sichersten sind.

4.3.3 Sicherung der Datenträger während des Transports

nein ja, durch ☐ Transportkoffer ☐ Verschlüsselung ☐ Wertbrief
☐ Wertpaket ☐ -----

Ein „Nein“ wird nicht akzeptiert. Mindestens sind Transportkoffer einzusetzen oder bei anderer Art muss verschlüsselt werden nach aktuellem Standard.

4.3.4 Liefer- bzw. Begleitschiene

nein ja ☐ Rückgabeschein ☐ Begleitschein ☐ Protokolldatei
☐ Liefer-/Abholschein ☐ -----

Sofern „nein“ bitte begründen -----

Grundsätzlich sollte mit „Ja“ geantwortet werden. Wenn ein „Nein“ angegeben wird, sollte eine nachvollziehbare Begründung geliefert werden.

4.4 Fernwartung von Systemen

4.4.1 Es findet Fernwartung statt

nein (weiter mit Frage 4.5)
ja ☐ Hardwarewartung ☐ Softwarewartung ☐ Betriebssystem
☐ Anwendung ☐ Benutzeradministration
☐ -----

Fernwartung ist zugelassen. Falls keine Fernwartung stattfindet, weiter mit 4.5.

4.4.2 Für unser Unternehmen gibt es ein Fernwartungskonzept

nein ja, bitte beifügen

Zwingend ist ein Fernwartungskonzept (Ausnahme: wenn nur eigene IT eingesetzt wird), Fernwartungskonzept muss die Art des Zuganges, der Autorisierung, der Protokollierung, Berechtigungen, Auswertung der Protokolle und Beauftragung enthalten. Weiterhin muss erläutert werden, ob nur im Beisein von eigener IT Fernwartung erfolgt und wer die Fernwartung startet.

4.4.3 Die Fernwartungstätigkeit erfolgt durch (Bitte Vertrag beifügen)

Hier sind externe oder interne Dienstleister denkbar. Bei externen Dienstleistern ist zusätzlich ein Fernwartungsvertrag erforderlich, welcher ggf. vorzulegen ist.

4.4.4 Leitungsweg

Schutz	nein	ja	wie
<input type="checkbox"/> Modem/Telefonnetz			-----
<input type="checkbox"/> Internet			-----
<input type="checkbox"/> Standleitung			-----
<input type="checkbox"/> -----			-----
für folgende Anwendungen	-----		

Als Standard wird eine Standleitung mit Schutz erwartet (z.B. VPN-Tunnel). Bei ISDN und Internet müssen Verschlüsselungsverfahren angegeben werden.

4.4.5 Fernwartungsverbindung

☐ Systemadministrator vor Ort ☐ Fernwartungstechniker

Beide Angaben sind denkbar.

4.4.6 Identifizierung und Authentifizierung

☐ nein

<input type="checkbox"/> Token	<input type="checkbox"/> Benutzerkennung	<input type="checkbox"/> automatischer Rückruf
<input type="checkbox"/> Passwort	<input type="checkbox"/> Zertifikat	<input type="checkbox"/> Vier-Augen-Prinzip
<input type="checkbox"/> -----		

Ein "Nein" wird nicht akzeptiert.

4.4.7 Zugriff auf personenbezogene Daten im Rahmen der Fernwartung

nein ja, bei _____

Eine Datenschutzvereinbarung liegt vor nein ja

Sofern ein Zugriff nicht ausgeschlossen werden kann ist eine Datenschutzvereinbarung zwingend. Ohne Datenschutzvereinbarung ist eine Zusammenarbeit mit der SBK nicht möglich.

4.4.8 Privilegien bei der Durchführung (Umfang des Zugriffsrechts)

- ☐ Benutzerrechte ☐ größtmögliche Privilegien (root, admin, etc.)
☐ Administrationsrechte ☐ Shell-Kommando-Zugriffe ☐ _____

Rechte sind abhängig von der Tätigkeit, Fernwartung des Betriebssystems benötigt Admin-Rechte, die Rechte müssen hinterlegt werden und der Aufgabe angepasst werden (Abhängig von Angaben bei Ziffer 4.4.1.)

4.4.9 Protokollierung der Fernwartung

nein ja, Art und Umfang _____

Ein "Nein" wird nicht akzeptiert. Siehe Anforderungen Fernwartungskonzept. Diese Daten müssen auch in der Protokollierung enthalten sein.

4.4.10 Auswertung der Protokolle

nein ja, durch wen _____ wie häufig _____

Ein "Nein" wird nicht akzeptiert. Monatliche Auswertung erforderlich.

4.5 Papierentsorgung

4.5.1 Entsorgung von bedrucktem Papier mit personenbezogenen Daten

- ☐ erfolgt nicht getrennt von sonstigem Papiermüll
☐ erfolgt getrennt von sonstigem Papiermüll
☐ erfolgt in regelmäßigen Abständen von ____
☐ erfolgt nach Bedarf, durchschnittlich alle ____
☐ erfolgt in ungesicherten Behältern (z. B. Altpapiertonne)
☐ erfolgt in gesicherten, verschlossenen Behältern

Zwingend ist eine getrennte Entsorgung von sonstigem Papiermüll in geschlossenen Behältern (Container). Abweichungen davon sind auf separatem Blatt mit Darstellung der Vorgehensweise zu begründen.

4.5.2 Zuständigkeit der Papierentsorgung

Sofern eine getrennte Entsorgung erfolgt, geben Sie bitte die Angaben für das Unternehmen an, welches für die Entsorgung der personenbezogenen Papierdaten beauftragt ist

Ist der Dienstleister zertifiziert

nein

ja

Es muss sich um einen zertifizierten Dienstleister handeln.

4.5.3 Protokollierung der Entsorgung

nein

ja, Art und Umfang -----

Eine Protokollierung ist zwingend.

4.5.4 Umsetzung Din Norm 66399

nein

ja (Schutzklasse und Sicherheitsstufe angeben)

Die Vernichtung muss nach Din Norm 66399 mindestens auf Schutzklasse 3 und Sicherheitsstufe 4 erfolgen.

5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten im Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.

5.1 Protokollierung der Eingabe

nein ja, ☐ immer ☐ Nutzer ☐ Lesen ☐ Schreiben
☐ auf Verdacht ☐ Zeitpunkt/Zeitraum ☐ Löschen ☐ Shell-Zugriff
☐ Programm-Zugriff

Eine Protokollierung wird immer zwingend verlangt (Nutzer, Zeitpunkt, Schreiben, lesen, löschen).

5.2 Auswertung der Protokolle

nein ja, durch wen _____ wie häufig _____

Ein "Nein" wird nicht akzeptiert, monatliche Auswertung erforderlich.

5.3 Aufbewahrung der Protokollierung

nein ja, wie lange _____

Ein "Nein" wird nicht akzeptiert. Eine Aufbewahrung von mindestens 1 Jahr ist ausreichend.

6. Auftragskontrolle von Unterauftragnehmern

Unterauftragnehmer sind alle Vertragspartner Ihres Unternehmens, die einen Zugriff auf Daten aus Ihrem Vertrag mit der SBK haben **könnten** (nicht nur Vertragspartner, die Sie im Rahmen unseres Vertrages unterstützen, sondern auch z.B. Reinigungsfirmen etc.). Auch hier bleibt die SBK die verantwortliche Stelle. Es wird gewährleistet, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

Bestehen mehrere Unterauftragsverhältnisse bitte die Punkte 6.1 und 6.2 im Anhang B je Unterauftragnehmer beantworten.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

7.1 Betriebsbereitschaft

24 Stunden an sieben Tagen pro Woche

von _____ Uhr bis _____ Uhr

☐ Montag

☐ Donnerstag

☐ Sonntag

☐ Dienstag

☐ Freitag

☐ Mittwoch

☐ Samstag

Einträge sind erforderlich.

7.2 Auslagerung von Sicherheitskopien

Sicherheitskopien werden ausgelagert

nein

ja, bei _____

Auslagerung muss zwingend erfolgen. Eine räumliche Trennung ist ausreichend.

7.3 Prüfung der Logdateien der Datensicherung

Es erfolgt eine Prüfung

nein

ja, durch wen _____ wie häufig _____

Eine Prüfung wird vorausgesetzt. Täglich ist sehr gut, mindestens wöchentlich.

7.4 Wiederherstellung der Daten

Die Wiederherstellung der Daten wird regelmäßig geübt und protokolliert

nein

ja, durch wen _____ wie häufig _____

Die Wiederherstellung muss regelmäßig geübt und protokolliert werden. Wiederherstellung üben reicht halbjährlich oder bei Änderung des Verfahrens.

7.5 Prüfung der Sicherungsmedien

Es wird regelmäßig geprüft und protokolliert, ob die Sicherungsmedien noch lesbar sind

nein

ja, durch wen _____ wie häufig _____

Prüfung muss zwingend erfolgen. Prüfung reicht regelmäßig halbjährlich oder bei Änderung des Verfahrens.

7.6 Unterbrechungsfreie Stromversorgung (USV)

Es besteht eine ausreichende unterbrechungsfreie Stromversorgung (USV)

nein ja

Ausreichende USV ist zwingend.

7.7 Verantwortlichkeit für IT-Sicherheit

Für die IT-Sicherheit ist verantwortlich

☐ Informations-/IT-Sicherheitsbeauftragter ☐ -----

IT-Leiter bzw. Administratoren sollten aufgrund evtl. Interessenskonflikte nicht verantwortlich sein.

7.8 Richtlinien zum Datenschutz und zur Datensicherheit

7.8.1 Es liegen schriftliche und aktuelle Richtlinien/Anweisungen zu den folgenden Aspekten vor und sind beigefügt

nein ja

Allgemeine Dienstanweisung zum Thema Datenschutz und Datensicherheit

Geeignete IT-Sicherheitsmaßnahmen (Datensicherungskonzept)

Sicherheits- und Notfallkonzept

IT-Sicherheitsanforderungen

Förderung des Sicherheitsbewusstseins (z.B. bei den Mitarbeitern)

Überwachung der Implementierung

Überwachung des laufenden Betriebs

Entdeckung u. Reaktion auf sicherheitsrelevante Risiken

Sicherheitszielen, -strategien

Analyse von Bedrohungen und Risiken

Zur Langzeit-Archivierung

Nutzung von E-Mail

Nutzung von Internet

Zur Systemadministration

Zur Netzwerkadministration

Schutz, Bekanntgabe und Vernichtung von Dateien

Zur Sicherheitsarchitektur

Bewertung über mögliche Schäden bei Verlust von Verfügbarkeit, Integrität oder Vertraulichkeit für die SBK

Sicherheitsleitlinien für Mitarbeiter (wenn ja, bitte beifügen)

Verfügen Sie über eine Zertifizierung

→ Wenn „ja“, welche (bitte Kopien beifügen) -----

Alle genannten Punkte sind mit "Ja" zu beantworten. Sofern die Unterlagen nicht beigefügt werden, ist eine Erklärung erforderlich.

7.8.2 Prüfung der Richtlinien/Anweisungen innerhalb der letzten 12 Monate

In den letzten 12 Monaten erfolgte eine Prüfung hinsichtlich der Effektivität

nein ja

Eine Prüfung ist zwingend erforderlich.

7.8.3 Einflussfaktoren

Folgende Faktoren beeinflussen die Effektivität der IT-Sicherheit unseres Unternehmens

nein ja

Zunehmende Komplexität der Sicherheitsbedrohung

Zeitmangel

Tempo der Veränderungen

Komplexität der Technologie

Unzureichende Sicherheitsfunktionen der Software

Mangel an Problembewusstsein der Mitarbeiter

Externe Zugriffe auf das Netz

Alle Punkte sollten mit "nein" beantwortet sein. Alle mit „ja“ beantworteten Punkte sind auf gesondertem Blatt zu erläutern und darzulegen, wie dem Risiko begegnet wird.

7.8.4 Folgenden Aktivitäten führen wir regelmäßig durch

nein ja

Wartung von Sicherheitseinrichtungen

Administrativer Support von Sicherheitseinrichtungen

Reaktion auf sicherheitsrelevante Ereignisse

Fortlaufende Überwachung der IT-Systeme

Change-Management

Überprüfung von Maßnahmen auf die Übereinstimmung der Sicherheitspolitik

Mitarbeiterschulungen

Alle Punkte sollten grundsätzlich mit "ja" beantwortet sein.

Ausnahme: Change Management ist nicht zwingend erforderlich.

7.8.5 Folgende Programme bzw. Maßnahmen setzen wir ein

nein ja

Basis-Benutzerpassworte
Einmal-Passwörter/Access Token/Smartcard
Mehrfach-Logons und -Passwörter
Single-Sign-On-Software

Virtual Private Network (VPN)
Secure Sockets Layer (SSL)
Spam-Filter
Paket-Filter
Content-Filter

Desktop-Antiviren-Software
Gateway-Antiviren-Software
Personal-Firewalls
Software für PC-Zugriffskontrolle
Automatisiertes Daten-Backup

Application-Firewalls
Netzwerk-Firewalls
Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)

Pro Block muss mindestens die Hälfte (2-3 Kästchen) mit JA angekreuzt sein, da die Verfahren aufeinander beruhen. Nicht zwingend Content-Filter, Software für PC-Zugriffskontrolle, IPS, Single-Sign-On-Software, Einmal-Passwörter.

7.8.6 Umgang mit Schutzprogrammen

Folgende Vorgehensweise ist Standard in unserem Unternehmen:

- ☐ Automatische Downloads
 - ☐ Regelmäßige Updates in Abständen von
 - ☐ Vor der Implementierung werden mögliche negative Auswirkungen auf die IT-Struktur geprüft
 - ☐ Updates erfolgen durch Serviceprovider
 - ☐ Auswertung von Vorfällen/Meldungen
 - ☐ Reaktion auf Vorfälle/Meldungen
 - ☐
- Anmerkungen

Folgende Punkte sind zwingend regelmäßig, täglich durchzuführen:

- Automatisch Downloads
- Regelmäßige Updates in Abständen von
- Vor der Implementierung werden mögliche negative Auswirkungen auf die IT-Struktur geprüft

- Auswertung von Vorfällen/Meldungen
- Reaktion auf Vorfälle/Meldungen

7.8.7 Schilderung von Verstößen/Vorkommnissen bezogen auf die IT-Sicherheit der letzten 12 Monate

- | | |
|--|---|
| <input type="checkbox"/> SPAM-Mails | <input type="checkbox"/> Viren/Würmer/Trojaner |
| <input type="checkbox"/> keine Verstöße/Vorkommnisse | <input type="checkbox"/> Datenverlust |
| <input type="checkbox"/> Dialer (z.B. 0190-Dialer) | <input type="checkbox"/> Hacker |
| <input type="checkbox"/> Interne Datenschutzverletzung | <input type="checkbox"/> Hardwareverlust durch <input type="checkbox"/> Diebstahl |
| <input type="checkbox"/> Ausfall | |
| <input type="checkbox"/> ----- | |

SPAM, Hardwareverlust, Viren können teilweise akzeptiert werden, Datenverlust, Hacker, interne Datenschutzverletzungen und Hardwareverlust durch Diebstahl werden nicht akzeptiert, eine Zusammenarbeit mit der SBK ist dann nicht möglich.

7.8.8 Die Verstöße/Vorkommnisse sind zurückzuführen auf

- | | |
|--|--|
| <input type="checkbox"/> Technische Ursache und menschliches Versagen/Fehler | <input type="checkbox"/> Technische Ursachen |
| <input type="checkbox"/> Menschliches Versagen/Fehler | <input type="checkbox"/> Missbrauch |
| <input type="checkbox"/> ----- | |
- Anmerkungen -----

Bei Angaben sind die Bemerkungen auszuwerten und ggf. einer Klärung zuzuführen.

7.8.9 Sicherheitsaudits

Es werden Sicherheitsaudits durchgeführt

nein ja (bitte Nachweise beifügen)

In welchen zeitlichen Abständen -----

Ein Sicherheitsaudit sollte erfolgt sein. Ein Zertifikat allein ist nicht ausreichend. Es sollte regelmäßig (mindestens alle zwei Jahre) ein Sicherheitsaudit durchgeführt werden. **Ohne Sicherheitsaudits ist eine Zusammenarbeit mit der SBK nicht möglich.**

7.8.10 Programmabbrüche/Programmfehler

Der Auftraggeber wird über Programmabbrüche/Programmfehler informiert

nein ja

Ein "Nein" wird nicht akzeptiert.

7.9 Löschkonzept

Ein Löschkonzept existiert

nein ja, bitte beifügen

Ein "Nein" wird nicht akzeptiert.

8. Trennungsgebot (bezogen auf die in 4.2.1 genannten Datenträger)

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

8.1 Abschottung personenbezogener Daten verschiedener speichernder Stellen gegeneinander

Es erfolgt eine Abschottung personenbezogener Daten

nein ja, wie

☐ Organisatorische Trennung

☐ Physikalische Trennung

Verfahren

Ein "Nein" wird nicht akzeptiert. Ohne organisatorische bzw. physikalische Trennung ist eine Zusammenarbeit mit der SBK nicht möglich.

8.2 Trennung der DV-Anlagen und Datenträger für besonders sensible Daten

Es erfolgt eine Trennung

nein ja, wie

☐ Organisatorische Trennung

☐ Physikalische Trennung

Art der Daten

Ein "Nein" wird nicht akzeptiert. Ohne organisatorische bzw. physikalische Trennung ist eine Zusammenarbeit mit der SBK nicht möglich.

9. Datenschutzbeauftragter

9.1 Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist vorhanden:

ja ☐ intern ☐ extern

nein, weil er noch nicht ernannt worden ist, obwohl es gesetzlich vorgeschrieben ist

nein, weil gesetzlich nicht vorgeschrieben

*Ein "Nein" wird nicht akzeptiert, wenn ein Datenschutzbeauftragter gesetzlich vorgeschrieben ist. Es besteht insoweit Klärungsbedarf. **Eine Zusammenarbeit mit der SBK ist dann nicht möglich.***

9.2 Automatisierte Verarbeitung personenbezogener Daten

Der Datenschutzbeauftragte wird frühzeitig informiert

nein ja

Bei allen geplanten automatisierten Verarbeitungen personenbezogener Daten

Bei automatisierter Verarbeitung personenbezogener Daten zur Durchführung der Vorabkontrolle

Ein "Nein" wird nicht akzeptiert.

9.3 Datenschutz- und Datensicherheitskontrollen

Es werden durch den Datenschutzbeauftragten regelmäßig Datenschutz- und Datensicherheitskontrollen durchgeführt:

nein ja (Bitte Bericht beifügen)

*Ein "Nein" wird nicht akzeptiert. **Eine Zusammenarbeit mit der SBK ist dann nicht möglich.***

9.4 Datenschulungen

Der Datenschutzbeauftragte führt regelmäßig Schulungen durch

nein ja, folgende Themen wurden aufgegriffen

Ein "Nein" wird nicht akzeptiert.

9.5 Verfahrensverzeichnis

Ein Verfahrensverzeichnis wird zugänglich für den Datenschutzbeauftragten geführt

nein ja

Ein "Nein" wird nicht akzeptiert.

9.6 Weiterbildung

Der Datenschutzbeauftragte bildet sich regelmäßig weiter

nein ja, durch folgende Maßnahmen _____

Ein "Nein" wird nicht akzeptiert.

Wir bestätigen die Richtigkeit der Angaben.

Ort, Datum

Unterschrift Datenschutzbeauftragter

Ort, Datum

Unterschrift Geschäftsleitung, Stempel

10. Anhang A – Anmerkungen und Beispiele für die korrekte Befüllung der Datenschutz- / Datensicherheitserklärung

Die in der Datenschutz- / Datensicherheitserklärung abgefragten Punkte beziehen sich ausdrücklich auf die allgemeine Betriebs- und Systemumgebung des Auftragnehmers, aus der heraus die Leistungen für den Auftraggeber erbracht werden.

Sicherheitsspezifische Anforderungen, die sich konkret aus der Leistungsbeschreibung ergeben, sind dort vertraglich geregelt und nicht Gegenstand der Datenschutz- / Datensicherheitserklärung.

In Abhängigkeit von der Art der zu erbringenden Leistungen ergeben sich unterschiedliche Perspektiven für die Beantwortung des Fragebogens, die wir nachfolgend exemplarisch darstellen. Die Perspektiven sind nicht trennscharf zu sehen und können fließend ineinander übergehen.

Betriebsleistungen

Betrachtungsgegenstand ist die allgemeine Betriebs- und Systemumgebung des Auftragnehmers, aus der heraus Mitarbeitende den Betrieb der DKS- Umgebung im Zusammenhang mit dem Auftrag erbringen.

Dies umfasst insbesondere die Maßnahmen zur Absicherung

- der Büro- und Betriebsräume, in denen Mitarbeitende Betriebstätigkeiten, Support- oder Koordinationstätigkeiten im Zusammenhang mit dem Auftrag übernehmen,
- der Arbeitsplatz- und Mobilgeräte dieser Mitarbeitenden, die für die Erbringung der Betriebstätigkeiten eingesetzt werden,
- der internen Netzwerke und Systeme, die diese Mitarbeitenden für die Erbringung der Betriebstätigkeiten sowie zur Ablage auftragsbezogener Daten (z. B. Betriebsdokumentation, Tickets, Konfigurationsunterlagen) nutzen,
- sowie der Zugänge dieser Mitarbeitenden zu den für den Auftrag relevanten Systemen und Umgebungen des Auftraggebers (z. B. Verwaltungsoberflächen, Remote-Zugänge, Administrationschnittstellen).

Es sind die Maßnahmen darzustellen, mit denen der Auftragnehmer die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten und Geschäftsgeheimnissen im Rahmen seiner Betriebsleistung sicherstellt.

Entwicklungsleistungen

Betrachtungsgegenstand ist die allgemeine Betriebs- und Systemumgebung des Auftragnehmers, aus der heraus Mitarbeitende Entwicklungs-, Build- und Testtätigkeiten im Zusammenhang mit dem Auftrag erbringen.

Der Geltungsbereich umfasst insbesondere die Maßnahmen zur Absicherung

- der Büro- und Betriebsräume, in denen Mitarbeitende Entwicklungs-, Build- oder Testtätigkeiten im Zusammenhang mit dem Auftrag übernehmen,
- der Arbeitsplatz- und Mobilgeräte dieser Mitarbeitenden, die für Entwicklungs-, Build- oder Testtätigkeiten eingesetzt werden,
- der internen Netzwerke und Systeme, die diese Mitarbeitenden für Entwicklungs-, Build- und Testtätigkeiten sowie zur Ablage auftragsbezogener Daten (z. B. Quellcode, Konfigurationsdateien, technische Dokumentation) nutzen,

- sowie der Zugänge dieser Mitarbeitenden zu Entwicklungs-, Integrations- und Testumgebungen, in denen Systeme für den Auftraggeber vorbereitet oder geprüft werden.

Es sind die Maßnahmen darzustellen, mit denen der Auftragnehmer die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten und Geschäftsgeheimnissen im Rahmen seiner Entwicklungsleistung sicherstellt.

Hosting

Betrachtungsgegenstand ist die allgemeine Betriebs- und Systemumgebung und insbesondere die Hosting-Umgebung des Auftragnehmers, aus der heraus Mitarbeitende Betriebs-, Administrations- und Überwachungstätigkeiten an der für den Auftrag eingesetzten Infrastruktur erbringen.

Der Geltungsbereich umfasst insbesondere die Maßnahmen zur Absicherung

- der Büro- und Betriebsräume einschließlich der Betriebsflächen in Rechenzentren bzw. Cloud-Standorten, in denen Mitarbeitende Betriebs- und Administrationsaufgaben für die dort betriebenen Systeme übernehmen,
- der Arbeitsplatz- und Mobilgeräte dieser Mitarbeitenden, die für Betriebs- und Administrationsaufgaben in den Rechenzentrums- bzw. Cloud-Umgebungen eingesetzt werden,
- der internen Netzwerke und Systeme, die diese Mitarbeitenden zur Administration und Überwachung der in den Rechenzentrums- bzw. Cloud-Umgebungen betriebenen Systeme sowie zur Ablage auftragsbezogener Daten (z. B. Betriebsdokumentation, Konfigurationsdaten) nutzen,
- sowie der Zugänge dieser Mitarbeitenden zu den in den Rechenzentrums- bzw. Cloud-Umgebungen betriebenen Systemen und zu den hierfür bereitgestellten Verwaltungs- und Administrationsschnittstellen.

Es sind die Maßnahmen darzustellen, mit denen der Auftragnehmer die Vertraulichkeit, Integrität und Verfügbarkeit der Infrastruktur sicherstellt, auf der Systeme für den Auftraggeber betrieben werden.

11. Anhang B - Auftragskontrolle von Unterauftragnehmern

Unterauftragnehmer sind alle Vertragspartner Ihres Unternehmens, die einen Zugriff auf Daten aus Ihrem Vertrag mit der SBK haben **könnten** (nicht nur Vertragspartner, die Sie im Rahmen unseres Vertrages unterstützen, sondern auch z.B. Reinigungsfirmen etc.). Auch hier bleibt die SBK die verantwortliche Stelle. Es wird gewährleistet, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

Bestehen mehrere Unterauftragsverhältnisse bitte die Punkte auf separatem Blatt je Unterauftragnehmer beantworten.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

6.1 Vertragsverhältnis zwischen Auftragnehmer und Ihnen als Auftraggeber

Auftragnehmer _____ Auftragsgegenstand _____

- ☐ keines
- ☐ mündlicher Vertrag
- ☐ schriftliches Angebot ohne besondere Weisungen
- ☐ Besondere Datenschutzregelungen
- ☐ keine besonderen Datenschutzregelungen im Hinblick auf §80 SGB X i.V.m Art. 32 DSGVO
- ☐ _____

Besondere Datenschutzregelungen sind erforderlich, wenn Eintrag vorgenommen wird. Bei nur einem mündlichen Vertrag oder nur einem schriftlichen Angebot ohne besondere Weisungen oder wenn keine besonderen Datenschutzregelungen im Hinblick auf § 80 SGB X i.V.m. Art. 32 DSGVO getroffen wurden, ist eine Zusammenarbeit mit der SBK nicht möglich.

6.2 Kontrolle Ihrer Auftragnehmer

Auftragnehmer _____

- ☐ Prüfung des Sicherheitskonzepts
- ☐ Besichtigung der Räumlichkeiten des Auftragnehmers
- ☐ Besichtigung der Datenverarbeitungsanlagen
- ☐ _____

Durchführung der Kontrollen durch wen _____

wie häufig _____

Wann zuletzt _____ Prüfbericht bitte beifügen.

Bei Unterauftragnehmern ist eine Prüfung zwingend. Als zeitlicher Abstand ist mindestens der Prüfrhythmus anzusetzen, in welchem Abstand die SBK Ihr Unternehmen prüft. Ohne eine Prüfung ist eine Zusammenarbeit mit der SBK nicht möglich. Der letzte Prüfbericht ist vorzulegen.

Notizen

Notizen

Notizen

Notizen