

Checkliste IT-Sicherheit & Datenschutz

Stand: 1.1.2021

IT-Sicherheit ist für moderne Unternehmen überlebensnotwendig – Hackerangriffe, IT-Ausfälle, Datenverluste etc. sind an der Tagesordnung und bedrohen ganz real kleine und mittlere Firmen.

Hinzu kommt seit Mai 2018 die **rechtliche Verpflichtung**, Daten mit dem aktuellen Stand der Technik zu schützen. Ein Backup, Virenschutz, starke Passwörter usw. sind somit rechtlich vorgeschrieben.

Die Umsetzung der DSGVO ist für mittlere Firmen aufwändig – führt jedoch zu einer deutlichen Steigerung der IT- und Datensicherheit – **ein echtes PLUS für Ihr Unternehmen.**

- ✓ Die Datenschutzgrundverordnung betrifft alle Firmen – egal welcher Größe
- ✓ Bei groben Verstößen droht die persönliche Haftung der Geschäftsführer
- ✓ Der Einsatz des aktuellen Stands der Technik ist somit gesetzlich vorgeschrieben. Zusätzlich drohen seit Mai 2018 Abmahnungen durch Mitbewerber oder Abmahnvereine.

Die folgende Checkliste beinhaltet die Anforderungen, die Unternehmen jeder Größe mindestens erfüllen müssen.

Je nach Größe, Art und Inhalt der Unternehmen gelten jedoch weitaus umfangreichere Vorschriften.

Allerdings ersetzt diese Checkliste keine individuelle Beratung – vor allem wenn Sie viele personenbezogenen Daten verarbeiten.

Inhalt:

1. Datensicherheit organisieren

Wie werden Daten bei Ihnen im Unternehmen verarbeitet und geschützt.
Datenschutzhandbuch organisieren

2. Verzeichnis der Verarbeitungstätigkeiten erstellen

3. Informationspflichten und Löschfristen organisieren

4. Prüfen und Abschließen von Auftragsdatenverarbeitungsverträgen

5. Bestellung eines Datenschutzbeauftragten, wenn mehr als 9 Personen
(Köpfe) Zugriff auf personenbezogene Daten haben.

6. Mitarbeiter verpflichten und schulen

7. Dokumentation

8. Datenschutzfolgeabschätzung prüfen

Physikalische Sicherheit und Zugangskontrolle		
1.1	Sie haben einen Einbruchsmelder/eine Alarmanlage	<input type="checkbox"/>
1.2	Sie haben einen Brandmelder	<input type="checkbox"/>
1.3	Die Stromversorgung ist gesichert (USV)	<input type="checkbox"/>
1.4	Sie haben einen kontrollierten Zugang für Kunden, Dienstleister, Mitarbeiter?	<input type="checkbox"/>
1.5	Ihr Zugang zu Telekommunikation und DSL ist stabil	<input type="checkbox"/>
1.6	Werden zu löschende Dokumente sicher verwahrt	<input type="checkbox"/>
1.7	Werden Dokumente rechtssicher entsorgt	<input type="checkbox"/>
1.8	Die vorherigen Punkte sind dokumentiert	<input type="checkbox"/>
Server		
2.1	Auf dem Server läuft ein aktuelles Betriebssystem Es werden automatisch alle Patches und Updates installiert	<input type="checkbox"/>
2.2	Unbenutzte Software wurde deinstalliert	<input type="checkbox"/>
2.3	Auf dem Server läuft eine Benutzerverwaltung	<input type="checkbox"/>
2.4	Konten von ehemaligen Usern sind deaktiviert	<input type="checkbox"/>
2.5	Die Funktionalität des Servers wird überwacht	<input type="checkbox"/>
2.6	Alte Geräte werden fachgerecht gelöscht/entsorgt	<input type="checkbox"/>
2.7	Die vorherigen Punkte sind dokumentiert	<input type="checkbox"/>
PC & Laptops / Clients		
3.1	Anwender melden sich an den Clients über die Benutzerverwaltung an	<input type="checkbox"/>
3.2	Die Passwörter haben eine ausreichende Länge und sind unterschiedlich	<input type="checkbox"/>
3.3	Die Passwörter müssen alle 90 Tage geändert werden	<input type="checkbox"/>
3.4	Wird der Client 5 Minuten nicht genutzt, so wird der Anwender abgemeldet	<input type="checkbox"/>
3.5	Auf den Clients läuft ein aktuelles Betriebssystem	<input type="checkbox"/>
3.6	Es werden automatisch alle Patches und Updates installiert	<input type="checkbox"/>
3.7	Es läuft immer ein aktueller Virenschanner	<input type="checkbox"/>
3.8	Es können keine USB-Geräte angeschlossen werden	<input type="checkbox"/>
3.9	Alte Geräte werden fachgerecht gelöscht/entsorgt	<input type="checkbox"/>
3.10	Die vorherigen Punkte sind dokumentiert	<input type="checkbox"/>

Smartphones, Tablets		
4.1	Es wird aktuelle Software genutzt	<input type="checkbox"/>
4.2	Passwortschutz wird genutzt	<input type="checkbox"/>
4.3	Nur notwendige Apps sind installiert	<input type="checkbox"/>
Netzwerk		
5.1	Ihr WLAN ist deaktiviert oder verschlüsselt	<input type="checkbox"/>
5.2	Gäste und Kunden nutzen Ihr Gast-WLAN, nicht das firmeninterne WLAN	<input type="checkbox"/>
5.3	Sie nutzen VPN	<input type="checkbox"/>
5.4	Sie nutzen eine Firewall	<input type="checkbox"/>
5.5	Die vorherigen Punkte sind dokumentiert	<input type="checkbox"/>
Backup		
6.1	Es gibt ein regelmäßiges Backup	<input type="checkbox"/>
6.2	Das Backup ist verfügbar	<input type="checkbox"/>
6.3	Das Backup ist gegen Diebstahl oder Brand gesichert	<input type="checkbox"/>
6.4	Rücksicherung ist möglich	<input type="checkbox"/>
6.5	Die vorherigen Punkte sind dokumentiert	<input type="checkbox"/>
Website/ Homepage		
7.1	Die Homepage wird per SSL verschlüsselt	<input type="checkbox"/>
7.2	Die Software erhält regelmäßige Updates	<input type="checkbox"/>
7.3	Das Webhostingpaket nutzt aktuelle Software	<input type="checkbox"/>
7.4	Zugangspasswörter werden regelmäßig gewechselt	<input type="checkbox"/>
7.5	Wird eine aktuelle Datenschutzerklärung verwendet	<input type="checkbox"/>
7.6	Genügt das Impressum der aktuellen Gesetzeslage	<input type="checkbox"/>
7.7	Sammeln Sie nur notwendige personenbezogene Daten und klären Sie den Besucher darüber auf	<input type="checkbox"/>
7.8	Google Analytics oder andere Analysesystem: Hier gelten verschärfte Vorschriften.	<input type="checkbox"/>
7.9	Cookie Hinweise: Einsatz muss geprüft werden	<input type="checkbox"/>
7.10	Newsletter-Anmeldung nur per Double-Opt-In	<input type="checkbox"/>
7.11	Google Webfonts vom eigenen Webserver laden	<input type="checkbox"/>

Emails		
8.1	Es wird ausschließlich die verschlüsselte Übertragungstechnik verwendet - STARTTLS oder SSL	<input type="checkbox"/>
8.2	Das Emailsysteem nutzt Antivirensoftware	<input type="checkbox"/>
8.3	Es gibt Verhaltensvorschriften für die Öffnung von Anhängen und Links	<input type="checkbox"/>
8.4	Sollten Massen-E-Mails versendet werden, so stehen die Empfänger im Feld „Blindkopie bcc“	<input type="checkbox"/>
Mitarbeiter		
9.1	Es gibt Verhaltensvorschriften für die Öffnung von Anhängen und Links aus Emails	<input type="checkbox"/>
9.2	Es gibt Verhaltensvorschriften für die Nutzung des Web und von Browsern	<input type="checkbox"/>
9.3	Jeder Mitarbeiter hat eigene Zugangsdaten	<input type="checkbox"/>
9.4	Mitarbeiter kennen die Gefahren und handeln umsichtig mit Daten	<input type="checkbox"/>
9.5	Zuständigkeiten sind geklärt und dokumentiert (Notfälle, Rücksicherungen, TK Anlage)	<input type="checkbox"/>
Notfall		
10.1	Es gibt eine Dokumentation aller Maßnahmen und Passwörter	<input type="checkbox"/>
10.2	Es gibt einen Maßnahmenplan für Notfälle	<input type="checkbox"/>
10.3	Wichtige Ansprechpartner und Adressen sind verzeichnet.	<input type="checkbox"/>

Personenbezogene Daten / Datenschutz		
11.1	<p>Bestandsaufnahme von personenbezogenen Daten:</p> <ol style="list-style-type: none"> 1. Verarbeitung von Kundendaten 2. Verarbeitung von Beschäftigtendaten 3. Verarbeitung von Kinder-Daten 4. Verarbeitung von Daten für Dritte als Auftragsverarbeiter 	<input type="checkbox"/>
11.2	<p>Zulässigkeit der Verarbeitung:</p> <p>Sie benötigen für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.</p>	<input type="checkbox"/>
11.3	<p>Betroffenenrechte und Informationspflichten</p> <ol style="list-style-type: none"> 1. Kontaktdaten des Datenschutzbeauftragten (falls vorhanden) 2. Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten 3. Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer 4. Hinweis auf Betroffenenrechte 5. Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Widerruf 6. der Einwilligung 7. Recht auf Beschwerde bei der Aufsichtsbehörde 8. Herkunft der Daten 9. Recht auf Auskunft 10. Recht auf Berichtigung 11. Recht auf fristgemäße Löschung der verarbeiteten Daten 12. Recht auf Einschränkung der Verarbeitung <p>Recht auf Datenübertragbarkeit</p>	<input type="checkbox"/>
11.4	Prüfen Sie, ob Sie einen Datenschutzbeauftragten benötigen	<input type="checkbox"/>
11.5	<p>Erstellen Sie eine Dokumentation über die Daten (Verfahrensverzeichnis):</p> <ul style="list-style-type: none"> - Wo fallen diese Daten an? - Wer verarbeitet die Daten? - Welche Daten fallen an? Zweckbestimmung! 	<input type="checkbox"/>

	<ul style="list-style-type: none"> - Wer hat Zugriff? - Beschreibung der Kategorien betroffener Personengruppen (Beschäftigte, Interessenten, Lieferanten, Kunden/Gäste, Beschäftigte von Kunden oder Lieferanten, Sonstige) - Beschreibung der diesbezüglichen Daten oder Datenkategorien (Beschäftigtendaten, Interessentendaten, Lieferantendaten, Kundendaten/Gastdaten, Beschäftigtendaten von Kunden oder Lieferanten, sonstige Daten) - Interne Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt sind oder werden (Abteilung, Person usw.) - Externe Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt sind oder werden (Firma, Name usw.) - Datenübermittlung in ein Drittland? Wenn ja, welches? - Wo werden die Daten gespeichert? - Wie können die Daten gelöscht werden 	
11.6	<p>Prüfen Sie Verträge mit anderen Unternehmen (so genannte Auftragsverarbeitungsverträge), bei denen personenbezogene Daten ausgetauscht werden:</p> <p>Allgemein:</p> <ul style="list-style-type: none"> - Liegt der Vertrag vor? - Gegenstand und Dauer des Auftrags - Art und Zweck der Verarbeitung - Art der Daten - Kategorien betroffener Personen - Technische und organisatorische Maßnahmen (TOMs) gem. Art 32 Abs. 1 DSGVO - Rechte des Verantwortlichen (Kontrollen) - Weisungsbefugnisse des Verantwortlichen 	<input type="checkbox"/>
11.7	<p>Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult.</p>	<input type="checkbox"/>
11.8	<p>Meldepflicht</p> <p>Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von</p>	<input type="checkbox"/>

	<p>Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DSGVO)?</p> <ul style="list-style-type: none"> - Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet? - Wer ist in Ihrem Unternehmen für die Meldung zuständig? 	
11.9	Prüfen Sie die Notwendigkeit einer Datenschutzfolgeabschätzung	<input type="checkbox"/>
11.10	<p>Dokumentation</p> <ul style="list-style-type: none"> - Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen? - Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist? 	<input type="checkbox"/>
11.11	Überprüfungszyklus einführen	

Die Begeisterung für die digitale Welt

treibt uns an - wir wollen Ihnen die Möglichkeiten der digitalen Welt eröffnen und Sie gleichzeitig vor den Gefahren schützen.

Wir beraten **mittelständische Unternehmen** im Nordwesten Deutschlands.

- **Datenschutz**
- **Stellung des Datenschutzbeauftragten**
- **IT-Sicherheitsaudit & -Beratung**
- **Mitarbeiterschulungen**
- **Begleitung von Digitalisierungsprojekten**

Die Preise für die Stellung des Datenschutzbeauftragten beginnen bei 150,- pro Monat inkl. aller notwendigen Leistungen. Die Preisliste finden Sie hier:
<https://www.i-wid.com/101-202-303>

go digital Förderung

Wir sind autorisiertes Beratungsunternehmen des Förderprogrammes "go-digital". Kleine und mittlere Unternehmen erhalten hier Zuschüsse (bis zu 50%) zu Beratungsleistungen aus den Bereichen:

- IT-Sicherheit
- Digitale Markterschließung
- Digitalisierte Geschäftsprozesse

Weitere Infos finden Sie unter <http://www.bmwi-go-digital.de/>