Anhang C: Kontrollkonzept

Kontrollkonzept für die Auftragskontrolle nach § 80 SGB X inkl. Checkliste für Kontrollen	
1. Schritt: Vorbereitung der Auftragskontrolle nach § 80 SGB X	Für die Vorbereitung der Auftragskontrolle nach § 80 SGB X bei einem Auftragnehmer bzw. einem Anbieter ist es erforderlich, folgende Unterlagen heranzuziehen: 1. Vertragsgegenstand/ Hauptvertrag 2. Datenschutzvertrag/ Datenschutzvereinbarung mit entsprechenden Anlagen (siehe Mustervertrag) – es muss geprüft werden, ob der bestehende Datenschutzvertrag den aktuellen Regelungen (siehe Mustervertrag) entspricht 3. Berichte über ggf. vorangegangene Kontrollen 4. ggf. bekannt gewordene Beschwerden im Zusammenhang mit Datenschutzverstößen Terminvereinbarung mit dem Auftragnehmer: In bestimmten Fällen kann auch eine unangemeldete Kontrolle angezeigt sein (z.B. bei der Papiervernichtung).
2. Schritt Durchführung der Auftragskontrolle (Dauer: 1 bis 2 Tage je nach Firmengröße/ Auftrag)	Vorgehen bei der Auftragskontrolle: 1. Zu Beginn sollte die Geschäftsführung, der betriebliche Datenschutzbeauftragte und ggf. der Leiter der DV-Abteilung über die Schwerpunkte der Auftragskontrolle informiert werden. Ziel des Besuchs ist es, sich davon zu überzeugen, dass die beschriebenen technischen und organisatorischen Maßnahmen vom Auftragnehmer auch tatsächlich eingehalten werden. Ggf. muss der bestehende Datenschutzvertrag den neuen (rechtlichen) Bedingungen angepasst werden. 2. Der Auftragnehmer sollte gebeten werden, das aktuelle Sicherheitskonzept inkl. PC-Dienstanweisung, die internen Datenschutzdienstanweisungen oder vergleichbare Papiere und eine Muster-Verpflichtungserklärung nach § 5 BDSG zur Verfügung zu stellen. 3. Des Weiteren sollte ein Nachweis über die Bestellung des betrieblichen Datenschutzbeauftragten und seine Fachkunde (z.B. Nachweis über Fort- und Weiterbildung, ggf. Zertifizierung) vorgelegt werden. 4. Anschließend ist es sinnvoll, sich den Verfahrensablauf der Auftragsabwicklung darstellen zu lassen und mit den Vertragsunterlagen zu vergleichen. 5. Es muss erfragt werden, mit welchen Firmen ggf. Unterauftragsverhältnisse bestehen (z.B. Reinigungsfirmen, Wartungsfirmen, Papiervernichtungsfirmen). In diesem Zusammenhang ist zu überprüfen, ob hier bereits vertragliche Regelungen/ Datenschutzvereinba-

	rungen getroffen wurden. 6. Es ist vorteilhaft, die Begehung der Räumlichkeiten des Auftragnehmers, in denen die Auftragsverarbeitung durchgeführt wird, am Schluss durchzuführen. Ggf. ist anschließend noch zu prüfen, ob alle erforderlichen Punkte der Checkliste angesprochen wurden. Es ist sinnvoll und notwendig, zum Abschluss der Kontrolle zusammen mit der Geschäftsführung bzw. deren Vertreter die ggf. erforderlichen Maßnahmen zur Sicherstellung des Datenschutzes und der Datensicherheit abzustimmen. Bei Beanstandungen ist es erforderlich, diese sofort anzusprechen und zu versuchen eine Übereinstimmung zur Umsetzung der festgestellten organisatorischen und technischen Maßnahmen zu erzielen. Des Weiteren muss bewertet werden, ob festgestellte Mängel ggf. direkte Auswirkungen auf das Vertragsverhältnis haben. Dies kann im Extremfall auch dazu führen, dass die Auftragsverarbeitung eingestellt/unterbrochen werden muss. Es ist allerdings sinnvoll, in derartigen Fällen sofort mit dem Referat Datenschutz Kontakt aufzunehmen.
Hinweise zur Durchführung der Auftragskontrolle aufgrund bereits gewonnener Erfahrungen	Eine ausreichend sichere Form der Auftragsdatenverarbeitung wird nur erreicht, wenn die vertraglichen Vereinbarungen und die tatsächlich getroffenen technischen und organisatorischen Maßnahmen einen hinreichenden Schutz bieten. Folgende Hinweise beziehen sich auf die Regelungen des § 78a SGB X (technische und organisatorische Maßnahmen): **<u>1. Zutrittskontrolle:</u>** Regelungsbedarf: a) Festlegung von Sicherheitsbereichen b) Zutrittskontrollsysteme (elektronisches System oder Schlüssel) c) Alarmanlagen, Bewegungsmelder, Wachpersonal, Videoüberwachung d) Festlegung von Zugangsberechtigungen (für Mitarbeiter und Fremde/Besucher) e) Legitimation der Zugangsberechtigung f) Kontrolle des Zugangs Mögliche Kontrollfragen: • Gibt es einen Verantwortlichen, der die gewünschten Berechtigungen (Schlüsselvergabe, Freischaltung) genehmigt? • Gibt es eine Schlüsselverwaltung? • Gibt es Regelungen für Firmenfremde (Handwerker, Besucher, Reinigungspersonal)? • Gibt es verschiedene/gegliederte Sicherheitsbereiche? • Erhalten mit der Codekarte wirklich nur berechtigte Personen Zugang zu den Sicherheitsbereichen? • Werden die Türen stets verschlossen gehalten oder gibt es eine Vorrichtung etc. (z.B. Holzkeil) mit der die Zugangskontrolle umgangen wird?

2. Zugangskontrolle:

Regelungsbedarf:

a) Identifizierung und Authentifizierung des Nutzers
b) Festlegung der Befugnisse für die Eingabe von Daten
c) Regelung bei Ausscheiden eines Mitarbeiters
d) Passwortverfahren
e) Sperrung (z.B. Bildschirmschoner)
f) Verschlüsselung sensibler Daten

Mögliche Kontrollfragen:

- Werden für Anwendungen und Programme Benutzernamen und Passwörter eingesetzt?
- Gibt es Regelungen über Vergabe, Änderung von Passwörtern?
- Gibt es Passwortregelungen (Mindestlänge, Sonderzeichen, etc.)?
- Wird eine Verschlüsselungssoftware eingesetzt?
- Erfolgt eine Protokollierung und werden die Protokolle ausgewertet?
- Wird beim Master-Passwort (Systemverwaltung) das Vier-Augen-Prinzip eingehalten? Wo wird das Passwort aufbewahrt? (z.B. im Tresor?)
- Gibt es einen Notfallplan?
- Ist die Passwortdatei verschlüsselt? Ist sie vor dem Zugriff durch Unberechtigte (auch Administrator) geschützt?

3. Zugriffskontrolle:

Regelungsbedarf:

a) Aufgabenbezogene Berechtigungen (Profile, Rollen, etc.)
b) Genehmigungsverfahren für Zugriffsrechte (Antragsteller, Genehmiger und Einrichter)

Mögliche Kontrollfragen:

- Werden einzelne Terminals und Identifikationsmerkmale ausschließlich für bestimmte Funktionen zugeordnet?
- Gibt es Datenstationen mit Funktionsberechtigungsschlüsseln?
- Direkter Zugriff, Stapelbetrieb, Zugriff auf Arbeitsbereiche (z.B. Spoolbetrieb)?
- Sind bereits ausgeschiedenen Mitarbeitern die Zugriffsrechte entzogen?
- Wie und wo erfolgt die Dokumentation? Liegen schriftliche Anträge vor? Oder gibt es ein prüfsicheres DV- System?

4. Weitergabekontrolle:

Regelungsbedarf:

a) Übertragungswege und -arten

b) Sicherungsmechanismen bei der Übertragung
c) Zuständigkeiten
d) Kontrollmöglichkeiten

Mögliche Kontrollfrage:

- Erfolgt die Übertragung über Internet, E-Mail, Tunnelverbindung (VPN), Punkt-zu-Punkt-Verbindung oder per Datenträger (CD, DVD)?
- Sind die Daten verschlüsselt?
- Ist der Zugriff auf die Datenlieferung geregelt?
- Ist eine elektronische Signatur notwendig bzw. im Einsatz?
- Werden die Übermittlungen protokolliert?
- Wie werden die Datenträger beim Transport gesichert?
- Sind die Datenträger eindeutig beschriftet?
- Wie werden die Datenträger entsorgt (intern oder extern)?
- Gibt es Regelungen, wie mit USB-Schnittstellen umgegangen wird? (Einschränkung oder Sperrung)
- Gibt es ein Verbot der Nutzung privater Datenträger, Software, etc.?
- Wo werden die Datenträger bis zur Vernichtung aufbewahrt? (Sicherheitsbereich, Tresor, Archiv?)

5. Eingabekontrolle:

Regelungsbedarf:

a) Dokumentation der Eingabeverfahren und der Möglichkeit, nachträglich die erfolgten Dateneingaben zu überprüfen

Mögliche Kontrollfragen:

- Werden die Dateneingaben, -veränderungen und -löschungen protokolliert?
- Wie werden die Protokolle kontrolliert?
- Gibt es Aufbewahrungsfristen für die Protokolle?

6. Auftragskontrolle:

Regelungsbedarf:

a) Eindeutige Vertragsgestaltung sowie die Kontrolle der Vertragsausführung

Mögliche Kontrollfragen:

- Liegt für die beauftragten Unterauftragnehmer die Zustimmung des Auftraggebers vor bzw. wurde der Auftraggeber darüber informiert?

	• Liegen entsprechende schriftliche Vereinbarungen vor? • Wurden die Unterauftragnehmer vom betrieblichen Datenschutzbeauftragten geprüft? **<u>7. Verfügbarkeitskontrolle:</u>** Regelungsbedarf: a) Erstellung eines umfassenden Sicherheitskonzepts Mögliche Kontrollfragen: • Wurde ein Datensicherheitskonzept erstellt? • Gibt es ein Notfallkonzept? **<u>8. Trennungsgebot</u>** Regelungsbedarf: a) Berücksichtigung des Trennungsgebots Mögliche Kontrollfragen: • Können die Daten unterschiedlicher Auftraggeber getrennt verarbeitet werden? Es müssen nicht zwingend physisch getrennte Systeme zum Einsatz kommen. Eine logische Trennung ist ausreichend. • Sind die DV-Systeme mandantenfähig? • Werden Produktions- und Testdaten getrennt? Achtung: Besonderer Wert ist auf die Datenverschlüsselung zu richten (Punkte 2 – 4)
<u>3. Schritt</u> Nachbereitung der Auftragskontrolle nach § 80 SGB X	Nach der durchgeführten Auftragskontrolle nach § 80 SGB X sind noch folgende Punkte umzusetzen: • Erstellen eines Prüfberichtes (siehe Musterprüfbericht) mit den Feststellungen der erforderlichen organisatorischen und technischen Maßnahmen. • Übersendung des Prüfberichtes an den Datenschutzbeauftragten. • Nach Freigabe durch den Datenschutzbeauftragten, Übersendung des Prüfberichts an die geprüfte Firma. • Ggf. Aktualisierung der Datenschutzvereinbarung nach § 80 SGB X entsprechend der Musterdatenschutzvereinbarung. • Die Prüfung ist abgeschlossen, sobald der Auftragnehmer die Umsetzung der im Prüfbericht getroffenen erforderlichen organisatorischen und technischen Maßnahmen bestätigt hat. Falls keine Bestätigung erforderlich ist, ist die Prüfung nach Übersendung des Berichts abgeschlossen.

Checkliste für die Durchführung der Kontrolle eines Auftragnehmers auf der Grundlage von § 80 SGB X

Firma: ...			
Datenverarbeitung im Unternehmen			
Zweck und Umfang der Auftragsverarbeitung und oder -nutzung:	...		
Datenschutzbeauftragter:		☐ ja	☐ nein
Name des Datenschutzbeauftragten: Datenschutzbeauftragter seit: Schriftliche Bestellung vom:	...		
Verpflichtungserklärung nach § 5 BDSG			
Sind alle bei der personenbezogenen Datenverarbeitung beschäftigten Personen auf das Datengeheimnis verpflichtet worden? *(Blanko-Muster vorlegen)*		☐ ja	☐ nein
	☐ separate Erklärung ☐ mit Merkblatt ☐ mit Verpflichtung Post-/Fernmeldegeheimnis	☐ mit Arbeitsvertrag	
Wer übernimmt die Verpflichtung?	☐ Datenschutzbeauftragter ☐ Personalabteilung ☐ Verwaltung ☐ Abteilungsleiter ☐ ...		
Räumliche Lage des Unternehmens			
	☐ Industriegebiet ☐ Wohngegend ☐ Ortszentrum ☐ belebte Straße		
	☐ Ortsrand ☐ abgeschiedene Gegend		
Bemerkungen zum Gebäude gem. **§ 78a SGB X**			
Allgemeines:	**Mehretagengebäude**	☐ ja	☐ nein
	weitere Mieter / Nutzer	☐ ja	☐ nein
	Eingangstüren / Anzahl der Eingänge	...	
	☐ elektronische Schließeinrichtung	☐ mechanische Schließeinrichtung	
	☐ Türknauf ☐ Türschnapper	☐ Türschließer	
	Fensterverglasung	☐ ja	☐ nein
	☐ im Parterre	☐ in den Obergeschossen	
	Sicherung der Kellerfenster	☐ ja	☐ nein
	Sicherung der Tiefgarage	☐ ja	☐ nein
	Zugangsmöglichkeiten aus der Tiefgarage	☐ ja	☐ nein
	wie viele? ... gesichert?	☐ ja	☐ nein
	Feuerlöscher, frei zugänglich	☐ ja	☐ nein
	Fluchtwege (Flure, Treppenhäuser)	☐ ja	☐ nein
	Kennzeichnung, frei zugänglich	☐ ja	☐ nein
	Fluchttüren nur von innen zu öffnen	☐ ja	☐ nein
	Panikschlösser	☐ ja	☐ nein

Prüfung der Geschäftsräume	Büroräume werden bei Dienstende verschlossen	☐ ja	☐ nein
	Umgang mit Publikumsverkehr	☐ ja	☐ nein
Kundenbereich	Mobiliar abschließbar / Schlösser intakt	☐ ja	☐ nein
	Einsicht auf Bildschirme	☐ ja	☐ nein
	Wartezonen / Besprechungsräume eingerichtet	☐ ja	☐ nein
Bürogeräte	Faxgeräte	☐ ja	☐ nein
	Kopiergeräte (keine Papierkörbe)	☐ ja	☐ nein
Reinigung der Büroräume	eigenes Personal	☐ ja	☐ nein
	Fremdpersonal tätig? auf Datenschutz verpflichtet	☐ ja	☐ nein
	☐ während Geschäftszeit	☐ nach Dienstschluss	
	☐ Schlüssel	☐ Generalschlüssel	

Aktenablage, Archiv und Aktenvernichtung

Beschaffenheit der Türen: ☐ Stahl ☐ Holz		☐ F30	☐ F60
Zugangsberechtigung		☐ ja	☐ nein
Schließeinrichtung		☐ ja	☐ nein
	zum Prüfzeitpunkt:	☐ offen	☐ geschlossen
Ablagesystem	☐ Stahlschränke	☐ offene Regale	
Aktenvernichtung		☐ ja	☐ nein
	☐ im Hause, eigene Geräte	☐ bei/durch Fremdfirma	
auf Datenschutz verpflichtet (bei Fremdfirma)		☐ ja	☐ nein

Zutrittskontrolle (Nr. 1 der Anlage zu § 9 BDSG)

Sicherungsmaßnahmen außerhalb der Geschäftsräume, Betriebsgelände und Gebäude betreffend

An folgenden Standorten des Auftragnehmers (bitte die jeweiligen Anschriften angeben) besteht die Möglichkeit, dass Daten, sonstige Informationen, technische Einrichtungen/Geräte für die Erbringung der Dienstleistung für die / den Auftraggeber vorhanden und genutzt werden	1. ... 2. ... 3. ... nn. ...
Beschreibung der allgemeinen technischen Ausstattungen, die für alle genannten Standorte zutreffen (z.B. PC, Drucker etc.):	...
Überwachung des Geländes/Gebäudes außerhalb der Betriebsstunden:	☐ eigenes Wachpersonal ☐ externer Wachdienst ☐ Bewegungsmelder ☐ Videoüberwachung ...

Alarmanlage:		☐ ja	☐ nein
Verbindung der Alarmanlage zu: ***** Externer Wachdienst Art der Herausgabe der Warnungen (Akustisch, Optisch, etc.)	☐ Feuerwehr	☐ Wachdienst*	☐ Polizei
	☐ zentraler Pförtner / Empfang		
	☐ Firmeninhaber / Firmenangehörige		
	☐ ...		

Sicherungsmaßnahmen innerhalb der Geschäftsräume

Ist für jeden Standort eine Bestimmung der schutzbedürftigen Räume eines Gebäudes erfolgt (auch auf mehrere Standorte verteilt. Dokumentation!) **Zutrittsregelung**	☐ ja	☐ nein
Wenn ja, wo ist diese Dokumentation jeweils einsehbar:	...	
Welche Räume sind generell als schutzbedürftige Räume deklariert worden?	☐ RZ-Bereich	☐ Maschinenraum
	☐ Serverraum	☐ TK-Anlage
	☐ Flurbereiche	☐ Büroräume
	☐ Besprechungsräume	☐ USV-Anlage (Kaltstrom)
	☐ ...	

Speziellen Sicherheitsmaßnahmen für die festgelegten schutzbedürftigen Räume einheitlich für alle Standorte:	
Gibt es eine generelle Schließeinrichtung:	☐ ja ☐ nein
Welcher Art:	☐ elektronisch ☐ mechanisch
Sicherung der Türen?	☐ mechanischer Türschließer ☐ Türknauf außen ☐ Sicherheitsbeschlag
Sicherung der Fenster?	☐ durchwurfhemmende Verglasung ☐ Spezialglas ☐ Sichtschutz
Brandschutz vorhanden?	☐ ja ☐ nein ☐ F30 ☐ T30
Klimaanlage vorhanden?	☐ ja ☐ nein
Wasserführende Leitungen mit Leckanzeige, Feuchtigkeitsmelder vorhanden?	☐ ja ☐ nein
Kabelführung (Stromleitungen)	☐ ja ☐ nein ☐ Wandkabelkanäle ☐ Doppelboden
Serverschränke, Verteilerschränke abgeschlossen?	☐ ja ☐ nein
RZ-Bereich	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
Maschinenraum	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
Serverraum	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
TK-Anlage	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
Flurbereiche	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
Büroräume	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
Besprechungsräume	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...
USV-Anlage	☐ Videoüberwachung ☐ Rauchmelder ☐ Bewegungsmelder ☐ Brandmeldesystem mit Verbindung Feuerwehr ☐ Einbruchmeldeanlage mit Alarmschaltung ☐ Polizei ☐ Sicherheitsdienst ☐ Alarmanlage mit Verbindung externer Wachdienst ☐ ...

Ist eine Dokumentation über Vergabe/Rückgabe von Tür-Schlüsseln vorhanden?		☐ ja	☐ nein
Wo ist die Dokumentation für jeden Standort einsehbar.	...		
Erfolgt an jedem Standort eine Besucherüberwachung		☐ ja	☐ nein
Wenn ja, in welcher Form findet die Überwachung statt:	☐ in Begleitung von Mitarbeitern ☐ Besucherausweis, sichtbar tragend ☐ Laufzettel / Besucherschein ☐ ...	☐ Besucherbuch	
Begründung, wenn an den Standorten keine Besucherüberwachung stattfindet – ggf. getrennt nach Standorten	...		
Zugangskontrolle (Nr. 2 der Anlage zu § 9 BDSG)			
Erfolgt eine Dokumentation der Vergabe sowie der Löschung von Zugangsberechtigungen und Zugangsmitteln?	☐ ja	☐ nein	☐ teilweise
Wenn ja, wo ist diese Dokumentation einsehbar:	...		
Finden Penetrationstests statt:		☐ ja	☐ nein
wenn ja, wie häufig (in einem Jahr)?	...		
von wem / welche Firma?	...		
Benutzerauthentifikation			
Welche generellen Regelungen gelten für alle Standorte:		*Client*	Host
Identifikation von Benutzern	*User-ID*	☐	☐
	☐ *Magnetkarte* ☐ *Chipkarte*	☐	☐
	...	☐	☐
	keine	☐	☐
Authentifikation von Benutzern	☐ *Passwort* ☐ *Chipkarte*	☐	☐
	...	☐	☐
	keine	☐	☐
Single Logon. Single Sign On	☐ *ja* ☐ *Nein*	☐	☐
Passwortkonventionen **Hier Anzahl der Anmeldeversuche (Falschangabe des Passwortes)*	*Einhaltung*	*Client*	Host
	☐ *Zeichen Mindestlänge (min. 6)*	..	..
	☐ *Ausschluss Trivialkennworte*	☐	☐
	☐ *Klein-/Großbuchstaben*	☐	☐
	☐ *Zahl*	☐	☐
	☐ *Sonderzeichen*	☐	☐
	☐ *Tage Gültigkeitsdauer (z. B. 90)*	..	..
	☐ *Zahl der Generationen (z.B. 5)*	..	..
	☐ *Kontensperrungsschwelle**	..	..
	☐ *keine*	☐	☐
Kontrolle der Passwortkonventionen		☐ ja	☐ nein
Durch wen: ...	*Wie häufig in einem Jahr: ...*		
Passwörter für den Ausnahmefall (Hier Notfalluser)		☐ ja	☐ nein
[1] Passwortkomplexität oder Passwortrichtlinien (*gültig für die ganze Domäne*) [2] z. B. Safe	[1]*Art der Passwörter: ...* [2]*Art der Hinterlegung: ...* *Dokumentation der Nutzung: ...*		
Schutz vor unbefugtem Zugriff der Berechtigungs- und Passworttabellen	☐ *Verschlüsselung* ☐ *versteckte Verzeichnisse (Shadow-Files)* ☐ ...		
Passwortgeschützter Bildschirmschoner		☐ ja	☐ nein
Sperrung der Zugangsberechtigungen bei längerer Abwesenheit von Benutzern		☐ ja	☐ nein
Wie? ...			

Zugriffskontrolle (Nr. 3 der Anlage zu § 9 BDSG)		
Ist ein Berechtigungskonzept für jeden Standort vorhanden?	☐ ja	☐ nein
Wenn ja, wer führt es und wo ist dieses einsehbar?	...	
Wen nein, warum nicht? bitte je Standort begründen	... ...	
In welcher Form wurden Regelungen bezüglich der Befugnisse für die • Eingabe von Daten, • Kenntnisnahme gespeicherter Daten, • Veränderung gespeicherter Daten • Löschung gespeicherter Daten, den Mitarbeitern bekannt gegeben?	☐ *mündlich* ☐ *schriftlich* ☐ *keine* ☐ *mündlich* ☐ *schriftlich* ☐ *keine* ☐ *mündlich* ☐ *schriftlich* ☐ *keine* ☐ *mündlich* ☐ *schriftlich* ☐ *keine*	
Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?	☐ ja	☐ nein
Wo ist es dokumentiert?	...	
Technische Realisierung der unterschiedlichen Zugriffsberechtigungen	☐ *Programmausführung* ☐ *Datei* ☐ *Datensatz* ☐ *Datenfeld* ☐ *Terminal* ☐ *Shell-Zugriff*	☐ *Lesen* ☐ *Schreiben* ☐ *Löschen* ☐ *Keine*
Protokollierung der Zugriffe der Benutzer	☐ *Programmausführung* ☐ *Schreiben von Daten* ☐ *Lesen von Daten* ☐ *versuchter Richtlinienverstoß*	☐ *Shell-Zugriff* ☐ *Löschen* ☐ *An / Abmeldung*
Auswertung der Protokolle	☐ ja	☐ nein
Durch wen: ...	*Wie häufig im Jahr: ...*	
Welche Aufbewahrungszeiträume sind für die Protokolle vorgesehen?	*...*	
Kryptographische Verschlüsselung gespeicherter personenbezogener Daten:	☐ ja	☐ nein
Verfahren: ...	*Verschlüsselte Daten: ...*	
Ist ein Virenschutz vorhanden und aktuell?	☐ ja	☐ nein
Welcher Kopierschutz ist generell für die Arbeitsplätze der Mitarbeiter aktiviert *****Prüfung von Schnittstellen, z.B. Infrarot, Bluetooth, USB mit Hilfe von Anwendungen	☐ Kein Diskettenlaufwerk ☐ Kein CD-Brenner ☐ Laufwerk-Schloss ☐ Download-Funktion deaktiviert ☐ Kopieren auf Diskette deaktiviert ☐ Kopierschutz nicht vorhanden	☐ Schnittstellenprüfung***** ☐ keine Infrarot ☐ keine Bluetooth ☐ keine USB ☐ keine Wireless ☐ ...
Systemadministration (nur für Administrative Zwecke! Bei 1 Person-Betrieb muss ein separater Account eingerichtet werden)		
Ist ein Administrationskonzept für alle Standorte vorhanden?	☐ ja	☐ nein
Abgestufte Administrationsrechte	☐ ja	☐ nein
Art der Differenzierung:	☐ Systemadministration ☐ Datenbankadministration ☐ Vergabe der Benutzerberechtigungen ☐ Einrichten von Benutzerberechtigungen	
Zuständig für Systemadministration	Name: ...	Funktion: ...
Identifizierung und Authentifizierung	☐ *Benutzerkennung* ☐ *Passwort* ☐ *Chipkarte* ☐ *Magnetkarte* ☐ *keine* ☐ ...	
Vier-Augen-Prinzip	☐ ja	☐ nein
	☐ *Vier-Augen-Prinzip* ☐ *doppeltes Passwort* ☐ *geteiltes Passwort* ☐ *für alle Administratoren* ☐ *für besondere Administratoren*	
Protokollierung der Administrationstätigkeiten und Auswertung der Protokolle:	☐ ja	☐ nein
Durch wen: ...	*Wie häufig im Jahr: ...*	
Welche Aufbewahrungszeiträume sind für die Protokollierung vorgesehen?	*...*	

Zweckbindung bei der Nutzung von Protokolldaten		
Wird bei der Nutzung von Protokolldaten auf die Zweckbindung geachtet?	☐ ja	☐ nein
Sind alle, die Zugriff auf Protokolldaten haben, auf die Einhaltung der Zweckbindung hingewiesen worden?	☐ ja	☐ nein
Wie lange werden Protokolldaten aufbewahrt?	...	
Werden die Protokolldaten regelmäßig gelöscht?	☐ ja	☐ nein
Weitergabekontrolle (Nr. 4 der Anlage zu § 9 BDSG)		
Automatisierte Übertragung		
Gibt es für alle Standorte einheitliche Regelungen für die Übertragung personenbezogener Daten	☐ ja	☐ nein
Wenn ja, Detailbeschreibung	...	
Art/Umfang der Daten:	...	
Zwecke der Übertragung:	...	
beteiligte Stellen:	...	
Art der Übertragung	☐ *Modem/Telefonnetz* ☐ *ISDN* ☐ *Internet* ☐ *Standleitung* ☐ ...	
Identifizierung und Authentifizierung (z. B. Token-Card)	☐ *keine* ☐ *automatischer Rückruf* ☐ *Rufnummernidentifikation (ISDN)* ☐ *Benutzerkennung* ☐ *Passwort* ☐ ...	
Kryptographische Verschlüsselung der übertragenen Daten:	☐ ja	☐ nein
Verfahren: ...	*Verschlüsselte Daten: ...*	
Protokollierung der Datenübertragung	☐ ja	☐ nein
	Art/Umfang: ...	
Auswertung der Protokolle:	☐ ja	☐ nein
Durch wen: ...	*Wie häufig im Jahr: ...*	
Abwehr unberechtigter Zugriffe aus dem Telekommunikations-Netz	☐ *keine besonderen Maßnahmen* ☐ *Firewall* ☐ ...	
Wenn nein, Standorte ermitteln, bei denen dieses nicht zutreffend ist und Begründung nennen.		
Datenträger		
Gibt es für alle Standorte einheitliche schriftliche Regelungen über den Einsatz von Datenträgern inkl. Anfertigen von Datenträgerkopien	☐ ja	☐ nein
In welchen Bereichen befinden sich Datenträger:	☐ Keine Beschränkung ☐ Schrank ☐ Archiv ☐ Sicherheitsschrank ☐ Robotersystem ☐ Sicherheitsbereich ☐ ...	
Aufbewahrung von Datenträgern	☐ unverschlossen ☐ Schrank ☐ Archiv ☐ Sicherheitsschrank ☐ Robotersystem ☐ Sicherheitsbereich ☐ ...	
Entfernung von Datenträgern aus Bereichen:	☐ ja	☐ nein
und zwar für folgende Zwecke:	...	
Wird dieser Vorgang dokumentiert:	☐ ja	☐ nein
Finden an allen Standorten Datenträgerbestandskontrollen statt?	☐ ja	☐ nein
Wenn nein, Standorte ermitteln und Begründung einholen.		
Protokollierung des Entfernens von Datenträgern und Auswertung der Protokolle	☐ ja	☐ nein
Anfertigung von Datenträgerkopien		
Art und Umfang der Sicherung:	☐ Vollsicherung ☐ Änderungssicherung ☐ Programmsicherung ☐ ...	
Häufigkeit:	☐ täglich ☐ wöchentlich ☐ monatlich ☐ Quartalsweise ☐ halbjährlich ☐ jährlich ☐ ... Dauer der Aufbewahrung: ...	

Externe Auslagerung von Datenträgern:		☐ ja	☐ nein
Ort der Auslagerung:	bei ...		
Gibt es an allen Standorten Regelungen über die Vernichtung von Datenträgern:		☐ ja	☐ nein
Ermitteln der Standorte, bei denen keine Regelungen bestehen und begründen			
Protokollierung der Vernichtung von Datenträgern		☐ ja	☐ nein
Externe Vernichtung von Datenträgern		☐ ja	☐ nein
Schriftliche Auftragsvergabe		☐ ja	☐ nein
Firmen und Anschriften angeben, bei denen die Vernichtung vorgenommen wird:			
... ...			
Datenträgerversand			
Gibt es für alle Standorte Regelungen für den Transport:		☐ ja	☐ nein
Wenn nein, Begründung je Standort: ...			
Art des Transportes	☐ Selbstabholung ☐ firmeneigener Fahrdienst ☐ Postversand ☐ Bote /Kurierdienst /fester Taxifahrer ☐ ...		
Sicherung der Datenträger während des Transportes:		☐ ja	☐ nein
	☐ Transportkoffer ☐ Wertbrief ☐ Wertpaket ☐ Verschlüsselung ☐ ...		
Liefer- und Begleitscheine:		☐ ja	☐ nein
☐ Rückgabeschein ☐ Begleitschein ☐ Liefer-/Abholschein ☐ ...			
Fernwartung			
Finden durch Externe Fernwartungs- und Reparaturarbeiten statt?		☐ ja	☐ nein
☐ *Hardwarewartung* ☐ *Softwarewartung* ☐ *Betriebssystem* ☐ *Anwendung* ☐ *Benutzeradministration* ☐ *...*			
Angabe der Firmen und deren jeweiligen Wartungsbereiche – mit vollständiger Anschrift – hier ist auch die Angabe von Konzerntöchtern erforderlich	...		
Ist ein Fernwartungskonzept für alle Standorte vorhanden:		☐ ja	☐ nein
Wenn ja, Grundbedingungen, die für alle Standorte gelten, angeben: ...			
Findet an allen Standorten eine Beaufsichtigung der Externen im Hause durch fachkundige Mitarbeiter statt:		☐ ja	☐ nein
Fernwartungsverbindung:	☐ Systemadministrator vor Ort ☐ Fernwartungstechniker		
Identifizierung und Authentifizierung:	☐ *Vier-Augen-Prinzip (doppeltes oder geteiltes Passwort)* ☐ *Rufnummernidentifikation (ISDN)* ☐ *automatischer Rückruf* ☐ *Passwort* ☐ *Benutzerkennung* ☐ ... ☐ *keine*		
Zugriff auf personenbezogene Daten bei der Fernwartung:		☐ ja	☐ nein
Kryptographische Verschlüsselung der Daten bei der Übertragung:		☐ ja	☐ nein
	Verfahren: ... *Verschlüsselte Daten: ...*		
Privilegien bei der Durchführung:	☐ Größtmögliche Privilegien (root, admin etc.) ☐ Benutzerrechte ☐ Administrationsrechte ☐ Shell-Kommando-Zugriff ☐ *...*		
Protokollierung / Dokumentation der Fernwartung:		☐ ja	☐ nein
	Art/Umfang: ...		

Auswertung der Protokolle:		☐ ja	☐ nein
	☐ online ohne Eingriffsmöglichkeiten ☐ online mit Eingriffsmöglichkeiten (Remote) ☐ offline (nachträglich)	☐ nein	
Änderung der Passwörter nach Abschluss von Wartungs- oder Reparaturarbeiten?		☐ ja	☐ nein
Protokollierung, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde?		☐ ja	☐ nein ☐ teilweise
Überprüfung der IT-Systeme oder Komponenten nach der Rückgabe auf Vollständigkeit?		☐ ja	☐ nein ☐ teilweise
Änderung der Passwörter?		☐ ja	☐ nein ☐ teilweise
Durchführung eines Computer-Viren-Check nach Rückgabe?		☐ ja	☐ nein ☐ teilweise
Überprüfung aller Dateien oder Programme, die sich auf dem reparierten Gerät befinden, auf Integrität?		☐ ja	☐ nein ☐ teilweise
Eingabekontrolle (Nr. 5 der Anlage zu § 9 BDSG)			
Protokollierung der Eingabe		☐ ja	☐ nein
Was wird protokolliert?	☐ Dateien ☐ Datensätze ☐ Datenfelder		
Ist aus der Protokollierung erkennbar			
	• von welchem Mitarbeiter	☐ ja	☐ nein
	• welche Daten	☐ ja	☐ nein
	eingegeben	☐ ja	☐ nein
	verändert	☐ ja	☐ nein
	entfernt	☐ ja	☐ nein
	wurden?		
Auswertung der Protokolle		☐ ja	☐ nein
Durch wen: ...	*Wie häufig: ...*		
Auftragskontrolle (Nr. 6 der Anlage zu § 9 BDSG)			
Vertragsverhältnis zwischen Auftragnehmer und Auftraggeber:		☐ AGB	
	☐ Standard-Dienstleistungsvertrag ☐ besondere Datenschutzregelungen ☐ Festlegung Subunternehmer ☐ ...		
Kontrollmaßnahmen des Auftraggebers:	☐ Besichtigung der Räumlichkeiten des Auftragnehmers ☐ Besichtigung der Datenverarbeitungsanlagen ☐ Prüfung des Sicherheitskonzeptes ☐ ...		
Durchführung der Kontrolle	Durch wen: ...	Wie häufig: ...	
Verfügbarkeitskontrolle (Nr. 7 der Anlage zu § 9 BDSG)			
Betriebsbereitschaft:	☐ 8-Stunden ☐ 24-Stunden	von ...	bis ...
Notfallkonzept vorhanden (Katastrophenfall)?		☐ ja	☐ nein
Auslagerung von Sicherungskopien		☐ ja	☐ nein
Ist die Aktualität von Sicherungskopien (Katastrophensicherung) gewährleistet?		☐ ja	☐ nein
USV-Anlage (Kaltstrom, Not-Stromversorgungsanlage)		☐ ja	☐ nein
Notfallhandbuch vorhanden?		☐ ja	☐ nein
Notfallhandbuch aktuell und den Mitarbeitern bekannt?		☐ ja	☐ nein
Trennungsgebot (Nr. 8 der Anlage zu § 9 BDSG)			
Abschottung der personenbezogenen Daten der speichernder Stellen gegeneinander		☐ ja	☐ nein
Art der Abschottung:	☐ Logische Trennung	☐ Physikalische Trennung	
Trennung der DV-Anlagen und Datenträger für besonders sensible Daten		☐ ja	☐ nein
☐ physikalisch (Gesamtsystem) ☐ logisch (Betriebssystem)	☐ physikalisch (Datenträger) ☐ logisch (Anwendung)		

Übermittlung personenbezogener Daten ins Ausland		
Findet eine Übermittlung personenbezogener Daten in das Ausland statt?	☐ ja	☐ nein
wenn ja, in welche Länder, an welche Firmen (auch Konzerntöchter angeben): ... Welchen Zwecken dient die Datenübermittlung? (bitte konkrete Beschreibung der Zweckbestimmung(en))*: ...*		
Vorlage einer Auflistung (Firmenbezeichnung und Anschrift der Firma) , für welche Aufgaben bzw. welche Geräte Firmen mit der Wahrnehmung von Prüfungs- und Wartungsarbeiten beauftragt wurden. **Hinweis:** Diese Firmen sind für den Auftraggeber ein meldepflichtiger Tatbestand gegenüber der zuständigen Aufsichtsbehörde, § 80 Abs. 7 SGB X		
Firmenbezeichnung, Anschrift:	...	
Aufgabenbereich:	...	
Sonstige Hinweise/Vermerke:		

Anlage: Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses
Merkblatt zur Verpflichtungserklärung Texte der §§ 5, 43 Absatz 2, 44 BDSG
BDSG: § 5 Datengeheimnis
Anlage (zu § 9 Satz 1 BDSG)
§ 78a Technische und organisatorische Maßnahmen

Anlage

BDSG: § 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Anlage (zu § 9 Satz 1 BDSG)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. 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 (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Verpflichtungserklärung nach § 5 des Bundesdatenschutzgesetzes (BDSG) zur Wahrung des Datengeheimnisses

Name der verantwortlichen Stelle

Sehr geehrte(r) Frau/Herr _____

aufgrund Ihrer Aufgabenstellung verpflichte ich Sie auf die Wahrung des Datengeheimnisses nach § 5 BDSG. Es ist Ihnen nach dieser Vorschrift untersagt, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.

Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen das Datengeheimnis können nach §§ 44, 43 Absatz 2 BDSG sowie nach anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden.
In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

Eine unterschriebene Zweitschrift dieses Schreibens reichen Sie bitte an die Personalabteilung zurück.

, _____ _____

Ort, Datum Unterschrift der verantwortlichen Stelle

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verpflichtungserklärung (Texte der §§ 5, 43 Absatz 2, 44 BDSG) habe ich erhalten.

, _____ _____

Ort, Datum Unterschrift des Verpflichteten

Merkblatt zur Verpflichtungserklärung
§ 5 BDSG – Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 Absatz 2 BDSG – Bußgeldvorschriften

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

§ 44 BDSG – Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

§ 78 a Technische und organisatorische Maßnahmen

1 Die in § 35 SGB I genannten Stellen, die selbst oder im Auftrag Sozialdaten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzbuches, insbesondere die in der Anlage zu dieser Vorschrift genannten Anforderungen, zu gewährleisten. 2 Maßnahmen sind nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
Satz 1 geändert durch G vom 18. 5. 2001 (BGBl I S. 904).

Anlage (zu § 78 a)

Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass Sozialdaten 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 von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können (Auftragskontrolle),

7. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren

Anlage neugefasst durch G vom 18. 5. 2001 (BGBl I S. 904), geändert durch G vom 05.08.2010 (BGBl I s. 1127)
Zu § 78 a: Vgl. RdSchr. 01 f Zu § 78 a SGB X.