Anforderungen der Datenschutzgrundverordnung
an kleine Unternehmen, Vereine etc.

ID	Thema		trifft zu?
01.	Datenschutzbeauftragter (DSB)	Muss ein DSB benannt werden?	prüfen
02.	Verzeichnis von Verarbeitungstätigkeiten	Ist ein solches Verzeichnis erforderlich?	ja
03.	Sicherheit (setzt eine Erfassung der IT-Infrastruktur voraus)	Müssen die Daten besonders gesichert werden oder reichen etablierte Standartmaßnahmen aus?	prüfen
04.	Auftragsverarbeitung	Ist ein Vertrag zur Auftragsverarbeitung notwendig?	prüfen
05.	Informations- und Auskunftspflicht (Betroffenenrechte)	Bestehen irgendwelche Informationspflichten?	ja
06.	Speicherung und Löschen von Daten (Empfehlung: Löschkonzept)	Gibt es besondere Anforderung zur Datenlöschung?	prüfen
07.	Melde und Benachrichtigungspflicht (Datenschutzverletzungen)	Müssen bestimmte Vorfälle gemeldet werden?	ja
08.	Risikoanalyse / -bewertung / Folgenabschätzung (DSFA)	Muss eine DSFA durchgeführt werden?	prüfen
09.	Homeoffice (Telearbeitsplätze)	Gibt es Mitarbeiter die im Homeoffice arbeiten?	prüfen
10.	Regelungen zum Umgang mit mobilen Endgeräten	Sind Nutzungsvereinbarungen vorhanden?	prüfen
11.	Videoüberwachung (VÜ)	Praktizieren Sie in Ihrem Unternehmen Videoüberwachungen?	prüfen
12.	Einwilligungspflicht (z. B. für Bilder / Videos)	Sind Einwilligungen notwendig?	prüfen
13.	Website und Social-Media	Sind Websites und Social-Media-Kanäle vorhanden?	meist ja
14.	Sicherer E-Mail-Versand	Ist der sichere Versand mit personenbezogenen Daten geregelt?	prüfen
15.	Datenschutz-Verpflichtung von Beschäftigten	Ist eine solche Verpflichtung durchzuführen?	ja
16.	DV für Zwecke des Beschäftigungsverhältnisses *(von der Bewerbung bis zum Austritt des Beschäftigten)*	Gibt es Regelungen im Umgang mit Bewerber- und Mitarbeiterdaten?	prüfen
	Es sind evtl. noch viele weitere Punkte zu prüfen und zu berücksichtigen.	*z. B. Datenschutz in der Werbung, IT-Sicherheitskonzept*	prüfen

Bemerkung /weitere Themen:

Erläuterungen zu den Anforderungen

1. Datenschutzbeauftragter (DSB)

In aller Regel ist nur dann ein DSB zu benennen, wenn mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.
„Ständig beschäftigt“ ist, wer z. B. permanent Kunden- oder Personalverwaltung macht. „Nicht“ dagegen, wer z. B. als Handwerker oder Produktionsmitarbeiter nur mit Namen und Adressen von Kunden umgeht.
Der Verantwortliche und der Auftragsverarbeiter haben sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

2. Verzeichnis von Verarbeitungstätigkeiten (VV)

Kleine Unternehmen gehen regelmäßig mit Kunden- und Mitarbeiterdaten um und müssen ein – vom Umfang her überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.
(Dem Verzeichnis von Verarbeitungstätigkeiten sind die Technischen und Organisatorischen Maßnahmen beizufügen.)

3. Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virenscanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.
Hinweis: Eine gute Sicherheit setzt eine Erfassung der IT-Infrastruktur voraus, und ist ebenfalls der Grundstein für die Technischen und Organisatorischen Maßnahmen.

4. Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.
(z. B. externes Lohnbüro, ext. IT-Support, ext. Rechenzentren, evtl. Hosting-Anbieter)
Hinweis: Erstellen Sie eine Liste externer Dienstleister und eingesetzter Software (auch Apps).

5. Informations- und Auskunftspflichten (Transparenzpflicht des Unternehmens)

Jedes Unternehmen hat die betroffenen Personen (d.h. insbesondere Kunden und Mitarbeiter) schon bei der ersten Datenerhebung über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

<u>Benachrichtigungspflicht des Unternehmens:</u>
Wenn Daten über die betroffene Person von Dritten oder aus öffentlichen Quellen erhoben worden sind, ist die betroffene Person auf den gleichen Informationsstand zu bringen, als wenn Daten bei ihr erhoben worden sind.

(Zu beachten ist die hier auch die Erhebung von p. b. Daten über Websites, Apps usw.)

6. Speicherung und Löschen von Daten

Sobald keine gesetzliche Grundlage (z.B. steuerliche oder handelsrechtliche Aufbewahrungspflicht) für die Speicherung von personenbezogenen Daten mehr besteht, sind diese zu löschen. Dies ist z.B. der Fall, wenn ein Kunde mehrere Jahre lang keine neuen Aufträge mehr erteilt hat. Hinweis: Erstellung eines Löschkonzeptes!

7. Melde und Benachrichtigungspflicht (Datenschutzverletzungen)

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall - innerhalb von 72 Stunden - darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

8. Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

9. Homeoffice

Auch im Homeoffice muss ein hinreichender Schutz von personenbezogenen Daten gewährleistet sein, sofern der Mitarbeiter mit diesen im Rahmen seiner Tätigkeit zu tun hat.
Hinweis: Es gelten die gleichen Datenschutzregelungen wie im Unternehmen selbst.

10. Regelung zum Umgang mit mobilen Endgeräten

Erstellen Sie eine Nutzungs- /oder Dienstanweisung, in der der Umgang mit den mobilen Endgeräten Ihres Unternehmens geregelt ist (Notebooks, Tablets, Smartphones).
Hinweis: Nutzungsanweisungen sind sehr hilfreich, um meldepflichtige Datenschutzvorfälle zu vermeiden!

11. Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoaufnahmen zu informieren.
Hinweis! Zu beachten sind die Regelungen des Art. 6 Abs. 1 lit. f DSGVO zum berechtigten Interesse des Verantwortlichen in Abwägung gegen die Rechte und Freiheiten der betroffenen Personen.

12. Einwilligungspflicht

Personenbezogene Daten dürfen nur unter dem Vorbehalt einer Rechtsgrundlage oder einer Einwilligung verarbeitet werden.
Das heißt: Das Vorliegen einer Rechtsgrundlage prüfen! Wenn keine Rechtsgrundlage vorliegt, muss eine Einwilligung des Betroffenen eingeholt werden.

13. Website, Social Media (z.B. Facebook, Twitter usw.) sowie Mail-Versand

Sobald Verantwortliche eine Website oder Social-Media-Kanäle betreiben, ist der Datenschutz zu berücksichtigen.

14. Mail-Versand

Personenbezogene Daten (insbesondere besonders schützenswerte Daten) niemals unverschlüsselt versenden!

15. Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO erfolgt.

Hinweise:

- Vertraulichkeitsverpflichtung für Mitarbeiter
- regelmäßige Schulungen der Mitarbeiter

16. Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

Zu berücksichtigen sind unter anderem:

- Erhebung und Speicherung von Bewerberdaten
- Erhebung, Verarbeitung und Nutzung von Mitarbeiterdaten (Personaldaten – z. B. Personalfragebogen)
- Die Grundsätze zum Führen der Personalakte (Vertraulichkeit, Richtigkeit und Vollständigkeit, Zulässigkeit und Zweckbindung, Transparenz, BEM)
- Beendigung des Beschäftigungsverhältnisses
- Datenschutz und Betriebsrat
- u. s. w.

Achtung: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ist ein sehr umfangreicher Prozess. Die hier aufgeführten Punkte geben nur ein paar wenige Einblicke, worauf unbedingt zu achten ist!