Checklisten- und Datenquelle: https://www.datenschutz-wiki.de/Checkliste_TOM_Internetauftritt

Checkliste Technische und organisatorische Maßnahmen (Anlage zu § 9 Satz 1 BDSG a.F.)

Die nachfolgende Übersicht beruht auf der Checkliste zur Erfüllung der Aufgaben nach § 9 BDSG a.F. und Anlage, die anhand von Prüflisten der Datenschutzaufsichtsbehörden erstellt und angepasst wurde.

Organisationskontrolle (im BDSG a.F. nicht mehr als eigenständige Nr. in der Anlage aufgeführt)
"die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird"

Nr.	Vorgabe	erfüllt	nicht erfüllt	nicht erforderlich	Bemerkungen
1.1	Betriebsrat vorhanden?				
1.2	**Feststellung des Schutzbedarfs der personenbezogenen Daten:**				
1.2.1	Kundendaten				
1.2.2	Lieferantendaten				
1.2.3	Mitarbeiterdaten				
1.2.4	Besondere personenbezogene Daten gem. § 3 Abs. 9 BDSG a.F.				
1.3	Risikoanalyse liegt vor?				
1.4	Wird der BSI IT-Grundschutz umgesetzt?				
1.5	**Schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen**				
1.5.1	IT-Sicherheitskonzeption				
1.5.2	IT-Sicherheitsrichtlinien				
1.5.3	Arbeits- und Verfahrensanweisungen				
1.5.4	Stellenbeschreibungen				
1.6	Mitbenutzung der DV-Anlagen durch Fremdfirmen				
1.7	Mitbenutzung der TK-Anlagen durch Fremdfirmen				
1.8	Urlaubs-/Krankheitsvertretung des DV-Verantwortlichen				
1.9	DV-Revision, interne Revision				

1.10	Ausreichende Funktionstrennung, 4-Augen-Prinzip				
1.11	Regelungen zur Beschaffung von Hard- und Software				
1.12	Schriftliches Programmfreigabeverfahren				
1.13	Regelungen über Sicherung des Datenbestandes				
1.14	Regelmäßige Hinweise, Ermahnungen um das Problembewusstsein zu fördern				
1.15	Gelegentliche, unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen				
1.16	IT-Versicherungen				
1.17	**Ist ein Datenschutzbeauftragter (DSB) bestellt (§ 4f BDSG a.F.)?**				**Begründung, wenn „nicht erforderlich“**
1.17.1	Schriftliche Bestellung des DSB				1.17.1 bis 1.17.8 entfallen, wenn „nicht erforderlich"
1.17.2	Betriebliche Stellung				
1.17.2.1	hauptamtlich				
1.17.2.2	nebenamtlich				Haupttätigkeit? ... Wie viel Zeit zur Aufgabenerfüllung? ...
1.17.2.3	extern				
1.17.2.4	freiwillig bestellt (ohne gesetzlichen Zwang)				
1.17.2.5	der Geschäftsleitung direkt unterstellt				Wenn „Nein“, wem?
1.17.2.6	weisungsfrei				
1.17.2.7	Sind die Kündigungsregeln bekannt und werden sie umgesetzt?				
1.17.3	Liegt Kurzbeschreibung des beruflichen Werdeganges vor?				Ist der Aufsichtsbehörde vorzulegen
1.17.4	Welche Fortbildungsmaßnahmen sind abgeschlossen?				Ist der Aufsichtsbehörde vorzulegen
1.17.5	Welche Fortbildungsmaßnahmen sind geplant?				
1.17.6	Werden Fortbildungsmaßnahmen ermöglicht und entsprechende Kosten geplant/übernommen?				

1.17.7	Stellen-/Aufgabenbeschreibung vorhanden?				Ist der Aufsichtsbehörde vorzulegen
1.17.8	Tätigkeitsberichte des DSB				Ist der Aufsichtsbehörde vorzulegen
1.18	Datenschutzordnung				Ist der Aufsichtsbehörde vorzulegen
1.19	Verpflichtung nach § 5 BDSG a.F.				Ist der Aufsichtsbehörde vorzulegen
1.20	Verpflichtung nach § 88 TKG				Ist der Aufsichtsbehörde vorzulegen
1.21	Schulungs-/Informationsnachweise (§ 4g BDSG a.F.)				Ist der Aufsichtsbehörde vorzulegen
1.22	Verfahrensübersicht für jedermann (§ 4g BDSG a.F.)				Ist der Aufsichtsbehörde vorzulegen
1.23	Interne Verfahrensübersichten (§ 4d, § 4e, § 4g BDSG a.F.)				Ist der Aufsichtsbehörde vorzulegen
1.24	Verfahren zur Sicherung der Rechte von Betroffenen				Ist der Aufsichtsbehörde vorzulegen

Zutrittskontrolle (Anlage Nr.1)
"Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren"

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
2.1	**Gebäudeart**				
2.1.1	Innerhalb eines Betriebsgeländes				
2.1.2	Bürogebäude				
2.1.3	Büro- und Werkstattgebäude				
2.1.4	Büro- und Wohngebäude				
2.1.5	alleinige Nutzung				
2.1.6	Bewachung des Geländes/Gebäudes außerhalb der Betriebsstunden				
2.1.6.1	Wachpersonal				Zeiten:
2.1.6.1.1	extern				ADV Vereinbarung notwendig?
2.1.6.2	Bewegungsmelder				Erfasste Bereiche?
2.1.6.3	Gebäude-Alarmanlage				Aktive Zeit:
2.1.6.3.1	Verbindung zur Polizei				

2.1.6.3.2	Verbindung zur Feuerwehr				
2.1.6.3.3	Verbindung zu externem Wachdienst				
2.1.7	Videoüberwachung				Anforderungen in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“
2.1.7.1	Zeitraum				
2.1.7.2	Ort der Kameras				
2.1.7.3	Standort der Monitore				
2.1.7.4	Erfasste Bereiche				
2.1.7.5	Mit Aufzeichnung				Zugriffsregelung?
2.1.7.5.1	Aufbewahrungsdauer				
2.1.7.5.2	Aufbewahrungsort				
2.1.7.6	Betriebsvereinbarung vorhanden?				
2.2	**Lage der Räume**				
2.2.1	Serverräume abgegrenzt (Sperrbereich)?				
2.2.2	PC-Arbeitsplätze abgegrenzt?				
2.2.3	TK-Anlage abgegrenzt (Sperrbereich)?				
2.2.4	Netzverteiler abgegrenzt (Sperrbereich)?				
2.3	**Zutritt ausreichend abgesichert**				
2.3.1	Türen, Türschlösser				
2.3.2	Elektrische Türschlösser				
2.3.3	Lichtschächte				
2.3.4	Lüftungsöffnungen				
2.3.5	Fenster, Verglasungsart				
2.3.6	Rollos gegen Hochschieben gesichert				
2.3.7	Feuerleiter				
2.3.8	Feuertreppe				
2.4	**Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. –ende**				

2.4.1	Schlüsselregelung				
2.4.2	Quittierung der Schlüsselausgabe				
2.4.3	Generalschlüsselanlage?				
2.4.4	Aufbewahrung Generalschlüssel geregelt?				
2.5	**Überwachungseinrichtungen Räume**				
2.5.1	Alarmanlage				
2.5.2	Videoüberwachung				
2.5.2.1	Zeitraum				
2.5.2.2	Ort der Kameras				
2.5.2.3	Standort der Monitore				
2.5.2.4	Erfasste Bereiche				
2.5.2.5	Mit Aufzeichnung				Zugriffsregelung?
2.5.2.5.1	Aufbewahrungsdauer				
2.5.2.5.2	Aufbewahrungsort				
2.5.2.6	Betriebsvereinbarung vorhanden?				
2.6	**Schriftliche Festlegungen zur Zutrittsberechtigung**				
2.6.1	Generalschlüsselentnahme				
2.6.2	Ausweisregelungen				
2.6.3	Trennung von Bearbeitungs- und Publikumszonen				
2.6.4	Besucherregelungen				
2.6.5	Besucherbuch				Zugriffsregelung?
2.6.6	Kundenabfertigung (Schalterbetrieb)				
2.7	**Zutrittskontrollsystem**				
2.7.1	Ausweisleser				
2.7.2	Magnetkarte				
2.7.3	Transponderkarte				
2.7.4	Multifunktionale Kartennutzung				
2.8	**Kontrolle Reinigungs- und Wartungsarbeiten**				

2.9	**Anwesenheitskontrolle**				**Richtlinien/Vereinbarungen?**
2.9.1	Zeiterfassungssystem angeschlossen				
2.9.2	Stechuhren				
2.9.3	Schichtbuch				
2.9.4	Protokollierung				
2.10	**Zutrittskontrolle bei Tele-/Heimarbeitern geregelt?**				
2.11	**Beratung durch polizeiliche Beratungsstelle**				
2.12	**Beratung durch Feuerwehr?**				

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

Nr.	Vorgabe	erfüllt	nicht erfüllt	nicht erforderlich	Bemerkungen
3.1	**Passwortverfahren**				
3.1.1	Forderung einer unterschiedlichen Zeichenzusammensetzung				Groß- und Kleinschreibung, Zahlen, Sonderzeichen
3.1.2	Mindestlänge 8 Zeichen				besser: länger als 16 Zeichen (z.B. ein einfach zu merkender Satz)
3.1.3	Regelmäßiger Wechsel				
3.1.4	Erstanmeldeprozedur				Vergabe des ersten Passwortes durch wen? Aufforderung/Prüfung der Änderung
3.1.5	Bildschirmsperre bei Pausen mit Passwort-Aktivierung				
3.1.6	Zugangssperre bei mehr als 3 Anmeldeversuchen				Protokollierung fehlerhafter Anmeldeversuche? Auswertung wann durch wen?
3.1.7	Passworthistorie				
3.1.8	Verwendung Gruppen-Passwörter				Sollte aufgrund der Nachvollziehbarkeit von Zugriffen unbedingt vermieden werden
3.1.9	Richtlinie, Merkblatt				

3.1.10	Aufbewahrung Administrator-Passwörter				Zugriffsregelungen?
3.1.11	Einmal-Passwörter				Software-/Hardware-Token?
3.1.12	BIOS-Passwörter				
3.1.13	Boot-Passwörter				
3.1.14	Single-Sign-On (SSO)?				
3.2	**Andere Verfahren**				
3.2.1	Biometrische Verfahren (one-to-one)				
3.2.2	Biometrische Verfahren (one-to-many)				
3.2.3	Elektronische Signatur				
3.2.4	Chipkarten				PIN-Vergabe und -Änderung?
3.2.5	Magnetkarten				
3.2.6	Transponderkarten				
3.3	Protokollierung des Zugangs (An-/Abmeldung)				
3.4	Verschlüsselung mobiler Datenträger/Festplatten				
3.5	Zugang von außerhalb des Intranets				
3.6	**Wie erfolgt der Zugang ins Internet?**				
3.6.1	Kommunikationsserver				
3.6.2	Proxy-Server				
3.6.2.1	Vergabe der Accounts?				
3.6.2.2	Verwaltung der Passwörter?				
3.6.3	Wechsel des Betriebssystems				
3.6.4	Wechsel zu einem Live-Betriebssystem (read only)				
3.6.5	Stand-alone-PC				
3.6.6	Ohne Schließen der aktiven Anwendung				
3.7	**Welcher Internet-Provider wird genutzt?**				
3.7.1	Corporate Network				Wer?
3.7.2	Internet-Provider (direkt)				Wer?

3.7.3	Dienstleister (Hosting)				Wer?
3.8	**Verwendete Technik**				
3.8.1	ISDN				
3.8.1.1	Karte				
3.8.1.2	Modem				
3.8.1.3	Router				
3.8.2	DSL				
3.8.2.1	Karte				
3.8.2.2	Modem				
3.8.2.3	Router				
3.9	**Firewall**				
3.9.1	Betreuung durch Dienstleister				ADV Vereinbarung? SLA?
3.9.2	Zugriffsberechtigungskonzept				
3.9.3	Verantwortlich für Regelwerk				Wer darf Änderungen veranlassen?
3.9.3.1	Änderungsberechtigungen				Wodurch gewährleistet?
3.9.3.2	Nachvollziehbarkeit von Regeländerungen				Durch wen, wie oft?
3.9.3.3	Prüfung des Regelwerks				
3.9.4	Proxy-Server mit Software-Firewall				
3.9.5	Software-Firewall				
3.9.6	Hardware-Firewall (Appliance)				
3.9.7	Hersteller				
3.9.7.1	Support und Wartung (Fernwartung?)				Handhabung Support-Fall?
3.9.8	Wie oft werden Updates installiert?				Richtlinie/Vorgaben?
3.9.8.1	Laufend, automatisiertes Verfahren				Betriebssystem: ... Firewall: ...

3.9.8.2	Laufend, manuell				Betriebssystem: ... Firewall: ...
3.9.9	Wie werden Sicherheitslücken gehandhabt?				Vorgaben/Richtlinie?
3.9.9.1	Benachrichtigung durch wen?				z.B. CERT
3.9.9.1.1	Regelmäßig, automatisiertes Verfahren				
3.9.9.1.2	Regelmäßig, manuell				In welchen Fällen?
3.9.9.1.3	Manuell				In welchen Fällen?
3.9.9.2	Einspielung Sicherheitspatches				
3.9.9.2.1	Laufend, automatisiertes Verfahren				
3.9.9.2.2	Laufend, manuell				
3.9.10	Getrennte Administration der Komponenten?				Betriebssystem, Proxy, Firewall
3.10	**Welcher Browser wird genutzt?**				**Hersteller**
3.10.1	Wie oft werden Sicherheitspatches und/oder Updates installiert?				
3.10.1.1	Laufend, automatisiertes Verfahren				
3.10.1.2	Laufend, manuell				
3.10.2	Verwaltung der Konfiguration?				
3.10.2.1	Durch Administration				
3.10.2.2	Durch Nutzer				
3.11	**Werden Sicherheitseinstellungen durch Penetrationstests regelmäßig überprüft?**				**Wenn „Ja“, durch wen und wie häufig?**
3.12	**Systemadministration**				
3.12.1	Administrationsrichtlinie				
3.12.2	Administratoren sind tätig:				
3.12.2.1	hauptamtlich				
3.12.2.2	nebenamtlich				

3.12.2.3	extern				ADV Vereinbarung?
3.12.3	Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren				
3.12.4	Spezielle Passwortkonventionen zur Administration (abweichend von Nutzer-Passwörter)				
3.12.5	Getrennte Benutzerkonten für Systemadministration, Sachbearbeitung, persönlichen Nutzungen				
3.12.6	Anwendung des 4-Augen-Prinzips				
3.12.7	Protokollierung der Administrationsarbeit				
3.12.7.1	Protokoll-Server				Zugriffsregelungen?
3.12.7.2	Eigener Protokoll-Bereich				Wo?
3.12.7.3	Vorkehrungen gegen Protokollmanipulation				
3.12.7.4	Wer wertet Protokolle ggf. aus?				Anlassbezogen, regelmäßige Prüfung?
3.12.8	Sind Notfallpasswörter hinterlegt?				Wo? Zugriffsregelungen?

Zugriffskontrolle (Anlage Nr.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"

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
4.1	**Ausgestaltung des Berechtigungskonzeptes und der Zugriffsrechte**				
4.1.1	Schriftliches Berechtigungskonzept				
4.1.2	Programmtechnisches Berechtigungskonzept				
4.1.3	Rollendefinition				
4.1.4	Differenzierte Berechtigungen (Daten)				
4.1.5	Differenzierte Berechtigungen für Kenntnisnahme, Veränderung, Löschung				
4.1.6	Differenzierte Berechtigungen (Anwendungen)				
4.1.7	Differenzierte Berechtigungen (Betriebssystem)				
4.1.8	Protokollierung				

4.1.8.1	Verfahrensanweisung/Richtlinie				
4.1.8.2	Dateizugriffe				
4.1.8.3	Programmausführung				
4.1.8.4	Shell-Zugriff				Zugriff auf Dateisystemebene
4.1.8.5	Richtlinienverstoß				
4.1.8.6	Manuelle Protokollauswertung				Wie oft, durch wen?
4.1.8.7	Automatisierte Protokollauswertung				Wie oft, durch wen?
4.1.8.8	Aufbewahrung der Protokolle (max.1a)				
4.2	**Datenträger (DT)**				
4.2.1	Benennung eines Verantwortlichen				
4.2.2	Mobile DT - Art und Anzahl				
4.2.2.1	Festplatten				beweglich, nicht stationär eingebaut
4.2.2.2	USB-Sticks				Anzahl
4.2.2.3	SD-Karten				Anzahl
4.2.2.4	Disketten				Anzahl
4.2.2.5	Magnetbandkassetten				Anzahl
4.2.2.6	CD				Anzahl
4.2.2.7	DVD				Anzahl
4.2.3	Lagerung nach Dienstschluss				
4.2.3.1	Verfahrensanweisung/Richtlinie				
4.2.3.2	abschließbare Schränke				Sicherheits-, Schutzbedarfsstufe?
4.2.4	Auslagerung von Sicherungsdatenträgern				Wo?
4.3	**Datenträgerverwaltung**				
4.3.1	Nachweis über, Eingang, Ausgang sowie Bestand (Verzeichnisse)				
4.3.2	Datenträgerinventuren				
4.3.3	Festlegungen zur Datenträgerverwendung				
4.3.4	Abgrenzung der Bereiche, in denen sich DT befinden dürfen				

4.3.5	Festlegung der Personen, die DT befugt sind, DT zu entnehmen				
4.3.6	Festlegung der DT-Empfänger				
4.3.7	Quittierverfahren				
4.3.8	Datenträgerbegleitpapiere				
4.3.9	Äußerliche Kennzeichnung der eigenen DT zur Unterscheidung von fremden DT				
4.3.10	Trennung der DT verschiedener Auftraggeber				Mandanten, Verfahren
4.3.11	Eigener DT-Pool für jeden Kunden				Verfahren
4.3.12	Verbot des Einsatzes privater DT				Richtlinie, Dienstanweisung
4.3.13	Protokollierung der DT-Aussonderung				
4.4	**Datenträgervernichtung/-entsorgung**				
4.4.1	Richtlinien zur Entsorgung/Vernichtung von Fehldrucken und unbrauchbaren bzw. nicht mehr gebrauchten Datenträgern				
4.4.2	Datenschutzgerechte Löschung verwendeter DT vor neuer Verwendung bzw. Weitergabe				
4.4.3	Sichere Zwischenlagerung				
4.4.4	Einsatz von „Reißwolf“/Shredder				Schutzbedarfs-, Sicherheitsstufe
4.4.5	Einsatz von Datenträgerlöschgeräten oder -Software				Welche? Schutzbedarfs-, Sicherheitsstufe
4.4.6	Einsatz von Geräten zum Verbrennen/Zerstören				Welche? Schutzbedarfs-, Sicherheitsstufe
4.4.7	Kontrolle der ordnungsgemäßen Vernichtung				
4.4.8	Einsatz von Entsorgungsunternehmen				
4.4.8.1	Zuverlässiges Entsorgungsunternehmen ausgewählt?				Zertifizierungen? Kontrolle?
4.4.8.2	Vertragliche Regelung vorhanden				ADV Vereinbarung?
4.4.8.3	Entsorgungsbescheinigung, Löschprotokoll				
4.5	**Regelungen für das Kopieren von DT**				
4.5.1	Richtlinie vorhanden				
4.5.2	Sperrung der Laufwerke und Anschlüsse (USB, Diskette, CD/DVD ...)				Für jeden erfassten DT-Typ gesondert zu beachten
4.5.2.1	Mechanische Verriegelung				Disketten-/CD-Laufwerksschloss u.ä.

					Laufwerksverriegelung
4.5.2.2	Systemtechnische Einstellung				Wo? Wie geschützt? Konfiguration durch wen?
4.5.2.3	Einsatz spezieller Software				Welche? Installation, Konfiguration durch wen?
4.5.2.4	Weitere Schnittstellen, die Zugriff ermöglichen, gesperrt				
4.5.3	Kopierfunktion grundsätzlich deaktiviert				
4.5.4	Einsatz privilegierter Arbeitsplätze				
4.5.4.1	Wo?				Abteilung, Fachbereich
4.5.4.2	Zu welchem Zweck?				Verfahren
4.5.4.3	Wer hat Zugriff?				
4.5.4.4	Netzwerktechnische Anbindung				Stand-alone? Dedizierter Netzwerkbereich? Mit internem Netzwerk verbunden?
4.5.4.5	Besondere Sicherheitsmaßnahmen				Firewall, spezielle Zugriffs-/Nutzerkonten
4.6	**Taschenverbot bzw. -kontrollen**				
4.7	**Zugriffsschutz durch Bildschirmschoner**				
4.7.1	Automatische Sperre				
4.7.2	Sperre über Funktionstasten				
4.7.3	Ausschließlich passwortgestützte Aufhebung				
4.8	**Regelungen und Kontrolle von externer Wartung und Fernwartung**				
4.9	**Parasitäre Abstrahlung**				**elektromagnetische Abstrahlungen, Schallausbreitungen u.ä.**
4.9.1	Messungen durchgeführt				
4.9.2	Gegenmaßnahmen eingerichtet				

Weitergabekontrolle (Anlage Nr.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"

Nr.	Vorgabe	erfüllt	nicht erfüllt	nicht erforderlich	Bemerkungen
5.1	**Welche Datenträgertransporte finden statt?**				
5.1.1	Innerhalb des Unternehmens				
5.1.2	Zur Auslagerung				
5.1.3	Zwischen Auftraggeber/-nehmer				
5.1.4	Zu Dritten				
5.2	**Welche Versendungsarten (allgemein)?**				
5.2.1	Datenleitung				
5.2.2	E-Mail				
5.2.3	(S)FTP				
5.2.4	Post				
5.2.5	Bahn				
5.2.6	Kuriere				
5.2.7	Taxi				
5.2.8	Telefax				
5.3	**Welche Versendungsarten (DEÜV)?**				
5.3.1	Datenträgertransport				
5.3.2	Verschlüsselte Datenübertragung				
5.4	**Schriftliche Transportregelungen**				
5.4.1	zur Festlegung der Wege				
5.4.2	zu den Transportverfahren				
5.4.3	zu Datenempfängern				
5.4.4	zur Weitergabe Berechtigten				

5.4.5	zur Vollständigkeitsprüfung bei Rücklieferung vom Auftragnehmer				
5.5	**Transportsicherung**				
5.5.1	verschlossene Transportbehälter				
5.5.2	zuverlässige Boten / Transportunternehmen				Wer?
5.5.3	sichere Versendungsformen				
5.5.3.1	Wertpaket				
5.5.3.2	Einschreibesendungen				
5.5.3.3	Dateiverschlüsselung				
5.5.3.4	E-Mail-Verschlüsselung				Welcher Art?
5.5.3.5	Elektronische Signatur				
5.5.3.6	VPN				
5.5.3.7	Festplattenverschlüsselung (mobile Arbeitsgeräte)				
5.6	**Telefax-Regelungen**				
5.7	**Lieferscheine / Quittierverfahren bei Eingang und Ausgang von Datenträgern**				
5.7.1	Legitimation der Abholer				
5.7.2	Empfangsbestätigungen				
5.7.3	Ein-/Ausgangsbücher				
5.7.4	Lieferscheine				
5.7.5	Protokollierung				
5.8	**Vorgesehene Datenübermittlungen in den Verfahrensübersichten vermerkt?**				
5.9	Dokumentation der Abruf- und Übermittlungsprogramme				
5.10	Protokollierung der Übermittlung				
5.11	Regelungen für Tele- / Heimarbeiter?				
5.12	**Fernwartung**				**Wenn "Nein", entfallen nachfolgende Punkte**
5.12.1	Bestehen Zugriffsmöglichkeiten auf personenbezogene Daten?				Welche Datenkategorien?
5.12.2	ADV notwendig / vorhanden (§ 11 BDSG a.F.)				Bei Fernwartung durch Datenverarbeitung im Auftrag - Kontrolle des Auftragnehmers

					wie? Verschiedene Auftragnehmer in nachfolgenden Punkten benennen.
5.12.3	Wofür wird Fernwartung durchgeführt?				
5.12.3.1	Hardware				PC, Server
5.12.3.1.1	Netzwerk				
5.12.3.1.2	Firewall				
5.12.3.1.3	Festplattensysteme (SAN, NAS)				
5.12.3.1.4	Backupsysteme (Tape-Libraries)				
5.12.3.1.5	Andere				Welche?
5.12.3.2	Software				
5.12.3.2.1	Betriebssystem				Welche Systeme? Ergänzung zu Hardware
5.12.3.2.2	Firmware				Welche Systeme? Ergänzung zu Hardware
5.12.3.2.3	Anwendungen				unterstützende Anwendungen und Programme
5.12.3.2.4	Andere				Welche?
5.12.3.3	Benutzeradministration				
5.12.3.4	Helpdesk				
5.12.4	Umfang der Zugriffsrechte				
5.12.4.1	Allgemeine Benutzerrechte				
5.12.4.2	Administrationsrechte				
5.12.4.3	Shell-Kommando- / Dateisystem-Zugriff				
5.12.4.4	Andere Privilegien				Welche?
5.12.5	Zugangs-/Zugriffsweg				
5.12.5.1	permanent bestehende bzw. intern vorhandene Verbindung				z.B. internes Netzwerk
5.12.5.2	Internet				externe Netzwerkverbindungen
5.12.5.3	Standleitung				
5.12.5.4	ISDN				
5.12.5.5	Telefonnetz / Modem				

5.12.6	explizites Freischalten durch Auftraggeber				Nach welcher Vorgabe? Gruppenrollen? Spezifische, einzelne Nutzerkonten?
5.12.7	Verschlüsselung				
5.12.7.1	des (gesamten) Übertragungsweges				Wie?
5.12.7.2	ausnahmsweise zu übertragender Daten				Wie?
5.12.8	Zugangskontrolle				
5.12.8.1	Benutzerkennung / Passwort				
5.12.8.2	4-Augen-Prinzip (gesplittetes Passwort)				
5.12.8.3	Einmal-Passwort (Token)				
5.12.8.4	Automatischer Rückruf (RAS)				
5.12.8.5	Rufnummernidentifikation (ISDN)				
5.12.8.6	Beteiligte vorgelagerte Systeme				Firewall, Proxy
5.12.9	Monitoring der Fernwartungsaktivitäten				Wie?
5.12.10	Protokollierung der Fernwartung				Wie? Wo?
5.12.11	Protokollauswertung				Durch wen?
5.12.12	Regelungen zur Verwaltung und Konfiguration der Wartungszugriffe				
5.12.12.1	Freigabeverfahren				Beantragung wie? Genehmigung durch wen?
5.12.12.2	Prüfung der Berechtigungen				Ablauffristen, Erneuerungen

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

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
6.1	**Protokollierungs- und Protokollauswertungssysteme**				
6.1.1	Wer hat wann was eingegeben?				

6.1.2	Protokollierung bei Heimarbeitern				
6.1.3	Protokollauswertungsroutine?				
6.1.4	Wer hat Zugriffsrechte auf Protokolle bzw. Auswertungsroutine?				
6.1.5	Kennzeichnung der Belege oder Laufzettel mit Namenszeichen/Stempel				
6.1.6	Kennzeichnungen bei Online-Eingaben bzw. Änderungen				
6.1.7	Aufbewahrungsdauer der Protokolle fixiert				
6.2	**Dokumentation der Eingabeverfahren**				
6.2.1	Festlegung der Befugten für die Erstellung von Datenträgern (DT) und der Bearbeitung von Daten				
6.2.1.1	in Stellenbeschreibungen				
6.2.1.2	in Dienstanweisung				
6.2.1.3	im Geschäftsverteilungsplan				

Auftragskontrolle (Anlage Nr.6)
"zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können"

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
7.1	**Sorgfältige Auswahl der Auftragnehmer durch wen?**				
7.2	**Kriterien zur Auswahl der Auftragnehmer festgelegt**				
7.2.1	Referenzen				
7.2.2	Zertifizierungen / Gütesiegel				
7.2.3	Vorlage Datensicherheitskonzeption				
7.3	**Prüfung vor Auftragsvergabe durchgeführt und dokumentiert?**				
7.4	Unternehmen ist selbst als Auftragnehmer tätig				
7.5	**Detaillierte schriftliche Regelungen (Vertrag/Vereinbarung) der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmen, eindeutige Regelungen der Zuständigkeiten**				

	und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim DT-Transport)				
7.5.1	Datenerhebung				
7.5.2	Datenerfassung				
7.5.3	Datenverarbeitung				
7.5.4	Mikroverfilmung				
7.5.5	Datenträgerentsorgung				
7.5.6	Aktenvernichter				
7.5.7	Call-Center/Helpdesk				
7.5.8	Reinigungsfirma				
7.5.9	Wartung				
7.5.10	Prüfung				
7.6	**Formalisierte Auftragserteilung (Auftragsformular / Quittung)**				
7.7	**Auftragsdurchführung kontrolliert und dokumentiert?**				

Verfügbarkeitskontrolle (Anlage Nr.7)
"zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
8.1	**Brandschutzeinrichtungen**				
8.1.1	Feuerlöscher im Serverraum				
8.1.2	Feuerlöscher an/in den PC-Arbeitsräumen				
8.1.3	Rauch- oder Brandmelder				
8.1.4	Sprinkleranlage				
8.1.5	Feuerfeste Schränke				
8.1.6	Brandschutztüren, Brandschutzklappen				
8.1.7	Brandklasseneinteilung (Kennzeichnung besonders gefährdeter Räume)				

8.2	**Rauchverbot in Server- und PC-Arbeiträumen**				
8.3	**Wasserschutzeinrichtungen**				
8.4	**Stromversorgung**				
8.4.1	Unterbrechungsfreie Stromversorgung (USV)				
8.4.2	Motorgenerator				
8.4.3	Überspannungsschutzeinrichtungen				
8.5	**Klimaversorgung Serverraum**				
8.6	**Datensicherungsverfahren**				**Backup, Archivierung**
8.6.1	Datensicherungskonzept vorhanden				
8.6.2	Datenlöschkonzept bzw. -vorschrift vorhanden				
8.6.3	Sicherungen zur Sicherstellung eines ordnungsgemäßen Betriebes				Konfigurationen, vom Standard abweichende Einstellungen
8.6.3.1	Server				zentrale / dezentrale Betriebssystemeinstellungen
8.6.3.2	Netzwerkkomponenten				Konfigurationen
8.6.3.3	Datensicherung				Konfigurationen, Zeitpläne
8.6.3.4	SAN-Switche				Konfigurationen
8.6.3.5	andere Komponenten				Konfigurationen welcher Komponenten?
8.6.3.6	Benutzeradministration				Nutzerkonten, Zugriffsrechte
8.6.3.7	Konfigurations- und Softwaremanagement				
8.6.3.8	genutzte Programme				
8.6.3.9	Einzelrechner				stand-alone PC
8.6.3.10	Andere				
8.6.4	Sicherungen zur Sicherstellung einer ordnungsgemäßen Datenverarbeitung				Datenbestand
8.6.4.1	Datenbestand / -kategorien				
8.6.4.1.1	Trennung nach Verarbeitungszweck				
8.6.4.1.2	Trennung nach Aufbewahrungsfrist				
8.6.4.1.3	Trennung Datenträger				logische oder physische Trennung unterschiedlicher Sicherungen für

					unterschiedliche Verarbeitungen
8.6.5	Sicherungen für Datenschutzkontrollen oder Wartungs- und Prüfaufgaben				
8.6.5.1	Protokolle Zutrittsdaten				
8.6.5.2	Protokolle Zugangsdaten				
8.6.5.3	Protokolle Zugriffsdaten				
8.6.5.4	Protokolle von Daten zur Eingabekontrolle				
8.6.5.5	Fachliche Protokolle				anwendungs- und datenspezifisch
8.6.5.6	Technische Protokolle				Server etc.
8.6.5.7	Andere				Welche?
8.6.6	Datenarchivierung				
8.6.6.1	Archivierungskonzept vorhanden				
8.6.6.2	Maßnahmen zur Datensperrung vorhanden				
8.6.6.3	Räumlich getrennte Aufbewahrung von Datenträgern				z.B. zur Trennung von Sicherungen und zur Archivierungen
8.7	**Spiegeln der Festplatten (z.B. RAID)**				
8.7.1	lokale Server-Festplatten				
8.7.2	zentrale Festplattensysteme				
8.8	**Virenschutz**				
8.8.1	Werden mehrere Virenschutzprogramme genutzt?				
8.8.2	Schutzsoftware erkennt nur bekannte Schadsoftware				
8.8.3	Schutzsoftware erkennt unbekannte Schadsoftware (Heuristik)				
8.8.4	Schutzsoftware erkennt auch Schadsoftware in verschlüsselten Dateien				
8.8.5	Update der Schutzsoftware				
8.8.5.1	zentraler Update-Server				interner Server, der Updates verteilt
8.8.5.2	je Einzelplatz, Server				direktes Update über Verbindung zum Hersteller der Schutzsoftware
8.8.5.3	automatisch				wie häufig?
8.8.5.4	manuell per Abruf				wie häufig?

8.9	**Spammfilter**				
8.10	**Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)**				
8.11	**Havariearchiv**				**Auslagerung von DT**
8.12	**Notfallplan**				**Wiederanlaufplan**

Trennungskontrolle (Anlage Nr.8)
"zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können"

Nr.	Vorgabe	erfüllt	nicht erfüllt	nicht erforderlich	Bemerkungen
9.1	**Regelungen und Maßnahmen zur Sicherstellung der Trennung von Daten mit unterschiedlichen Vertrags- / Verarbeitungszwecken bei der**				
9.1.1	Speicherung				
9.1.2	Veränderung				
9.1.3	Löschung				
9.1.4	Übermittlung				
9.1.5	Sicherung				
9.2	**Interne Mandantenfähigkeit**				
9.3	**Interne Zweckbindung**				
9.4	**Interne Zugriffssicherung**				Abschottung
9.5	**Trennung der verarbeitenden Systeme**				im Backend: Server, Netzwerke, Software
9.5.1	Produktion				
9.5.2	Integration				
9.5.3	Test				
9.5.4	Entwicklung				
9.5.5	Arbeitsplätze und Server				Wie sind PC-Arbeitsplätze von der Serverlandschaft getrennt?
9.5.5.1	Firewall				

9.5.5.2	Unterschiedliche Subnetze				
9.5.5.3	Unterschiedliche Nutzerkonten				
9.6	**Trennung der verarbeitenden Systeme**				**im Frontend: Arbeitsplätze, Software**
9.6.1	Arbeitsplätze für Verarbeitung unterschiedlicher Daten				spezielle Einzelplätze?
9.6.2	Aufruf und Start von Programmen				z.B. Trennung zwischen der Verarbeitung von Produktions- und Testdaten
9.7	**Trennung der Nutzerkonten**				**unterschiedliche Nutzer der verarbeitenden Systeme**
9.7.1	Produktion				
9.7.2	Integration				
9.7.3	Test				
9.7.4	Entwicklung				
9.8	**Trennung Pseudonym- / Zuordnungsmerkmal**				
9.9	**Trennung besonders sensibler Daten**				

Internetauftritt (Anlage Nr.9)

Nr.	**Vorgabe**	**erfüllt**	**nicht erfüllt**	**nicht erforderlich**	**Bemerkungen**
10.1	**Telemediendienste-Anbieter?**				
10.2.	Umsetzung gesetzlicher Forderungen				
10.2.1	Anbieterkennzeichnung (§ 5 TMG)				
10.2.2	Kennzeichnung „kommerzielle Kommunikation“ (§ 6 Abs. 1 TMG)				
10.2.3	Kennzeichnung „kommerzielle Kommunikation“ bei E-Mail-Nachricht (§ 6 Abs. 2 TMG)				
10.2.4	Unterrichtung des Nutzers (Datenschutzerklärung) gem. § 13 Abs. 1 TMG				
10.2.5	Nutzungsprofile zu Werbe- und Marktforschungszwecken (§ 15 Abs. 3 i.V.m. § 13 Abs. 4 Nr. 6 TMG)				
10.2.6	Widerspruchsregelung gem. § 13 Abs. 3 TMG				
10.2.7	Pseudonymbehandlung gem. § 15 Abs. 3 TMG				Abschottung

10.2.8	Einwilligungsregelung zur Datenerhebung / -verarbeitung und -nutzung gem. § 12 TMG				
10.2.9	ProduktionElektronische Einwilligung gem. § 13 Abs. 2 TMG				
10.2.10	Anonyme bzw. pseudonymisierte Nutzungsmöglichkeit gem. § 13 Abs. 6 TMG				
10.2.11	Hinweis auf Weiterleitung an Dritte gem. § 13 Abs. 5 TMG				
10.2.12	Gewährleistung der Auskunftsrechte gem. § 13 Abs. 7 TMG				
10.3	**Arbeitnehmerbezogene Regelungen**				
10.3.1	Einwilligung zur Veröffentlichung von Bildern der Mitarbeiter				
10.3.2	Private Internet- / E-Mail-Nutzung erlaubt?				
10.3.3	Arbeits- / Verfahrensanweisung enthält				
10.3.3.1	Regelungen zu unerlaubten Handlungen				
10.3.3.2	Regelungen zur Protokollierung				
10.3.3.3	Regelungen zum Spamfiltereinsatz				
10.3.3.4	Regelungen zum Einsatz von Content-Filtern				
10.3.3.5	Vertreter-Regelungen (E-Mail)				
10.4	**Allgemeine Regeln zum E-Mail-Verkehr**				
10.4.1	"Nettiquette"-Regeln festgelegt?				
10.4.2	Vertraulichkeitsklausel (Confidential-Klausel)?				
10.4.3	Angaben zum Geschäftsbriefcharakter?				

Angaben unter Vorbehalt.
Diese grobe Strukturübersicht soll einen ersten Überblick geben, wie gut Sie mit Ihrem Unternehmen datenschutztechnisch aufgestellt sind. Je nach Unternehmen können sich Anforderungen und Umfang der Checkliste/Fragen ändern. Wir empfehlen daher eine unverbindliche Erstberatung, um alle wichtigen Punkte vorab zu klären.

Renovatio GmbH
Formerstraße 47
40878 Ratingen
+49 2102 85 00 160
info@renovatio.me
www.renovatio.me

Renovatio
Datenschutz & Managementsysteme