Ratgeber zur Erfüllung der Datenschutzgrundverordnung

Stand August 2022

Auf den folgenden Seiten haben wir verschiedene Themen zusammengestellt, die einem Unternehmen helfen können, Anforderungen der Datenschutzgrundverordnung (DSGVO) zu erfüllen. Die Hinweise basieren auf unseren Erfahrungen in der Beratung von Unternehmen.

Wenn Sie Fragen haben oder Unterstützung bei der Umsetzung der DSGVO Anforderungen suchen, dann schreiben Sie uns einfach eine Mail unter info@plainadvisor.de oder melden sich gerne telefonisch unter 0241 89439 348. Ansprechpartner ist Herr Dieter Froning.

Die Hinweise erheben keinen Anspruch auf Vollständigkeit und stellen keine Rechtsberatung dar. Wir übernehmen ebenfalls keine Haftung für die Verfügbarkeit oder den Inhalt der von uns verwendeten Links.

Kann man sich den Aufwand mit der vollständigen Umsetzung der DSGVO sparen, es passiert doch fast nichts?

Wir beobachten, dass die Aufsichtsbehörden sehr aktiv sind. Allerdings werden nur die größten Fälle in der Presse veröffentlicht. Einen guten Überblick über bekanntgewordene Fälle sind auf der Seite https://www.enforcementtracker.com/ zu finden. Darüber hinaus lässt sich im Internet schnell feststellen, dass auch für einfachere Verfehlungen auch bei KMUs Bußgelder verhängt werden. Klassisch gehört hierzu das Nichtbestellen oder Melden von Datenschutzbeauftragten, fehlerhafte Datenschutzerklärungen oder fehlende Verarbeitungsverzeichnisse. Da niemand hierüber gerne spricht entsteht der Eindruck, als würde nichts passieren.

Wenn sie zukünftig einen Fragebogen von einer Aufsichtsbehörde erhalten, sollten Sie diesen sorgsam durchgehen und beantworten. Denn je nach Antworten reagiert die Aufsichtsbehörde recht schnell mit weiteren Auskunftsersuchen und Ihr finanzielles Risiko steigt, wenn Sie nicht vorbereitet sind.

Ein Beispielfragebogen wird z.B. vom Landesamt für Datenschutz in Bayern zur Verfügung gestellt. https://www.lda.bayern.de/media/pruefungen/201811_kmu_fragebogen.pdf

Testen Sie mal, wie weit Sie mit der Beantwortung kommen!

PLAIN ADVISOR GMBH & CO. KG

Maastrichter Straße 65
52074 Aachen

KONTAKT

Tel.: +49 · 241 · 89 43 93 48
Email: info@plainadvisor.de
Web: plainadvisor.de

Berücksichtigen Sie auch, dass eine Aufsichtsbehörde verpflichtet ist, angezeigte Verstöße durch z.B. unzufriedene Kunden, verärgerte Mitarbeiter, abgelehnte Bewerber oder neidischen Mitbewerbern nachzugehen. Dieser Fall tritt ebenfalls viel häufiger auf, als Sie vermuten.

Bitte denken Sie auch daran, dass die Kunden durch das Internet deutlich aufgeklärter sind. Ein lascher Umgang mit dem Datenschutz kann Kunden durchaus von einer Zusammenarbeit mit Ihrem Unternehmen abschrecken.

Ein Datenschutz-Audit als erste Maßnahme

Als erster Schritt sollte eine Feststellung des Datenschutz-Status in Ihrem Unternehmen durch ein Audit erfolgen. Damit kann festgestellt werden, wo Sie bei der Umsetzung des Datenschutzes stehen und wo die für Sie größten Risiken sind.

Wir geben beispielsweise in einem solchen Auditbericht auch Hinweise, wie Sie diese Risiken minimieren können, so dass Sie einen unabhängigen Leitfaden bekommen, den Sie selber umsetzen können.

Wir konzentrieren uns bei der Prüfung z.B. auf folgende Themen:

- Besitzen Sie die Pflicht einen Datenschutzbeauftragten zu bestellen?
- Was gibt es für Verarbeitungen in Ihrem Unternehmen?
- Gibt es für die von Ihnen verarbeiteten personenbezogenen Daten eine rechtliche Grundlage wie z.B. (Arbeitsverträge oder Einwilligungen) und sind diese DSGVO konform?
- Welche technischen und organisatorischen Maßnahmen haben Sie getroffen und wie sorgen Sie für eine ständige Verbesserung? In diesem Zusammenhang prüfen wir auch, ob Sie ein Informationssicherheitsmanagement etabliert haben.
- Wie stellen Sie den Datenschutz in Ihrem Unternehmen nach außen dar? Hierzu gehören die datenschutzrechtlichen Fragen Ihrer Publikationen wie z.B. Web, Zeitschriften, Newsletter, aber auch die Gestaltung von Videoüberwachung oder Zutrittskontrolle?
- Verarbeiten Unternehmen in Ihrem Auftrag Daten und wie haben Sie dies DSGVO konform abgesichert?
- Wie protokollieren Sie alle Maßnahmen zum Thema Datenschutz, so dass Sie die vom Gesetzgeber geforderte Rechenschaftspflicht erfüllen?
- Welche Prozesse und Rahmenbedingungen sind bei Ihnen vorhanden, um den Datenschutz im Sinne der DSGVO sicherzustellen?

Ein Verarbeitungsverzeichnis erstellen

In einem der nächsten Schritte sollte ein Verarbeitungsverzeichnis erstellt oder ergänzt werden. Aus diesem Verzeichnis ergeben sich viele Grundlagen für andere Themen fast automatisch.

Die Pflichtangaben hierzu sind in Artikel 30 DSGVO vorgegeben. Wir empfehlen zusätzlich noch die Themen

- Rechtsgrundlage der Verarbeitung
- Dienstleister, die im Auftrag verarbeiten
- Software die eingesetzt wird

zu ergänzen.

Da viele Angaben für jede Verarbeitung anzugeben sind, empfehlen wir das Ganze mit einem Deckblatt und den Pflichtangaben zum Verantwortlichen bzw. dem Datenschutzbeauftragten am Anfang und den zusammenfassenden TOMs (technischen und organisatorischen Maßnahmen) nach Artikel 32 DSGVO am Ende zu versehen

Bitte berücksichtigen Sie, dass Sie als Auftragsverarbeiter ein weiteres Verarbeitungsverzeichnis nach Artikel 30 Abs. 2 DSGVO pflegen müssen!

Links zu den Themen und Vorlagen finden Sie beispielsweise unter:

- https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
- https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Betriebliche_Datenschutzbeauftragte/Inhalt/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO.html

Datenschutzkonforme Webseite herstellen

Beginnen Sie anschließend die Lücken zu schließen, auf die jeder Außenstehende sofort stoßen könnte. Hierzu gehört als Insbesondere Ihre Webseite, denn diese ist mittlerweile Ihre öffentliche Visitenkarte.

Wir empfehlen, keine Datenschutzerklärungen von anderen Seiten zu kopieren. Jede Datenschutzerklärung ist spezifisch für die Angebote auf einer Seite. Bitte klären Sie vorab, welche Dienste oder Funktionen Sie online auf Ihrer Webseite anbieten oder nutzen wollen. Anschließend können beispielsweise mit den folgenden Generatoren kostengünstig die Datenschutzerklärungen erzeugt werden:

- https://www.e-recht24.de/muster-datenschutzerklaerung.html
- https://datenschutz-generator.de

Denken Sie bitte auch daran, dass Social Media Kanäle wie Facebook, Instagram, etc. eine eigene Datenschutzerklärung erforderlich machen, wenn Sie z.B. gewerblich tätig sind.

Einverständnis für die Nutzung von Cookies

Sofern Sie Cookies verwenden oder das Verhalten von Benutzern auf Webseiten tracken, brauchen Sie vor der Aktivierung eine Einverständniserklärung des Besuchers der Webseite. Meldungen, in denen nur steht „Mit dem Besuch dieser Webseite akzeptieren Sie alle Cookies“ reichen nicht aus. Bitte berücksichtigen Sie, dass neben dem Einverständnis auch der Widerruf möglich sein muss und zu den gesetzten Cookies weitere Informationen verfügbar sein sollten.

Wir empfehlen daher den Einsatz kommerzieller Cookiebanner, die diese Funktionen abdecken und eine Menge Arbeit ersparen. Hierzu gehören beispielsweise Cookiebot, Borlabs Cookie oder GDPR Cookie Consent.

Weiter Informationen zu diesem Thema erhalten Sie z.B. auf folgender Seite:

https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/

Über Videoüberwachung informieren

Nutzen Sie eine Videoüberwachung?

Dann wird von Ihnen unter anderem verlangt, dass Sie

- auf eine Videoüberwachung auf Ihrem Gelände gut sichtbar hinweisen
- einen Aushang mit den Informationspflichten nach Artikel 13 DSGVO für das Verfahren der Videoüberwachung an einer geeigneten Stelle vornehmen (z.B. Fenster neben dem Eingang).
- Videoaufnahmen kurzfristig wieder löschen.

In vielen Fällen ist eine Videoüberwachung nicht gesetzeskonform, insbesondere wenn Sie versehentlich öffentliche Räume oder auch Mitarbeiter „überwachen“. Dies sollten Sie z.B. durch ein Audit herausfinden und geeignete Maßnahmen ergreifen.

Weitere Informationen und Vorlagen finden Sie beispielsweise hier:

https://lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/videouberwachung/fragen-und-antworten-zur-videoueberwachung-175245.html/

Bewerbungen datenschutzkonform managen

Der ordnungsgemäße Umgang mit Bewerberdaten ist sehr außenwirksam. Sowohl die Aufsichtsbehörden als auch informierte Bewerber, die sich möglicherweise zu Unrecht abgelehnt fühlen, schauen sich Ihren Umgang mit Bewerbdaten gerne an. Dann spielen nicht nur das allgemeine Gleichbehandlungsgesetz, sondern auch die DSGVO eine Rolle.

Denken Sie z.B. an folgendes:

- Der Bewerber muss über seine Rechte nach Artikel 13 DSGVO bzgl. der Verarbeitung seiner Daten informiert werden. Lassen Sie den Bewerber die Kenntnisnahme dieser Informationen bestätigen.
- Sofern Sie einen Bewerber abgelehnt haben löschen und vernichten Sie alle Bewerbungsunterlagen. Im Rahmen des allgemeinen Gleichbehandlungsgesetzes ist es aber möglich, die Daten zur Abwehr von Klagen noch eine gewisse Zeit aufzubewahren.
- Bewahren Sie keine Bewerbungsunterlagen „für später“ auf. Wenn Sie dies tun möchten, dann lassen Sie sich für diesen Zweck (z.B. Berücksichtigung bei zukünftigen Vakanzen) die Aufbewahrung vom Bewerber schriftlich bestätigen. Hier ist auch eine zeitliche Angabe sinnvoll.

Einwilligungen prüfen und rechtssicher gestalten

Einwilligungen müssen nach Artikel 6, 7 DSGVO bestimmte Informationen aufweisen. Fehlen beispielsweise Zweck und Widerrufsrecht sind die Einwilligungen ungültig. Daher ist es erforderlich für jede Art von Einwilligung auch die Möglichkeit des Widerrufs vorzusehen und entsprechende Abläufe einzuplanen.

Umfangreiche Erläuterungen zu Einwilligungen finden Sie z.B. hier:

https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf

Sofern Sie Einwilligungen verwenden müssen, prüfen Sie diese Mustertexte und passen Sie diese ggfs. an die Anforderungen bzgl. der Inhalte an. Bitte berücksichtigen Sie bei der Verwendung von

Einwilligungen immer, dass Sie Prozesse etablieren müssen, um die Betroffenenrechte Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit umzusetzen.

Auftragsverarbeitungsverträge „AV-Verträge“

Klären Sie frühzeitig, welche Dienstleister Ihre personenbezogenen Daten in Ihrem Auftrag verarbeiten. Mit diesen müssen Sie einen AV-Vertrag abschließen, um diese Dienstleister in eine Pflicht zu nehmen, die Ihnen sonst alleine obliegt.

In Artikel 28. Abs. 3 DSGVO ist dazu geregelt, welche Pflichtbestandteile ein solcher AV-Vertrag beinhalten soll. Hierzu gehören auch die sogenannten technischen und organisatorischen Maßnahmen sowie die Angabe von Subdienstleistern.
Wenn Sie als Auftragsverarbeiter agieren, sollten Sie ein für Sie passenden Mustervertrag vorhalten, den Sie Ihren Auftraggebern anbieten.

Musterverträge finden Sie beispielsweise hier:

- https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_4_muster_auftragsverarbeitung
- https://www.lda.bayern.de/media/muster_adv.pdf

Als Auftragsverarbeiter sind Sie darüber hinaus verpflichtet, ein gesondertes Verarbeitungsverzeichnis zu führen und jeden Auftraggeber über einen beabsichtigten Wechsel eines Subunternehmers zu informieren. Etablieren Sie auch Prozesse, die einen Auftraggeber unverzüglich informieren, wenn ein Datenschutz- oder IT-Sicherheitsvorfall eintritt.

Sensibilisierung der Mitarbeiter

Als Unternehmen sind Sie verpflichtet, Ihre Mitarbeiter mit den Anforderungen der DSGVO (und des BDSG) vertraut zu machen.

Dies Maßnahmen sollte insbesondere überall dort erfolgen, wo Ihre personenbezogenen Daten gehäuft verarbeitet oder besondere Kategorien von personenbezogenen Daten (siehe Artikel 9 DSGVO) verarbeitet werden. Dies trifft z.B. für Mitarbeiter der Abteilungen IT, Personal (HR) und Vertrieb fast immer zu.

Es empfiehlt sich nach Artikel 5 DSGVO eine Verpflichtungserklärung für jeden Mitarbeiter abzuschließen. Diese sollte im Rahmen des Arbeitsvertrages geschehen, kann aber auch nachträglich

erfolgen und sollte für jede Person gemacht werden, die in Ihrem Unternehmen arbeitet (Mitarbeiter, Praktikanten, Zeitarbeitskräfte, Freelancer, Azubis, etc.).

Zur Sensibilisierung können Sie beispielsweise folgende Möglichkeiten nutzen:

- Schulungen durch den Datenschutzbeauftragten (persönlich, in Gruppen)
- Schulungen durch ein externes Unternehmen
- Webbased Trainings
- Informationsbroschüren

Auch hier gilt aufgrund der Rechenschaftspflicht: Protokollieren Sie die Durchführung und Teilnahme jedes einzelnen Mitarbeiters.

Dokumentieren

Mit der Rechenschaftspflicht nach Artikel 5 Abs. 2 besitzen Sie die umfangreiche Pflicht, alle Maßnahmen, Vorfälle, Verarbeitungen, etc. zu dokumentieren.

Hierzu empfehlen wir, eine zentrale Ablage aller datenschutzrelevanten Vorgänge anzulegen z.B. für

- Betroffenenersuchen
- Einwilligungen
- AV-Verträge
- Verarbeitungen
- Verfahren zum Datenschutz
- Informationsmaterial für Mitarbeiter inkl. Richtlinien, Leitlinien, etc.

Führen Sie bei Veränderungen von Dokumentieren eine Versionshistorie und bereiten Sie die Unterlagen immer so auf, dass eine Aufsichtsbehörde hieraus Ihre Maßnahmen sofort ersehen kann und die Daten aktuell sind.

Ein Datenschutz-Managementsystem einrichten

Ein Datenschutz-Managementsystem umschreibt eine Vorgehensweise sowie Regelungen, um das Thema Datenschutz zu managen. Neben der Datenschutzorganisation sind hier beispielsweise auch die Prozesse oder Vorgehensweisen hinterlegt, die zur Erfüllung des Datenschutzes in Ihrem Unternehmen erforderlich sind

Und außerdem hilft ein Managementsystem bei der Erfüllung der Rechenschaftspflicht nach Artikel 5 Abs. 2 DSGVO. Denn dazu gehören beispielsweise die folgenden Informationen:

- Leitlinie zum Datenschutz
- Richtlinie zum Datenschutz für Mitarbeiter
- Richtlinie mit Verfahren zum Datenschutz
- Systematik und Orte, an denen alle Aktivitäten dokumentiert werden.

Wir empfehlen Ihnen hierzu auf Standards oder Normen der Informationssicherheit zurückzugreifen und damit das Thema IT-Sicherheit direkt mitzulösen. Denn die technisch und organisatorischen Maßnahmen nach Artikel 32 DSGVO referenzieren genau hier auf die IT-Sicherheit. Folgende Normen empfehlen wir, in eine Betrachtung für eine Umsetzung zu ziehen:

- BSI Grundschutz https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- VdS 10000 https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu

Sofern Sie bereit ein ISO 9001 Zertifizierung besitzen, können Sie das Datenschutzthema auch in diese Regelungen und Prozesse integrieren.

Und wie geht’s weiter?

Wenn Sie feststellen, dass einige der hier erwähnten Themen und Maßnahmen sehr umfangreich sind und Zeit sowie Knowhow erfordern, dann liegen sie richtig.

Deshalb unterstützen wir Sie gerne, damit Sie sich auf Ihr Geschäft konzentrieren können. Wir zeigen Ihnen eine für Sie passende Umsetzung mit den Themen, die Sie wirklich brauchen. Hierzu gehören

- Pflege Ihrer Verarbeitungsverzeichnisse als Verantwortliche und als Auftragsverarbeiter
- Pflege Ihrer Dokumentationen zu technisch und organisatorischen Maßnahmen
- Planen und Implementieren eines Datenschutz-Managementsystem z.B. nach VdS 10010
- Coachen und Beraten Ihres internen Datenschutzbeauftragten

Mehr dazu finden Sie unter dem Thema Datenschutzberatung auf unserer Webseite.