Datenschutz – Checkup zur DS-GVO

Eine Handreichung für kleinere Gewerbetreibende und mittelständische Betriebe

Von Jürgen Hüneborn
Fachanwalt für IT-Recht

Am Mittelhafen 16
48155 Münster
hueneborn@port7.de
0251 – 203 18800

Kanzlei Port7
Rechtsanwälte

www.port7.de

Dieses Dokument erhebt nicht den Anspruch, eine vollständige Analyse Ihrer datenschutzrechtlichen Anforderungen zu erheben. Vielmehr soll es Ihnen als Verantwortlichem oder Geschäftsführer eine grobe Planungshilfe dafür bieten, welche Aufgaben in punkto Datenschutz in Ihrem Betrieb angegangen werden müssen.
Dazu ist es in die einzelnen Themengebiete gegliedert, auf die es jeweils versucht, eine Antwort zu geben.

1. Datenschutzbeauftragter

❒ In Ihrem Betrieb werden personenbezogene Daten verarbeitet…

- und -

❒ in Ihrem Betrieb sind regelmäßig mehr als neun Personen – auch in Teilzeit – mit der Verarbeitung dieser Daten befaßt…

- oder -

❒ in Ihrem Betrieb stellt die Verarbeitung personenbezogener Daten einen „Hauptunternehmenszweck“ dar (Auskunftei, Adressverlag, …)

- oder -

❒ in Ihrem Betrieb werden „besondere personenbezogene Daten“ gem. Art. 13 DSGVO verarbeitet (dies sind z.B. Daten über die Gesundheit, den Familienstand, die religiöse Weltanschauung etc.)

Sobald Sie bei der ersten und mindestens bei einer weiteren Frage ein Kreuzchen gesetzt haben, benötigen Sie einen (internen oder externen) Datenschutzbeauftragten.

2. Datenschutzerklärung

Die DSGVO sieht deutlich mehr Pflichtinformationen vor, die Sie in Ihrer Datenschutzerklärung auf der Website aufnehmen müssen. Beispielsweise muss jetzt immer die konkrete Rechtsgrundlage für die Verarbeitung genannt werden und Sie müssen über die Betroffenenrechte aufklären. Wenn Sie einen DSB haben, muss zumindest dessen E-Mail-Adresse + Name angegeben werden.

Tipp: Richten Sie eine E-Mail-Adresse nach dem Muster „datenschutz@mein-unternehmen.de“ ein und leiten Sie diese auf den jeweiligen DSB um. Wechselt der DSB, muss die Datenschutzerklärung nicht angepasst werden.
Der Link zur Datenschutzerklärung sollte genauso wie das Impressum mit nur einem Klick von der Startseite - besser: von jeder Unterseite – erreichbar sein und nicht in einem anderen Menüpunkt versteckt werden.

Für eine korrekte DSE für Ihre Webseite sollten Sie unbedingt die folgenden Punkte klären:

- Welche Daten sich für den Betrieb Ihrer Website technisch unbedingt erforderlich
- (z.B. IP-Adresse, Datum und Uhrzeit der Anfrage, Browser, Betriebssystemversion etc.)?
- Legen Sie Log-Files an und was speichern Sie darin zu welchem Zweck? Wann werden die Log-Files gelöscht?
- Setzen Sie Cookies ein? Wenn ja, welche und zu welchem Zweck?
- Haben Sie eine SSL-Verschlüsselung? Wenn nicht, sollten Sie dringend eine einrichten. Zum einen ist eine SSL-Verschlüsselung vorgeschrieben, wenn Sie z.B. einen Online-Shop betreiben oder ein Kontaktformular verwenden und zum anderen wirkt eine SSL-Verschlüsselung auch positiv auf Ihr Google-Ranking aus.
- Brauchen Sie wirklich ein Kontaktformular? Das Kontaktformular wirft im Hinblick auf den Datenschutz ein paar Fragen auf und war in der Vergangenheit schon öfter Gegenstand von Abmahnungen. Wenn sowieso keine nennenswerte Anzahl von Anfragen über das Kontaktformular kommt, entfernen Sie es. Wenn Sie auf ein Kontaktformular nicht verzichten wollen, fügen Sie unbedingt den passenden Textbaustein in Ihre Datenschutzerklärung ein.
- Betreiben Sie einen Newsletter? Prüfen Sie, ob Ihre bislang eingeholten Einwilligungserklärungen über den 25.05.2018 hinaus wirksam sind. Das ist nach derzeitiger Auffassung der Fall, wenn die „alte“ Einwilligung auch die Anforderungen an die Einwilligung nach DSGVO erfüllt. Im Zweifel holen Sie neue Einwilligungserklärungen ein. Verwenden Sie unbedingt das sog. double-opt-in-Verfahren und passen Sie die Datenschutzerklärung mit den Textbausteinen an.
- Setzen Sie ein Web-Analyse-Tool (z.B. Google-Analytics) ein? Wenn ja, fügen Sie den passenden Textbaustein in die Datenschutzerklärung ein. Verwenden Sie ein weniger verbreitetes Tool, fragen Sie beim Anbieter nach einem Textbaustein für die Datenschutzerklärung. Achten Sie darauf, dass Sie z.B. mit Google einen Auftragsverarbeitungs-vertrag geschlossen haben. Sie können diesen für die Zeit ab dem 25.05.18 auch bereits jetzt direkt online in Ihrem Google-Konto schließen.
- Verwenden Sie social-media-plug-ins (z.B. facebook)? Wenn ja, binden Sie die Buttons
- mit der sog. „Zwei-Klick-Lösung“ / Passivlösung ein. Stellen Sie also sicher, dass beim bloßen Aufruf Ihrer Website noch keine Daten an Dritte übertragen werden.
- Binden Sie YouTube-Videos ein? Wenn ja, setzten Sie soweit wie möglich den „erweiterten Datenschutzmodus“ ein.
  Haben Sie eine Karte von Google-Maps eingebunden? Wenn ja, nehmen Sie zumindest aus Gründen der Transparenz eine entsprechende Passage in Ihre Datenschutzerklärung auf.

3. TOMs (Liste der technischen und organisatorischen Maßnahmen)

Die DSGVO verlangt von Ihnen, dass Sie geeignete technische und organisatorische Maßnahmen (TOMs) treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Beispielsweise sollte gewährleistet sein, dass niemand Unbefugtes das Gebäude, in dem sich die IT-Anlagen Ihres Unternehmens befinden, betreten kann. Es geht aber auch um die Anwendung von Verschlüsselungstechniken, Pseudonymisierung und Backup-Strategien.
Näheres finden Sie auf den Mustervorlagen zum Thema TOMs.

4. Verfahrensverzeichnis (Verzeichnis der Verarbeitungstätigkeiten)

Was ist ein Verarbeitungsverzeichnis und brauche ich sowas?
Das Verarbeitungsverzeichnis ist das Verzeichnis aller Verarbeitungstätigkeiten mit Bezug zu personenbezogenen Daten. Es ist unabhängig von der Mitarbeiterzahl von jedem Unternehmen zu führen, da die einzige in der DSGVO vorgesehene Ausnahme in nahezu keinem Fall greift.
Eine Vorlage erhalten Sie auf der Webseite des Landesdatenschutzbeauftragten oder bei Ihrem IT-Anwalt.

5. Bestehen Meldepflichten?

Gegenüber der Aufsichtsbehörde können Ihrerseits verschiedene Meldepflichten bestehen.
Die Wichtigsten sehen Sie hier im Überblick:

- Wenn Sie einen Datenschutzbeauftragten haben, müssen Sie diesen der Aufsichtsbhörde melden

- Das Verzeichnis der Verarbeitungstätigkeiten muß nur auf Anfrage zur Verfügung gestellt werden
- Die Datenschutz-Folgenabschätzung wird aufgrund der von der Behörde veröffentlichten „Liste von Verarbeitungsvorgängen“ erstellt, soweit derartige Verarbeitungstätigkeiten im Unternehmen stattfinden.
- Die Pflicht zur Meldung von Datenschutzverstößen /-pannen ergibt sich demnächst aus Art. 33 I DSGVO. Vorgesehen ist ebenfalls eine Meldung an die jeweils betroffenen Personen oder Kunden.
  Achtung: Diese Pflichten können Sie bereits treffen bei: Verlust von Datenträgern, Diebstahl von Laptops, Fehlversendungen vom eMails!

6. Datenschutz-Folgenabschätzung

Die Datenschutz - Folgenabschätzung muß erfolgen, wenn "eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat".
Dabei kann für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung vorgenommen werden. Hierbei soll der Rat des Datenschutzbeauftragten (sofern benannt) eingeholt werden.
Der Gesetzgeber hält eine Datenschutz-Folgenabschätzung insbesondere in folgenden Fällen für erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

7. ADV

Was ist eine Auftragsverarbeitung?
Eine Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet. Mit anderen Worten: Alleine der Verantwortliche (=Auftraggeber) entscheidet über Zwecke und Mittel der Verarbeitung. Der Auftragsverarbeiter (=Auftragnehmer) handelt ausschließlich nach Weisung des Verantwortlichen.Der Verantwortliche muss den Auftragsverarbeiter sorgfältig auswählen und sich dabei nicht nur vom günstigen Preis leiten lassen. Schließlich haftet der Verantwortliche für das Fehlverhalten seines Auftragsverarbeiters.

8. Chefsache!

Bitte bedenken Sie, daß ab dem 25.05 2018 Datenschutz in Ihrem Unternehmen Chefsache ist. Das bedeutet für Sie konkret:
Für die Aufsichtsbehörde ist der Ansprechpartner in Sachen Datenschutz immer die Unternehmensleitung, der Vereinsvorstand, der Geschäftsführer. Er muß sich darum kümmern, daß er die einzelnen Bereiche korrekt deligiert hat, alle Anforderungen eingehalten werden und die beauftragten Personen fachlich und persönlich geeignet sind.