udis-zertifizierte Datenschutz-Fachkunde udiszert 12130114 www.udis.de

DeBONDT CONSULTING & IT SERVICES ...wir verstehen was Sie wollen!

Stephan De Bondt
Staatlich geprüfter Techniker „Datenverarbeitung"
Datenschutzbeauftragter nach Ulmer Modell
Sommerweg 16
D-34329 Nieste
Tel. +49 (05605) 806874
E-Mail info@debondt.de

– Checkliste für Unternehmen (Quelle IHK Würzburg) –

1. Sensibilisierung

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25. Mai 2018 nicht nur der Name der wichtigsten Datenschutzvorschriften ändern wird. Die DSGVO wird in vielen Bereichen direkte Auswirkungen auf jedes Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DS-GVO wird es weiterhin ein – **neues** – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DS-GVO geben.

2. Risikoanalyse

Vor allem aufgrund der steigenden Bußgeld- und Reputationsverlustrisiken sowie künftig drohender Schadenersatzforderungen betroffener Personen ist eine auf das gesamte Unternehmen und die einzelnen Geschäftsbereiche bezogene Risikoanalyse empfehlenswert.
Denkbare Risiken sind beispielsweise:

- Betroffenenrechte
- Mögliche Bußgelder
- Zivilrechtliche Haftungsrisiken
- Arbeitsrechtliche Aspekte
- Umgang mit Aufsichtsbehörden
- Reputationsschäden

3. Bestandsaufnahme

Um Änderungsbedarf identifizieren zu können, sollte eine Bestandsaufnahme sämtlicher Prozesse und Verfahren durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Ein möglichst aktuelles Verfahrensverzeichnis nach § 4 d Bundesdatenschutzgesetz (BDSG) kann ein wertvoller Ausgangspunkt zur Identifizierung sein. Wegen des gegenüber dem BDSG deutlich stärker risikobasierten Ansatzes der DSGVO kommen neben der Nutzung bereits bestehender Datenschutzstrukturen auch die Adaption von Prozessen und Strukturen eines bestehenden Compliancemanagements oder Qualitätsmanagementsystems in Betracht.

4. Gap-Analyse (Lückenanalyse)

Das Unternehmen sollte für die erfolgreiche Umsetzung der Vorgaben der DS-GVO einen strukturierten Abgleich des Ist-Zustandes mit dem künftigen Soll-Zustand vornehmen. Auf dieser Grundlage lassen sich dann alle weiteren Schritte planen. Die Gap-Analyse ist ein wichtiger Baustein jeglicher Projektplanung zum Thema Datenschutz, insbesondere bei der Umsetzung vorgeschriebener Transparenz- und Dokumentationspflichten. In einem ersten Schritt der Gap-Analyse sollten alle von der Umsetzung der DS-GVO betroffenen Organisationseinheiten und Prozesse und rechtlichen Einheiten identifiziert werden. Unternehmen sollten außerdem insbesondere ihre bestehenden Verträge mit Auftragsdatenverarbeitern (ADV) überprüfen und überarbeiten.

Stephan De Bondt
Staatlich geprüfter Techniker „Datenverarbeitung"
Datenschutzbeauftragter nach Ulmer Modell
Sommerweg 16
D-34329 Nieste
Tel. +49 (05605) 806874
E-Mail info@debondt.de

5. Einbindung des Datenschutzbeauftragten

Der betriebliche oder externe Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Außerdem sollte das Unternehmen die Umsetzung dieser Anforderung in einer dem Art. 24 Abs. 1 DS-GVO entsprechenden Weise dokumentieren. Der Datenschutzbeauftragte ist gleichzeitig verpflichtet, sein Unternehmen und die Beschäftigten in Datenschutzfragen zu beraten. Neben der Erfüllung der rechtlichen Pflichten ist die Einrichtung einer im Unternehmen gut kommunizierten und akzeptierten Datenschutzberatung ein wichtiges Mittel, um Fehler bei der Verarbeitung personenbezogener Daten und daraus folgende Risiken für das Unternehmen und dessen Entscheidungsträger zu vermeiden.

6. Datenschutzkommunikation

Viele Unternehmen werden dem Datenschutz aufgrund der Vorgaben der DS-GVO in Zukunft einen höheren Stellenwert zumessen müssen als nach den bisherigen Vorgaben des BDSG. Dies setzt ein klares Bekenntnis der Unternehmensführung zum Datenschutz sowie eine entsprechende Kommunikation gegenüber der Belegschaft und den Kunden voraus. Bei größeren Unternehmen bietet sich dazu – sofern nicht bereits vorhanden – die Einführung einer Datenschutzrichtlinie oder eine entsprechende Überarbeitung der EDV Richtlinie an.

7. Mitarbeiterschulungen

Aufgrund der Komplexität und den vielfältigen Anforderungen der DS-GVO sollten von den Änderungen betroffene Mitarbeiter gründlich im Umgang mit den Neuregelungen geschult werden. Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. b der DS-GVO ausdrücklich zur „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter" angehalten.

8. Betriebsrat und Betriebsvereinbarungen

Die DS-GVO zählt zu den Schutzvorschriften, über die der Betriebsrat zum Schutz der Arbeitnehmer zu wachen hat. Aus Unternehmersicht empfiehlt es sich deshalb zu Fragen der Umsetzung der DS-GVO frühzeitig den Betriebsrat in die Umsetzungsprozesse mit einzubeziehen. Aufgrund der DS-GVO werden außerdem teilweise erhebliche Anpassungen bei bestehenden Betriebsvereinbarungen notwendig. Zudem kann auch der Abschluss neuer Betriebsvereinbarungen Sinn machen.

9. Rechtzeitige Planung neuer Prozesse und Strukturen

Nach der DS-GVO werden zahlreiche neue Prozesse und Strukturen vorausgesetzt, die die Unternehmen bis Ende Mai 2018 umsetzen müssen. Dabei sollten insbesondere folgende Anforderungen besonders berücksichtigt werden:

a) Datenschutzdokumentation

Die DS-GVO enthält zahlreiche Dokumentationspflichten, wie etwa das Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO), die Dokumentation von Weisungen bei Auftragsverarbeitungsverhältnissen (Art. 28 Abs. 3 lit. a) sowie die rechtzeitige Meldung von Datenschutzvorfällen (Art. 33 Abs. 5 DS-GVO).

Stephan De Bondt
Staatlich geprüfter Techniker „Datenverarbeitung"
Datenschutzbeauftragter nach Ulmer Modell
Sommerweg 16
D-34329 Nieste
Tel. +49 (05605) 806874
E-Mail info@debondt.de

b) Privacy by design, privacy by default

Unternehmen sind in Zukunft nach Art. 25 DS-GVO dazu verpflichtet, die geltenden Datenschutzvorschriften durch eine datenschutzfreundliche Gestaltung der eingesetzten IT und entsprechende Voreinstellungen umzusetzen. Unternehmen müssen dies durch geeignete technische Maßnahmen umsetzen, etwa durch auf Datenminimierung ausgerichtete IT-Systeme und eine möglichst frühzeitige Pseudonymisierung von personenbezogenen Daten.

c) Transparenz

Eines der wichtigsten Gebote der DS-GVO ist das Transparenzgebot. Die von der Verarbeitung personenbezogener Daten betroffenen Personen müssen von der verantwortlichen Stelle über eine Vielzahl von Angaben bezüglich der geplanten Datenverarbeitung rechtzeitig informiert werden. Dies äußert sich in gegenüber dem BDSG deutlich erweiterten Mitteilungs- und Hinweispflichten (Art. 13 u. 14 DS-GVO). So müssen etwa Zweck und Zweckänderung einer erstmaligen Erhebung oder geplanten Datenverarbeitung gegenüber den Betroffenen transparent kommuniziert werden. Darüber hinaus werden Unternehmen verpflichtet, ein Löschkonzept mit entsprechenden Löschfristen zu entwickeln.

d) Datenschutzfolgenabschätzung

Sofern eine geplante Datenverarbeitung hohe Risiken für die Rechte und Freiheiten natürlicher Personen beinhaltet, ist der Verantwortliche verpflichtet, vor dem erstmaligen Einsatz des Verfahrens eine sog. Folgenabschätzung (Art. 35 DS-GVO) durchzuführen. Hierzu sollte in den Unternehmen rechtzeitig ein Konzept zur Durchführung und Dokumentation eines solchen Verfahrens erarbeitet werden.

e) Beschwerdemanagement zur Wahrung der Betroffenenrechte

Nach der DS-GVO stehen den von einer Verarbeitung von personenbezogenen Daten betroffenen Personen verschiedenen Mechanismen zur Geltendmachung ihrer Rechte zur Verfügung. Dies äußert sich etwa in dem Auskunftsrecht nach Art. 15 DS-GVO, das deutlich umfangreicher ist als das bisher nach § 34 BDSG bestehende. Außerdem sieht die DS-GVO u. a. ein Recht auf Berichtigung (Art. 16 DS-GVO), das „Recht auf Vergessenwerden" (Art. 17 Abs. 2 DS-GVO), ein Recht auf Datenübertragbarkeit (Art. 20 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 Abs. 1 DS-GVO) sowie ein Widerspruchsrecht (Art. 21 DS-GVO) vor. Die Umsetzung dieser Betroffenenrechte legt nahe, dass Unternehmen ein entsprechendes Beschwerdemanagement einrichten sollten, um die Geltendmachung der genannten Ansprüche umsetzen zu können, andernfalls droht eine Haftung.

f) Vertragsmanagement

Unternehmen sollten ein Vertragsmanagement für Verträge mit datenschutzrechtlichem Bezug einführen und bis zur Geltung der DS-GVO sicherstellen, dass bestehende Auftragsdatenverarbeitungsverträge (ADV), Verträge zur Übermittlung von personenbezogenen Daten und sonstige Verträge, die die Verarbeitung personenbezogener Daten beinhalten, den Anforderungen der Art. 28 und 29 DS-GVO entsprechen.

g) Einwilligungsmanagement

Die DS-GVO stellt hohe Anforderungen an die Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten. Daher sollte strukturiert geprüft und dokumentiert werden, an welchen Stellen personenbezogene Daten auf welcher Grundlage verarbeitet werden, um bestehende Prozesse von den bisherigen Vorgaben auf die des Art. 7 DS-

Stephan De Bondt
Staatlich geprüfter Techniker „Datenverarbeitung"
Datenschutzbeauftragter nach Ulmer Modell
Sommerweg 16
D-34329 Nieste
Tel. +49 (05605) 806874
E-Mail info@debondt.de

GVO umzustellen. Nach dem Beschluss des Düsseldorfer Kreises vom 14. September 2016 gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 DS-GVO). Bereits rechtswirksam erteilte Einwilligungen erfüllen grundsätzlich diese Bedingungen. Informationspflichten nach Art. 13 DS-GVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.