Schutt, Waetke
RECHTSANWÄLTE

Checkliste Datenschutzgrundverordnung

Was ist zu beachten? Welche Maßnahmen müssen Sie individuell in Angriff nehmen?

Mit dieser Checkliste wollen wir Mandaten und Interessierten

- helfen zu erkennen, ob sie von dem neuen Datenschutzrecht ab dem 25.05.2018 betroffen sind,
- verdeutlichen weshalb es so wichtig ist jetzt das Thema ganz oben auf die Prioritätenliste zu setzen und
- einen Leitfaden an die Hand geben, um die erforderlichen Maßnahmen individuell erfassen und in die Wege leiten zu können.

Ist mein Unternehmen betroffen?

Mit 99,9 % Wahrscheinlichkeit: Ja.

Denn betroffen ist jeder Unternehmer und jedes Unternehmen vom Freiberufler (bspw. Anwalt, Architekt) über den Kleinstunternehmer (bspw. Kaufmann, Gewerbetreibender, GbR, Einmann-GmbH) bis hin zum Konzern.

Einzige Bedingung: Sie verarbeiten personenbezogene Daten (automatisiert oder nicht-automatisiert). Personenbezogene Daten sind dabei schon die Daten der Mitarbeiter, der Kunden, der Lieferanten, der Interessenten o.ä. Damit betrifft das neue Datenschutzrecht jeden, der zum Beispiel eine Kundendatei führt oder ein CRM-System nutzt oder auch nur seine Mitarbeiterdaten digital erfasst bzw. verwaltet.

Warum muss ich handeln?

Das Datenschutzrecht wird ab dem 25.05.2018 wesentlich strenger und – was für Sie das Wichtigste sein dürfte – Verstöße werden umfassender verfolgt (Personalaufstockung der Aufsichtsbehörden, Schaffung von immateriellen Schadensersatzansprüchen Betroffener etc.) und die Bußgelder steigen exorbitant an auf bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes des Unternehmens (je nachdem, welche Summe höher ist).

Was ist konkret zu tun?

A. Verarbeitungsverzeichnis

Nach Art. 30 DSGVO müssen Sie ein Verzeichnis aller (!) Verarbeitungsvorgänge personenbezogener Daten aufstellen und pflegen, also aktuell halten.

Die Erstellung dieses Verzeichnisses betrifft jedes Unternehmen, dass unter die DSGVO fällt (siehe oben) und ist Ausgangspunkt jeder DSGVO-Compliance.

Wichtig: Da der Datenschutzbeauftragte die Vollständigkeit des Verarbeitungsverzeichnisses zu prüfen hat, bestünde bei seiner Beauftragung mit der Erstellung des Verzeichnisses eine Interessenkollision. Der (interne oder externe) Datenschutzbeauftragte darf also weder mit der Erstellung noch mit der Pflege des Verarbeitungsverzeichnisses beauftragt werden!

Die Pflicht gilt auch für Auftragsverarbeiter bzgl. der im Auftrag verarbeiteten Daten. Das heißt, dass Unternehmen, die für andere Daten verarbeiten nicht nur ihre eigenen Verarbeitungen, sondern auch diese Auftragsverarbeitungen auflisten müssen. Das betrifft bspw. Cloud-Services, SaaS-, IaaS- oder PaaS-Lösungen, aber auch die Verarbeitung von User-Daten auf dem eigenen Webserver, die Durchführung von Fernwartungsdiensten.

UNSERE LÖSUNG: Wir können Ihnen für diesen ersten Schritt Muster zur Verfügung stellen, sowie Sie bei der Erstellung, wie auch der Pflege begleiten und unterstützen.

B. Informationspflichten

Sie müssen bei der Erhebung der Daten die Person, um deren Daten es geht (= Den Betroffenen) umfangreich informieren. Diese Informationspflichten werden mit der DSGVO ausgeweitet. Beispiele für künftige Informationen, die Sie erteilen müssen sind:

- Speicherdauer der Daten,
- Quellen, aus denen die Daten stammen,
- Widerruflichkeit de Einwilligung,
- Hinweise auf die Rechte auf Sperrung, Löschung, Berichtigung,
- Hinweise auf (mögliche) Übermittlung ins EU-Ausland und Mitteilung der Rechtsgrundlage der Übermittlung.

Damit sind alle Datenschutzhinweise, alle Einwilligungserklärungen und alle Datenschutzbelehrungen anzupassen. Denken Sie daran, dass eine Auslandsübermittlung schon dann stattfindet, wenn die Daten über Tools, Plugins, Apps o.ä. von US-Anbietern verarbeitet werden.

UNSERE LÖSUNG: Wir helfen Ihnen bei der Anpassung, stellen die richtigen Fragen und erweitern bzw. modifizieren für Sie die entsprechenden Texte.

C. Einwilligung

Die Einwilligung durch die Betroffenen bleibt eine Möglichkeit der legalen Datenverarbeitung.

ABER: Die Voraussetzungen für eine wirksame Einwilligung werden verschärft und die Kopplung der Einwilligung mit der Erhebung nicht zwingend erforderlicher Daten kann die Einwilligung unwirksam machen.

Daher sind alle Einwilligungserklärungen, die Sie aktuell verwenden, anzupassen, damit auch künftig eine wirksame Einwilligung möglich ist.

UNSERE LÖSUNG: Wir prüfen und überarbeiten Ihre Einwilligungstexte.

Oftmals werden wir Ihnen auch von der Einwilligung abraten und Sie auf andere Möglichkeiten der legalen Datenverarbeitung hinweisen, bspw. die neue Möglichkeit sich auf ein berechtigtes Interesse an der Datenverarbeitung berufen zu können. Diese Möglichkeiten haben den zusätzlichen Charme, dass sie nicht, wie die Einwilligung, frei widerruflich sind.

D. Datenschutzfolgenabschätzung

Die neue DSGVO verpflichtet Sie alle künftigen Datenverarbeitungsvorgänge darauf zu prüfen, ob voraussichtlich ein hohes Risiko für die Betroffenen besteht. Das Risiko kann aufgrund Art, Umfang, besonderer Umstände oder Zwecke der Datenverarbeitung bestehen.

Sie müssen also immer diese Prüfung vornehmen und dann, wenn ein solches Risiko nicht auszuschließen ist, eine Abwägung des Nutzens mit den Folgen in Ansehung der Risiken vornehmen.

Prüfung und Abwägung sind exakt vorzunehmen und schriftlich zu dokumentieren, denn Sie müssen jederzeit die Rechtsmäßigkeit der bei Ihnen vorgenommenen Datenverarbeitungen nachweisen können (das gilt für alle Verarbeitungsvorgänge). Damit besteht also in Zukunft auch die Pflicht, umfangreiche Risikoanalysen vorzunehmen und diese gemeinsam mit den geplanten Abhilfemaßnahmen formgerecht zu dokumentieren.

Diese Prüfung und Dokumentation muss jetzt für Ihre Datenverarbeitungen erfolgen und künftig ist sicherzustellen, dass vor Beginn jeder neuen Datenverarbeitung eine solche Prüfung und Abwägung erfolgt.

UNSERE LÖSUNG: Wir helfen Ihnen ihre Datenverarbeitungsvorgänge auf die Erforderlichkeit einer Folgenabschätzung zu prüfen und ggf. die Abwägung und Dokumentation – auch gerne gemeinsam mit Ihrem Datenschutzbeauftragten – vorzunehmen.

E. Datenschutzbeauftragter

Auch nach neuem Recht muss ab 10 Mitarbeitern, die mit der Datenverarbeitung beschäftigt sind, ein Datenschutzbeauftragter im Unternehmen bestellt werden. Daneben gelten aber über die DSGVO weitere Bestellungsgründe, nämlich dann, wenn es zur Kerntätigkeit des Unternehmens gehört,

- die umfangreiche regelmäßige & systematische **Überwachung** von betroffenen Personen oder
- die umfangreiche Verarbeitung **sensitiver** Daten.

Der Datenschutzbeauftragte bekommt auch eine höhere Verantwortung und weitreichendere Befugnisse.

UNSERE LÖSUNG: Wir prüfen für Sie, ob Sie nach neuem Recht einen Datenschutzbeauftragten brauchen und klären, ob es sinnvoll ist einen internen oder besser einen externen Datenschutzbeauftragten zu bestellen. Wir können auch Vorschläge für externe Datenschutzbeauftragte machen und den Kontakt vermitteln.

F. Meldepflichten

Künftig ist bei jeder “Datenpanne” eine Meldung an die Aufsichtsbehörde zu machen. Es genügt, wenn eine Daten-Kompromittierung möglich war/ist. Natürlich ist dann auch zu melden, welche Daten betroffen und, welche Maßnahmen getroffen wurden, um die Panne zu beheben und zu verhindern, dass ein vergleichbarer Vorfall erneut entsteht.

Natürlich sind auch alle diese Vorfälle – auch die nicht meldepflichtigen – schriftlich zu dokumentieren und ein Protokoll darüber zu führen. Die Aufsichtsbehörden haben Anspruch jederzeit Einsicht in diese Dokumentation zu nehmen.

UNSERE LÖSUNG: Wir helfen Ihnen beim Aufbau innerbetrieblicher Strukturen zur Einhaltung dieser Pflichten und beraten Sie, was wann und wie künftig im Hinblick auf Datenpannen zu berücksichtigen ist. Ebenso können wir Ihnen ein Muster für eine solche Dokumentation zur Verfügung stellen.

G. Privacy by Default & Privacy by Design

Künftig ist es erforderlich schon in der Entwicklung die Datenschutzgrundsätze einzuhalten. Damit ist schon die Entwicklungsabteilung zu sensibilisieren und zu schulen, dass das zu entwickelnde Produkt die Grundsätze der Datensparsamkeit, Speicherbegrenzung, Datenminimierung etc. berücksichtigt.

Das Pendant dazu ist der Grundsatz, dass marktreife Produkte so voreingestellt sein müssen, dass nur die zwingend erforderlichen Datenübermittlungen freigeschaltet sind und alle weiteren aktiv per Opt-In vom Nutzer selbst freigeschaltet werden müssen. Damit muss also besonderer Wert darauf gelegt werden, wie das Produkt auf den Markt kommt und daneben, wie der zugrundeliegende

Nutzungsvertrag gestaltet wird, denn dadurch kann Einfluss auf die zwingend erforderlichen Datenverarbeitungen genommen werden.

UNSERE LÖSUNG: Wir schulen und sensibilisieren Ihre Mitarbeiter, sorgen für die erforderliche Beratung bei der Entwicklung von neuen Produkten und prüfen vor Markeinführung die Einhaltung der Anforderungen.

Wir gestalten bzw. ändern auch den zugrundeliegenden Vertrag, um Einklang zwischen dem Vertragszweck und dem Lesitungsumfang und den Datenverarbeitungen innerhalb des Produkts herzustellen.

H. Datenübertragbarkeit

Ab dem 25.05.2018 müssen Sie sicherstellen, dass die Kundendaten, die Sie direkt bei Ihrem Kunden erhoben haben, strukturiert in Standarddateiformate eingespielt und an andere Anbieter, bspw. einen Wettbewerber, übertragen werden können. Denn die DSGVO sieht vor, dass der Kunde einen Anspruch auf eine solche Datenübertragung hat.

UNSERE LÖSUNG: Wir unterstützen und beraten Sie bei der Umsetzung und prüfen für Sie, ob nicht eine Ausnahme greift, nach der bei technischer Unmöglichkeit der Anspruch nicht besteht.

I. Dokumentation & Verantwortlichkeiten

Alle Pflichten und Maßnahmen nach der DSGVO müssen von Ihnen dokumentiert werden.

Für die Durchführung der neuen Pflichten, wie auch für die Dokumentation derselben und für den Erhalt der Beweisführungsmöglichkeiten zur Einhaltung aller Pflichten müssen Sie Ihre internen Prozesse prüfen und anpassen, sowie geeignete Mitarbeiter auswählen, Verantwortlichkeiten vergeben, wie auch die betroffenen Mitarbeiter schulen und einweisen.

UNSERE LÖSUNG: Wir prüfen ihre Prozesse, optimieren und ändern sie hinsichtlich der neuen Anforderungen. Auf Wunsch beraten und unterstützen wir Sie dabei auch nur.

Wir schulen Ihre Mitarbeiter gezielt auf ihre künftige Rolle und wir können – gerne auch gemeinsam mit Ihrem Datenschutzbeauftragten – für die Einhaltung der Dokumentation sorgen oder aber auch „nur“ für die (stichprobenartige) Kontrolle derselben.

Was nun?

Sie haben jetzt einen Überblick über die Anforderungen und die ToDo’s aufgrund des neuen Datenschutzrechts bekommen.

Entscheiden Sie selbst wobei wir Ihnen konkret behilflich sein können. Wir arbeiten für Sie gezielt, punktuell oder aber auch innerhalb des gesamten DSGVO-Projekts komplett oder in Teilen, alleine oder gemeinsam mit Dritten. Damit wir mit Ihnen gemeinsam zur DSGVO-Compliance kommen.

Wir freuen uns auf Ihr Feedback.

Timo Schutt
Rechtsanwalt
Fachanwalt für IT-Recht

Schutt, Waetke
RECHTSANWÄLTE
Telefon 0721. 12 05 00
Telefax 0721. 12 05 05
Kriegsstraße 37
76133 Karlsruhe

Auftragserteilung / Einholung Angebot

Ihren Auftrag können Sie bereits hier erteilen oder aber nur ein Angebot für unsere Tätigkeit bzw. eine Einschätzung des voraussichtlichen Aufwands einholen:

Vorname, Name	
Straße, Haus-Nr.	
PLZ, Ort	
Telefon	
Telefax	
E-Mail	
Mobil-Telefon	

Ich brauche und möchte Hilfe und Unterstützung in den Bereichen

☐ A. Verarbeitungsverzeichnis
☐ B. Informationspflichten
☐ C. Einwilligung
☐ D. Datenschutzfolgenabschätzung
☐ E. Datenschutzbeauftragter
☐ F. Meldepflichten
☐ G. Privacy by Default & Privacy by Design
☐ H. Datenübertragbarkeit
☐ I. Dokumentation & Verantwortlichkeiten

oder

☐ Ich wünsche die Durchführung eines vollständigen DSGVO-Projekts

Auftrag / Angebot:

☐ Ich erteile einen Auftrag zur Bearbeitung der oben angekreuzten Punkte durch die Kanzlei
(Es gelten die Vergütungsvereinbarung der Kanzlei nebst Kanzleibedingungen. Die Abrechnung erfolgt nach Zeit im 15-Minuten-Takt. Stundensatz 240 € netto zzgl. 19% USt. & ggf. Auslagen.)

☐ Ich möchte ein Angebot bzw. eine Kostenschätzung zu den oben angekreuzten Punkten

Rücksendung bitte

per Fax an 0721 / 120 505

oder

per E-Mail an info@schutt-waetke.de