Maßnahmenplan zur Umsetzung des Datenschutzes gemäß Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSG) im Unternehmen

Vorgehen zur effizienten Implementierung des Datenschutzes im Unternehmen:

- Wer ist der Ansprechpartner des Datenschutzbeauftragten im Unternehmen? Gibt es einen einzelnen Datenschutzkoordinator oder ein Datenschutz-Team?
- Hat das Unternehmen sämtliche verfügbaren Ressourcen zur Umsetzung zur Verfügung gestellt?
- Sind im Unternehmen bereits Unterlagen zum Thema Datenschutz vorhanden? Entsprechen diese der aktuellen Rechtslage?

Was ist zu tun?

1. Sind alle **Informationspflichten nach Art. 13 DS-GVO** erfüllt?
   Erläuterung: Alle Personen, bei denen das Unternehmen Daten verarbeitet (z.B. Beschäftigte im weitesten Sinne des §26 BDSG, Vertragspartner und dortige Ansprechpartner, aber auch Besucher der Homepage) müssen darüber informiert werden, wie ihre Daten verarbeitet werden. Dies ist zum Beispiel über die Ausgabe oder digitale Bereitstellung von Dokumenten möglich.

2. Welche **Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten** bestehen?
   Erläuterung: In allen Abteilungen müssen die bestehenden Verarbeitungstätigkeiten erörtert und dokumentiert werden. Hierzu gehört insbesondere auch die Videoüberwachung mit genauer Dokumentation der Kameras und des Aufnahmebereiches oder der Versand von Newslettern. Alle Tätigkeiten müssen dann in Verzeichnis von Verarbeitungstätigkeiten (VVT) abgelegt werden.

3. Bestehen Verarbeitungstätigkeiten, die durch die technische Verarbeitung, das Handling an sich oder die Datenkategorie besondere Risiken schaffen und deshalb einer **Datenschutzfolgenabschätzung** (DSFA) bedürfen?
   Erläuterung: Zur Risikobewertung sowie zur Erörterung von Abhilfemaßnahmen führt die verantwortliche Stelle in Zusammenarbeit mit dem Datenschutzbeauftragten eine dokumentierte Datenschutzfolgenabschätzung durch.

4. Gibt es einen **Betriebsrat** im Unternehmen? Hat der Betriebsrat Betriebsvereinbarungen mit der Geschäftsleitung abgeschlossen, die personenbezogene Daten von Beschäftigten betreffen? Zum Beispiel: Betriebsvereinbarungen zu Zutrittsdokumentation, Arbeitszeitdokumentation, Videoüberwachung, GPS-Überwachung von Beschäftigten oder Fahrzeugen. Wurde der Betriebsrat im Umgang mit seinen eigenen Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten geschult?

5. Besteht eine interne **Anweisung zum Datenschutz**, damit sich Beschäftigte jederzeit eigenständig informieren können? Zum Beispiel als Teil eines Firmenglossars oder auch als Teil eines Welcome-Packages im Zuge der Einstellung.

6. Sind **Auftragsverarbeitungsverträge** (AVV) mit Dienstleistern geschlossen worden, die personenbezogene Daten im Auftrag verarbeiten? Sind zumindest Verschwiegenheitsvereinbarung-en geschlossen wurden, sofern keine Notwendigkeit zum Abschluss eines AVV bestand? Liegt eine Liste aller Auftragsverarbeiter des Unternehmens vor?

7. Wird das Unternehmen selbst als Auftragsverarbeiter tätig und sind diese Verarbeitungstätigkeiten in einem eigenen **Verzeichnis der Verarbeitungstätigkeiten für Auftragsverarbeiter** (VVT-AV) dokumentiert?

8. Sind die **räumlichen Gegebenheiten** den Anforderungen des Datenschutzes angepasst? Wo stehen die Drucker? Kann von außen Sicht auf Monitore genommen werden? Wo ist der Serverraum und wie ist dieser abgesichert?

9. Ist dokumentiert, wie das Unternehmen mit **Datenpannen** umgeht? Werden Datenpannen überhaupt gemeldet? Ist eindeutig geklärt, was eine Datenpanne ist? Wer bekommt wie schnell Kenntnis darüber? Kann die 72-Stunden-Meldefrist ab Kenntnis eingehalten werden? Sofern externe Dienstleister für IT verpflichtet wurden: Sind IT-forensische Maßnahmen oder zeitkritische Maßnahmen im Vertrag definiert? Ist dieser gesamte Prozess niedergeschrieben und zugänglich für die entsprechenden Personen?

10. Ist dokumentiert, wie das Unternehmen mit **Auskunftsersuchen** nach Art. 15 DS-GVO und anderen **Betroffenenrechten** umgeht? Ist geklärt und bewusst, was Betroffenenrechte sind? Sind diese Prozesse niedergeschrieben und den entsprechenden Personen zugänglich gemacht?

11. Ist geklärt, wie das Unternehmen mit **Anfragen der Aufsichtsbehörde** umgeht? Ist dieser Prozess niedergeschrieben?

12. Hat das Unternehmen **technische und organisatorische Maßnahmen** (TOM) für das eigenen Sicherheitsniveau niedergeschrieben? Reichen diese Maßnahmen für die Verarbeitungstätigkeiten und zu verarbeitende Datenkategorien aus? Gibt es Kenntnisse zu den Handreichungen TeleTrust, BSI oder auch VdS?

13. Wurden die Beschäftigten, die Zugang zu EDV-Anlagen haben (Beschäftigte, welche E-Mails schreiben, Telefonate beantworten, der Pförtner/Empfang, Schichtleiter und alle weiteren Personen) im Datenschutz unterwiesen und haben an **Schulungen** zum Datenschutz teilgenommen?

14. Sind die Beschäftigten auf den Datenschutz (z.B. als Anlage zu ihrem Arbeitsvertrag) **schriftlich verpflichtet** worden? Wissen alle Beschäftigten, dass sie sich jederzeit direkt an den Datenschutzbeauftragten wenden dürfen?

15. Bestehen **Richtlinien** oder Betriebsvereinbarungen zu verschiedenen Verarbeitungstätigkeiten, wie zum Beispiel: Mobile Arbeit, Telearbeitsplätze, Umgang mit E-Mail und Internet, BYOD u.a.?

16. Haben Beschäftigte oder andere Betroffene – in besonderen Fällen – **Einwilligungen** für die Verarbeitung ihrer Daten gegeben? Wo befinden sich die entsprechenden Dokumente?

17. Ist der Umgang mit **Messengern** und auch die Nutzung privater Mobilgeräte (z.B. zum Abrufen von dienstlichen Mails) im Unternehmen geklärt?

18. Bestehen **Social Media Profile** des Unternehmens? Ist hier in jedem Profil eine entsprechende Datenschutzerklärung hinterlegt?

19. Ist die **Homepage** auf Datenschutzkonformität überprüft worden? Insbesondere: Welche Cookies sind eingebunden? Welche Tracking- oder Analysetools werden verwendet? Greift Facebook automatisch auf die Nutzerdaten zu? Gibt es externe Inhalte, die beim Nutzen der Homepage nachgeladen werden und somit Dritte, welche Nutzerdaten übermittelt bekommen? Ist die Datenschutzerklärung auf der Homepage genau auf diese Herausforderungen angepasst? Ist ein sogenanntes Cookie-Banner erforderlich und konform eingebunden worden?

20. Liegt ein **Netzwerkplan** der IT vor?

21. Liegt eine Liste aller im Unternehmen **genutzten Software** vor?

22. Gibt es bereits ein **Löschkonzept** im Unternehmen, dass die Löschfristen, die in den Informationspflichten niedergeschrieben oder gesetzlich vorgeschrieben sind oder vom Unternehmen selbst definiert wurden, verbindlich regelt?

23. Liegt eine Bestellungspflicht für einen **IT-Sicherheitsbeauftragten** vor?

24. Findet eine **regelmäßige Überprüfung** aller Unterlagen und Maßnahmen statt?