IT Sicherheit und Datenschutz - für kleine und mittelständische Unternehmen

Schutz gegen Abmahnungen, Strafen und Ausfälle

Ein praktischer Leitfaden für die zwingenden Anforderungen der DSGVO an Unternehmen jeder Größe

Veröffentlicht von

Dipl. Inform. Thorsten Brendel
ViCoTec Internetsysteme GmbH & Co. KG

Stand: 19.6.2018

IT Sicherheit und Datenschutz

Checkliste IT-Sicherheit und DSGVO

Oft wird einem die Wichtigkeit der IT-Sicherheit erst bewusst, wenn ein Schaden entstanden ist. Jedoch sind IT-System heutzutage Lebensadern von kleinen und großen Unternehmen. Ein Ausfall kann teuer werden – bis hin zur Insolvenz.

Hinzu kommt, dass personenbezogene Daten einem besonderen gesetzlichen Schutz unterliegen. Dieser wird ab dem 25. Mai 2018 mit der europäischen Datenschutzgrundverordnung geregelt.

Datenschutzbehörden können bei Verstößen gegen geltende Verordnungen Geldbußen von bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist, festsetzen. Dazu können Schadensersatzforderungen von Geschädigten kommen.

- ✓ Die Datenschutzgrundverordnung betrifft auch kleine Unternehmen maßgeblich.
- ✓ Bei groben Verstößen droht die persönliche Haftung der Geschäftsführer
- ✓ Schutzmaßnahmen sind daher zwingend. Zusätzlich drohen ab Mai 2018 Abmahnungen durch Mitbewerber oder Abmahnvereine.

Die folgende Checkliste beinhaltet die minimalen 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.

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

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

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

Personenbezogene Daten / Datenschutz

11.1	**Bestandsaufnahme von personenbezogenen Daten:** 1. Verarbeitung von Kundendaten 2. Verarbeitung von Beschäftigtendaten 3. Verarbeitung von Kinder-Daten 4. Verarbeitung von Daten für Dritte als Auftragsverarbeiter	☐
11.2	**Zulässigkeit der Verarbeitung:** Sie benötigen für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.	☐

11.3	**Betroffenenrechte und Informationspflichten** 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 Recht auf Datenübertragbarkeit	☐
11.4	Prüfen Sie, ob Sie einen **Datenschutzbeauftragen** brauchen	☐
11.5	**Erstellen Sie eine Dokumentation über die Daten (Verfahrensverzeichnis):** - Wo fallen diese Daten an? - Wer verarbeitet die Daten? - Welche Daten fallen an? Zweckbestimmung! - 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	**Prüfen Sie Verträge mit anderen Unternehmen** (so genannte Auftragsverarbeitungsverträge), bei denen personenbezogene Daten ausgetauscht werden: Allgemein: - 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	☐
11.7	**Mitarbeiter sind im Umgang mit personenbezogenen Daten geschult**.	☐
11.8	**Meldepflicht** Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)? - 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**	☐
11.10	**Dokumentation** - Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen? - Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?	☐
11.11	**Überprüfungszyklus einführen**	

Quellen und weiterführende Informationen

1. Broschüre Datenschutz von der IHK: https://www.i-wid.com/101-202-302
2. „Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine“ Bayrisches Landesamt für Datenschutzaufsicht
3. www.erecht24.de
4. Landesbeauftragte für den Datenschutz Niedersachsen: www.lfd.niedersachsen.de
5. ZDH Leitfaden: Das neue Datenschutzrecht: https://www.i-wid.com/101-202-301
6. Diese Checkliste: https://www.i-wid.com/101-202-300
7. Preise und Leistungen von ViCoTec: https://www.i-wid.com/101-202-303

Abmahnwarner und Newsletter

- Warnungen zu Abmahnwellen und Verhaltensvorschläge
- Aktuelle Entwicklungen & Urteile
- Aktualisierte Checklisten
- Hinweise über spezielle Schulungen für KMU

Einfach unter **https://www.vicotec.de/datenschutz.html** in unseren Newsletter Verteiler eintragen

Wir nehmen Ihnen das Thema IT-Sicherheit und Datenschutz ab

– soweit und so viel, wie Sie das möchten

In Zusammenarbeit mit dem IT-Systemhaus Syntax aus Oldenburg bieten wir Ihnen unterschiedliche Lösungsmöglichkeiten.

Datenschutz:

1. Beratung, Umsetzung, Überwachung und Dokumentation der DSGVO in Ihrem Unternehmen – passend zu Ihrem Bedarf.
2. Stellung eines externen Datenschutzbeauftragten (bei Bedarf)

IT-Sicherheit

Beratung, Umsetzung, Überwachung und Dokumentation von IT-Sicherheitsmaßnahmen in Ihrem Unternehmen – passend zu Ihrem Bedarf.

Internet-Sicherheit und -Datenschutz

1. Überwachung Ihrer Website / Onlineshops
2. Beratung zu Datenschutz- und IT-Sicherheitsthemen
3. Umsetzung wichtiger Maßnahmen (Datenschutzerklärung, Impressum, SSL, …)
-