DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

DS-GVO „Readiness Check“

Fragebogen zur Umsetzung der DS-GVO zum 25.05.2018

Fragen	*Ja*	*Nein*
I. Allgemeine Angaben zum Unternehmen		
1. Ist das Unternehmen Bestandteil eines Konzern oder eines Unternehmensverbunds?		
2. Ist die Datenverarbeitung Kern der Tätigkeit des Unternehmens (Auskunftei, Adresshandel, Forderungsmanagement)?		
3. Verarbeiten Sie als Kern der Tätigkeit besondere personenbezogene Daten gemäß Art. 9 und 10 DS-GVO wie etwa Gesundheitsdaten, religiöse Überzeugungen, Daten über strafrechtliche Verurteilungen oder Straftaten?		
4. Verarbeiten Sie im Rahmen Ihrer Tätigkeit personenbezogene Daten von Auftraggebern oder Dritten?		
5. Sind in Ihrem Unternehmen in der Regel mindestens 10 Mitarbeiter ständig mit der Verarbeitung personenbezogener Daten beschäftigt?		
II. Datenschutz-Organisation im Unternehmen		
1. Gibt es bei Ihnen im Unternehmen das Bewusstsein, dass Datenschutz Aufgabe der Geschäftsleitung ist?		
2. Sind die Zuständigkeiten für die anstehenden Aufgaben eindeutig verteilt, gegebenenfalls auf weitere Mitarbeiter im Unternehmen?		
3. Gibt es eine Datenschutz-Richtlinie in Ihrem Unternehmen?		
4. Sind alle Mitarbeiter und Mitarbeiterinnen auf den Datenschutz verpflichtet?		
5. Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?		
6. Wenn ein Datenschutzbeauftragter bestellt ist, ist festgelegt, wer ihn wann einbezieht?		
7. Ist der Datenschutzbeauftragte bereits an die zuständige Aufsichtsbehörde gemeldet?		

Ihr Ansprechpartner: Rechtsanwalt Dr. Jens Eckhardt, Derra, Meyer & Partner, Düsseldorf, Ulm, Berlin,
Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV),
eckhardt@derra-d.de, Tel.: +49 211 17520660

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

	Ja	Nein
III. Verarbeitungstätigkeiten im Unternehmen		
1. Zunächst ist zu ermitteln, wo im Unternehmen welche personenbezogenen Daten (=Daten, die sich auf eine natürliche Person beziehen) verarbeitet werden. Ist in Ihrem Unternehmen eine Bestandsaufnahme erfolgt, in der festgehalten wurde, in welchen Bereichen personenbezogene Daten verarbeitet werden?		
2. Setzen Sie Videoüberwachung ein?		
3. Erstellen Sie Profile von Kunden, Interessenten, Beschäftigten, Lieferanten oder sonstigen Personen?		
4. Beziehen Sie von Dritten derartige Profile (beispielsweise Crefo, Schufa, Bürgel, etc.)?		
5. Grundsätzlich fordert Art. 30 DS-GVO, dass alle Verantwortlichen ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen haben, die in ihrem Unternehmen durchgeführt werden. Zu denken ist hier beispielsweise an Kundendaten, Beschäftigtendaten oder Verarbeitungen von Daten für Dritte. Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO?		
6. Wenn Sie ein solches Verzeichnis noch nicht haben, haben Sie ein Verfahrensverzeichnis nach BDSG alt?		
7. Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn es hierfür eine Rechtsgrundlage gibt. Eine Verarbeitung ohne Rechtsgrundlage ist unzulässig und kann zu hohen Bußgeldern führen. Wissen Sie, auf welche Rechtsgrundlage Sie bisher und künftig Ihre Verarbeitungen stützen können?		
8. Haben Sie für alle Verarbeitungen eine Rechtsgrundlage nach der neuen Rechtslage?		
9. Die Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 lit. a DS-GVO rechtmäßig, wenn die betroffene Person eine Einwilligung erteilt hat und die speziellen Anforderungen insbesondere nach Artt. 7, 8 DS-GVO erfüllt sind. Arbeiten Sie mit Einwilligungen?		
10. Die Verarbeitung personenbezogener Daten ist nach DS-GVO i. V. m. BDSG-2018 auch dann rechtmäßig, wenn sie durch eine Betriebsvereinbarung abgedeckt ist und diese den Anforderungen der DS-GVO und des BDSG-2018 genügen. Wird die Verarbeitung personenbezogener Daten bei Ihnen auch auf eine Betriebsvereinbarung gestützt?		
IV. Unterstützung durch Externe		
1. Selten erledigen Unternehmen ihre gesamten Aufgaben ohne fremde Hilfe. Häufig werden Dienstleister eingeschaltet, die für das Unternehmen z.B. die IT-Einrichtung warten, die Buchhaltung erledigen oder auch die Kundenberatung übernehmen. Haben Sie Externe zur Erledigung Ihrer Arbeiten eingebunden?		
2. Wenn ja, haben Sie eine Übersicht über die Dienstleister?		
3. Ist die Rechtsgrundlage zur Einbindung von Externen geprüft und dokumentiert?		

	Ja	Nein
4. Die Auftragsverarbeitung ist eine Möglichkeit zur Einbindung von Externen. Für die Auftragsverarbeitung ist ein Vertrag zwischen Ihrem Unternehmen und dem Auftragsverarbeiter zu schließen, der insbesondere das Weisungsrecht des Auftraggebers festschreibt, sowie beschreibt, was der Auftragsverarbeiter machen soll, ihn zur Vertraulichkeit und Einhaltung der Sicherheit der Verarbeitung verpflichtet und festlegt, was mit den Daten nach Beendigung der Auftragsverarbeitung geschehen soll. Haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 DS-GVO abgeschlossen?		
5. Sind Sie selbst als Auftragsverarbeiter für andere tätig?		
6. Haben Sie mit allen Ihren Auftraggebern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?		
V. Besondere Pflichten des Verantwortlichen		
1. Die DS-GVO schützt die Rechte und Pflichten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten. Diese Betroffenenrechte verpflichten unter anderem zur transparenten Information über die von Ihnen geplante Datenverarbeitung (Art. 12 Abs. 1 DS-GVO). Haben Sie Ihre Texte zur datenschutzrechtlichen Information betroffener Personen bei der Datenerhebung an die Anforderungen gem. Art. 12 Abs. 1, Art. 13 bzw. 14 DS-GVO angepasst?		

2. Haben Sie insbesondere folgende Informationen neu aufgenommen, sofern sie nicht bereits in der Information enthalten sind:
• Kontaktdaten Ihres etwaigen Datenschutzbeauftragten
• Zwecke und Rechtsgrundlage der Verarbeitung
• Für den Fall, dass Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen:
  ○ Nennung der berechtigten Interessen
• Bei Übermittlung von personenbezogenen Daten in Drittländer:
  ○ Nennung des Drittlands, das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der EU-Kommission, Nennung der angemessenen oder geeigneten Garantien bei ausnahmsweise zulässigen Datenübermittlungen wie Standarddatenschutzklauseln
• Dauer der Speicherung; wenn Sie diese nicht konkret benennen können, die Kriterien für die Festlegung dieser Dauer
• Hinweis auf das Bestehen der Rechte von Betroffenen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch aufgrund einer besonderer Situation des Betroffenen, Beschwerderecht bei der zuständigen Aufsichtsbehörde sowie auf Datenportabilität
• Wenn die Verarbeitung auf einer Einwilligung beruht:
  ○ das Recht, die Einwilligung jederzeit für die Zukunft widerrufen zu können
• Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
• Wenn eine automatisierte Entscheidungsfindung einschließlich Profiling stattfindet, sowie – in diesem Fall – Informationen über die dabei involvierte Logik, die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person
• Wenn Sie die Daten nicht beim Betroffenen direkt erhoben haben, aus welcher Quelle die personenbezogenen Daten stammen und ob sie aus öffentlich zugänglichen Quellen stammen		

3. Sind Ihre Einwilligungserklärungen inhaltlich an Artt. 7, 8 und 13 DS-GVO angepasst? Hinzuweisen ist besonders auf die erweiterten Informationspflichten und die jederzeitige Widerrufbarkeit der Einwilligung.		

	Ja	Nein
4. Die DS-GVO bestimmt in Art. 12, dass der Verantwortliche geeignete Maßnahmen zu treffen hat, um die Betroffenenrechte erfüllen zu können. Er muss sie unverzüglich, spätestens innerhalb eines Monats erfüllen können (Art. 12 Abs. 3 DS-GVO). Anderenfalls drohen auch hier erhebliche Bußgelder. Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft, Berichtigung und Löschung (Art. 15-17 DS-GVO) zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?		
5. Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragung betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?		
VI. Erfüllung der Nachweispflichten		
1. Nach Art. 5 Abs. 2 DS-GVO gilt die sog. Rechenschaftspflicht. Das bedeutet, dass die Einhaltung der in Art. 5 Abs. 1 DS-GVO genannten Grundsätze der Datenverarbeitung eingehalten werden und diese Prüfung dokumentiert ist. Können Sie für jede Verarbeitungstätigkeit beispielsweise die Rechtmäßigkeit die Transparenz und Zweckbindung der Verarbeitung oder die Speicherbegrenzung nachweisen?		
2. Ist sichergestellt, dass die Dokumentation laufend aktualisiert wird?		
3. Können Sie das Vorliegen einer Einwilligung gem. Art. 7 DS-GVO rechtssicher nachweisen?		
4. Haben Sie im Unternehmen Prozesse installiert, um nachweisen zu können, dass die Verarbeitungen die Bestimmungen der DS-GVO erfüllen (Art 24 Abs. 1 DS-GVO)?		
5. Haben Sie einen Prozess installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?		
VII. Technische Sicherheit der Verarbeitung		
1. Art. 32 DS-GVO regelt die Sicherheit der Verarbeitung personenbezogener Daten. Während sich die IT-Sicherheit am Schutz des Unternehmens ausrichtet, ist die Vorgabe durch Art. 32 DS-GVO am Schutz der Rechte und Freiheiten der betroffenen Person ausgerichtet. Mit der IT-Sicherheit ist daher nicht automatisch stets auch dem Datenschutzrecht genüge getan. Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau nach Maßgabe des Art. 32 DS-GVO gewährleisten?		
2. Sind die im Unternehmen bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die Anforderungen des Art. 32 DS-GVO angepasst worden?		
3. Ist ein geeigneter Prozess umgesetzt, das die regelmäßige Überprüfung, Bewertung und Verbesserung der Sicherheitsmaßnahmen beinhaltet?		

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

	Ja	Nein
VIII. Datenschutz-Folgenabschätzung		
1. Nach Art. 35 DS-GVO muss für jede Verarbeitung personenbezogener Daten die in Art. 35 DS-GVO vorgesehen Risikobewertung erfolgen. Sind Sie auf die mögliche Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?		
2. Gibt es einen definierten Prozess im Unternehmen zur Feststellung voraussichtlich hoher Risiken einer Verarbeitung für die Rechte und Freiheiten des Betroffenen?		
3. Ist festgelegt, wer für die Durchführung einer Datenschutz-Folgenabschätzung zuständig ist?		
4. Haben Sie eine Datenschutz-Folgenabschätzung zumindest einmal testweise durchgeführt?		
IX. Datenschutzverletzungen		
1. Ist sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können?		
2. Ist ein Prozess im Unternehmen vorhanden, wie mit möglichen Datenschutzverletzungen umzugehen ist?		
3. Ist sichergestellt, dass eine Datenschutzverletzung binnen 72 Stunden an die Aufsichtsbehörde mitgeteilt werden kann?		
X. Wiederkehrende Aufgaben		
1. Ist sichergestellt, dass Sie regelmäßig Änderungen in betrieblichen Abläufen dokumentieren, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben können?		
2. Wurden Ihre Mitarbeiterinnen und Mitarbeiter über die neuen Datenschutzregelungen informiert und/oder geschult?		

Rechtsanwalt Dr. Jens Eckhardt, Derra, Meyer & Partner, Düsseldorf, Ulm, Berlin
Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV)
eckhardt@derra-d.de, Tel.: +49 211 17520660