CHECKLISTE

DSGVO-Checkliste für die IT- und Software-Branche

DATENSCHUTZ EXPERTE.DE
Ein Service der Proliance GmbH

So komplex und aufwendig das Thema Datenschutz auf den ersten Blick wirkt – mit Unterstützung von Experten stellen Sie Ihre IT-Prozesse im Handumdrehen DSGVO-konform auf. Ob aus wettbewerbsrechtlicher Sicht, oder um das Vertrauen Ihrer Kunden zu stärken: Die folgende Checkliste für IT-Unternehmen zeigt, wie Sie den Anforderungen der DSGVO in nur 7 Schritten gerecht werden.

1. Lagern Sie den Datenschutz an einen Datenschutzbeauftragten aus

Worum geht es? Datenschutzbeauftragte sorgen in Unternehmen dafür, dass die Daten von Kunden und Mitarbeitern sicher und rechtmäßig behandelt werden.

Sie sind IT-Verantwortlicher in einem Startup und glauben, Ihr Unternehmen wäre zu klein für einen Datenschutzbeauftragten? Das ist ein Irrtum: Es genügt bereits, wenn 20 Personen bei Ihnen mit der Verarbeitung von Daten beschäftigt sind – Freelancer, Teilzeitkräfte, Werkstudenten und Praktikanten inbegriffen.

Achtung: Wenn Ihr Team mit besonders sensiblen Daten arbeitet (das ist zum Beispiel bei Health-Startups der Fall), gewerbsmäßig mit Daten handelt oder Daten im Rahmen der Markt- und Meinungsforschung verwendet, entfällt die 20-Personen-Grenze. Die Bestellung eines Datenschutzbeauftragten ist dann unabhängig von der Mitarbeiterzahl auf jeden Fall erforderlich.

Intern oder extern?

Sie haben die Wahl, ob Sie einen internen oder externen Datenschutzbeauftragten bestellen. Ihre Entscheidung ist von verschiedenen Faktoren abhängig. Für die meisten kleinen IT-Unternehmen ist ein externer Datenschutz-beauftragter die bessere Wahl: Sie vermeiden damit Interessenskonflikte und holen sich ohne Aufwand geballtes Datenschutzwissen ins Unternehmen.

Sie sind unsicher, welche Variante die beste ist?

Tipp: Sparen Sie Zeit mit unserer Entscheidungshilfe.

2. Implementieren Sie ein Verzeichnis von Verarbeitungstätigkeiten

Worum geht es? Die DSGVO verpflichtet Unternehmen dazu, sämtliche regelmäßig stattfindenden Datenverarbeitungsprozesse in einem Verzeichnis von Verarbeitungstätigkeiten (VVT) zu dokumentieren.

Beispiele für solche Prozesse sind:

- Nutzung von Content-Management-Systemen, die personenbezogene Daten enthalten
- Versand von Werbe-E-Mails
- Veröffentlichen von Teamfotos auf der Website des Unternehmens
- Speichern von IP- oder MAC-Adressen
- Lohnbuchhaltung

Unter anderem gehören folgende Angaben in ein VVT:

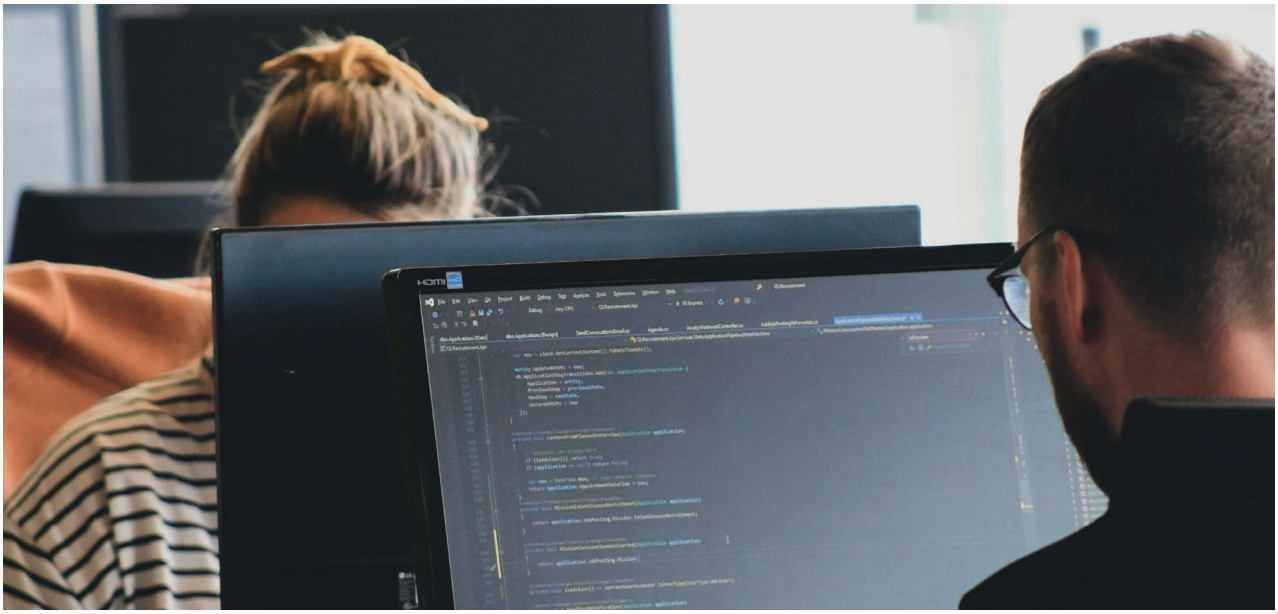
- ✔ Name und Kontaktdaten des Verantwortlichen
- ✔ Zweck der Verarbeitung der Daten
- ✔ Datenkategorien
- ✔ Auflistung der Betroffenen nach Kategorien
- ✔ Auflistung aller Datenempfänger/ zur Einsicht befugten Personen (oder Kategorien von Empfängern sowie Drittlandempfänger)
- ✔ Getroffene technische und organisatorische Maßnahmen (TOM, siehe Schritt 3)
- ✔ Löschfristen

Verantwortlich dafür, dass es ein solches Verzeichnis gibt, ist in der Regel die Geschäftsleitung. Diese ist auf die Mitarbeit der einzelnen Teams angewiesen, die aufführen müssen, welche Daten sie wie nutzen. Ihr Datenschutzbeauftragter informiert Sie darüber, wie detailliert dieses Verzeichnis sein muss und welche Informationen nicht fehlen dürfen.

Tipp: Auf unserer Website finden Sie ein kostenloses VVT-Muster.

3. Ergreifen Sie technische und organisatorische Maßnahmen (TOM)

Worum geht es? IT-Unternehmen müssen eine Vielzahl von technischen und organisatorischen Maßnahmen (TOM) ergreifen und dokumentieren, um den DSGVO-Anforderungen gerecht zu werden.



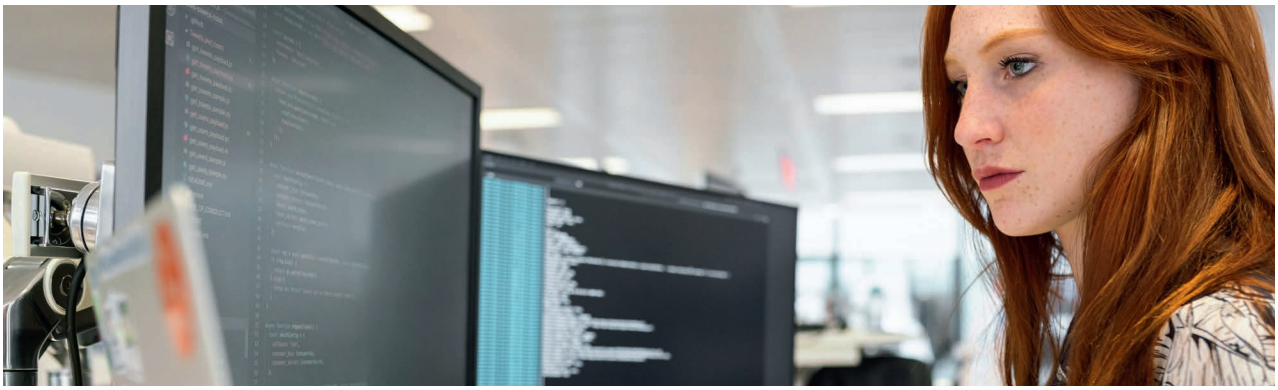
Konkret geht es um die Kontrolle der folgenden Aspekte:

- Zutritt zu den Räumlichkeiten des Unternehmens
- Zugang zu Datenverarbeitungssystemen
- Zugriff auf Daten und Verarbeitungsprozesse
- DSGVO-konforme Weitergabe von Daten
- Datenverwaltung und -pflege
- Daten, die für die Auftragsabwicklung notwendig sind
- Verfügbarkeit der Daten durch Backups, Virenschutz etc.
- Getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden

4. Führen Sie eine Datenschutz-Folgeabschätzung durch

Worum geht es? Bei diesem Punkt geht es darum, das Risiko für die Rechte und Freiheiten von natürlichen Personen abzuschätzen, das mit der Datenverarbeitung in Ihrem Unternehmen einhergeht.

In der Regel führt Ihr Datenschutzbeauftragter die Datenschutz-Folgeabschätzung für Ihr Unternehmen durch. Es besteht keine Pflicht, die Ergebnisse zu veröffentlichen.



5. Sichern Sie die Rechte Betroffener ab

Worum geht es? Was die Verarbeitung ihrer Daten angeht, haben EU-Bürger seit Einführung der DSGVO eine enorme Stärkung ihrer Rechte erfahren. Verantwortliche in IT- und anderen datenverarbeitenden Unternehmen haben die Pflicht, diese Rechte zu erfüllen.

Das bedeutet zum einen, sicherzustellen, dass die Verarbeitung von Daten ausschließlich auf einer entsprechenden Rechtsgrundlage erfolgt. Zum anderen müssen Unternehmen die Betroffenen nach Art. 13 bzw. 14 DSGVO darüber informieren, wie und zu welchem Zweck ihre Daten genutzt werden.

Außerdem zählen folgende Regelungen der DSGVO dazu:

- Recht auf Auskunft nach Art. 15
- Recht auf Berichtigung nach Art. 16
- Recht auf Löschung nach Art. 17
- Recht auf Einschränkung der Verarbeitung nach Art. 18
- Recht auf Mitteilung nach Art. 19
- Recht auf Datenübertragbarkeit nach Art. 20
- Widerspruchsrecht nach Art. 21
- Recht auf Widerruf der erteilten Einwilligung nach Art. 7

6. Schließen Sie Auftragsverarbeitungs-verträge mit Ihren Dienstleistern ab

Worum geht es? Im IT-Bereich arbeiten vor allem junge Unternehmen bei der Datenverarbeitung häufig mit Dienstleistern zusammenarbeiten – sei es durch den Einsatz von Software-as-a-Service-Lösungen (SaaS), KI-Tools oder durch die Nutzung von Cloud-Anbietern.

Damit Unternehmensdaten auch in der Zusammenarbeit mit Externen sicher bleiben, müssen Sie entsprechende Verträge mit diesen externen Dienstleistern abschließen.

> **Wichtig:** Nur wenn ein gültiger Auftragsverarbeitungsvertrag (AVV) vorliegt, kann die Weitergabe von Daten an weisungsgebundene Dienstleister DSGVO-konform sein.

7. Setzen Sie auf fachliches Know-how von Datenschutzexperten

Worum geht es? Unternehmen im IT-Bereich haben oft ambitionierte Pläne, unterliegen jedoch wie vielen Branchen einem hohen Kosten- und Wettbewerbsdruck. Am Budget für den Datenschutz sollten Sie allerdings auf keinen Fall sparen. Spätestens seit Einführung der DSGVO ist der rechtskonforme Umgang mit Daten extrem wichtig und sollte keineswegs vernachlässigt werden – selbst wenn Ihr IT-Unternehmen noch am Anfang steht.

Sie möchten Ihre Ressourcen schonen und Ihr Unternehmen gleichzeitig vor DSGVO-Bußgeldern schützen? Dann setzen Sie auf einen externen Datenschutzbeauftragten mit IT-spezifischem Fachwissen. Dieser berät Sie in allen Fragen rund um den Datenschutz für Ihr IT-Unternehmen und stellt sicher, dass Ihr Team und Ihre Prozesse in puncto DSGVO gut aufgestellt sind.

Datenschutz ist ein komplexes Thema, und diese Checkliste kann keine individuelle Beratung durch einen Experten ersetzen. Vielmehr soll sie jungen oder etablierten IT-Unternehmen den Einstieg in das Thema DSGVO erleichtern.

Sie haben Fragen?
Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung zu Datenschutzsoftware in Ihrem Unternehmen und dem Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de

Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist Ihr Partner im Datenschutz.
Wir glauben, dass Datenschutz nicht teuer und komplex sein muss. Mit unseren auf KMU zugeschnittenen Lösungen beraten wir Sie als externer Datenschutzbeauftragter. Alternativ unterstützen wir sowohl interne oder externe Datenschutzbeauftragte mit unserer smarten SaaS-Plattform Proliance 360. So lässt sich Datenschutz einfach & pragmatisch umsetzen. Wir sind ein junges Münchner Unternehmen mit mehr als 70 Mitarbeitern und helfen bereits über 2.000 Unternehmen, die Herausforderungen der DSGVO zu meistern. Sprechen Sie uns gerne an.