Ratgeber zur Erfüllung der Datenschutzgrundverordnung

Stand 2.Mai 2019

Auf den folgenden Seiten haben wir verschiedene Themen zusammengestellt, die einem Unternehmen helfen können, Anforderungen der Datenschutzgrundverordnung zu erfüllen. Die Hinweise basieren auf unseren Erfahrungen mit der Umsetzung der DSGVO und versuchen, einige immer wiederkehrende Fragen von Unternehmen aufzugreifen und hierzu kurze Hinweise zur Umsetzung zu geben.

Sofern Sie feststellen, dass Ihr Unternehmen weitere Besonderheiten aufweist verweisen wir auf unsere gesonderte Beratungsleistungen, auf Fachbücher oder auch Schulungen zum Thema „Umsetzen der DSGVO".

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

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 telefonisch unter 0241 89439348.

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

Aus unserer Erfahrung sind die Aufsichtsbehörden mittlerweile sehr aktiv. D.h. sie verschicken Fragebögen an Unternehmen und reagieren in Abhängigkeit von den Antworten recht schnell. 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! Darüber hinaus werden bereits heute für einfache Verfehlungen Bußgelder verhängt. Klassisch gehört hierzu das

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

Nichtbestellen von Datenschutzbeauftragten, fehlerhafte Datenschutzerklärungen, fehlende Verarbeitungsverzeichnisse, keine Rückmeldung an die Aufsichtsbehörde, etc. Da niemand hierüber gerne spricht und die Aufsichtsbehörden hierzu viel zu wenig veröffentlichen entsteht der Eindruck, als würde nichts passieren.

Berücksichtigen Sie auch, dass eine Aufsichtsbehörde verpflichtet ist, angezeigten Verstößen durch z.B. unzufriedene Kunden, verärgerte Mitarbeiter, abgelehnte Bewerber, neidische Mitbewerber nachzugehen. Dieser Fall tritt ebenfalls viel häufiger auf, als Sie vermuten.

https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html?ticket=ST-869176-ijQJ5OvUOC2GCxGmcFhQ-ap6

Bitte denken Sie auch daran, dass die Kunden durch das Internet deutlich aufgeklärter sind. Ein Nichterfüllen der für den Kunden transparenten Pflichten kann Kunden durchaus von einer Zusammenarbeit mit Ihnen abschrecken.

Ein Datenschutz-Audit als erste Maßnahme

Als erster Schritt sollte eine Feststellung des Datenschutz-Status in Ihrem Unternehmen durch ein Audit erfolgen. Damit wird festgestellt, wo Sie bzgl. Datenschutz 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, mit dem Sie auch selber weitermachen könnten.

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

- 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?

Wir führen hierzu Interviews i.d.R. mit Verantwortlichen der folgenden Abteilungen:

- Personal
- Finanzbuchhaltung / Controlling
- Vertrieb / Marketing
- Einkauf
- IT

Ein Verarbeitungsverzeichnis erstellen

Als eine der ersten Maßnahmen zur Umsetzung der DSGVO sollte ein Verarbeitungsverzeichnis erstellt werden, denn hieraus ergeben sich die Grundlagen für fast alle anderen Themen 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 berücksichtigen.

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
- https://www.froning.de/blog/

Datenschutzkonforme Webseite herstellen

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

Wir empfehlen, keine Datenschutzerklärungen von anderen Seiten zu kopieren, sondern je nach Umfang Ihrer Webseite spezifisch generieren zu lassen. Jede Datenschutzerklärung ist spezifisch für die Angebote auf Ihrer Seite. Bitte klären Sie vorab, welche Dienste oder Funktionen Sie online anbieten, damit diese berücksichtigt werden können. Hierzu gibt es einige Generatoren im Netz, die sie verwenden oder auf die wir kostengünstig zugreifen können.

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

Für Facebook Datenschutzerklärungen gibt es auf folgender Seite einen Mustertext:

https://lawlikes.de/fbdse/

Sofern Sie Cookies verwenden oder das Verhalten von Benutzern auf Webseiten tracken, müssen Sie klären, ob Sie weiteren Zustimmungsverpflichtungen nachkommen sollten. Hierzu sei auf das folgende Dokument der Datenschutzkonferenz verwiesen:

https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Eine gute Zusammenfassung des vorigen Dokumentes finden Sie auf der folgenden Seite des Landesdatenschutzbeauftragten aus Baden-Württemberg.

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

Über Videoüberwachung informieren

Nutzen Sie Videoüberwachung, um z.B. Gebäude und Grundstück abzusichern?

In vielen Fällen ist die 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. Hierzu gehört, dass Sie mindestens

- 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).

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 das 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 Sie alle Bewerbungsunterlagen. Im Rahmen des allgemeinen Gleichbehandlungsgesetzes ist es aber möglich, die

Daten zur Abwehr von Klagen noch eine gewisse Zeit bis zur Löschung 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.

Einwilligungen prüfen und rechtssicher gestalten

Einwilligungen müssen bestimmte Informationen aufweisen. Sollten diese nicht vorhanden sein, dann können diese ungültig sein. Sofern Sie beispielsweise Newsletter verschicken sollten Sie sicher sein, dass der Empfänger eine Einwilligung erteilt hat. Und außerdem muss geregelt werden, was Sie tun müssen, wenn die Einwilligung widerrufen wird.

Umfangreiche Erläuterungen 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.

Dazu müssen wesentliche Bestandteile in einem AV-Vertrag nach Artikel 28 Abs. 3 DSGVO vorhanden sein. Es empfiehlt sich, ein eigenes Muster vorzuhalten, welches diese und die von Ihnen zusätzlich präferierten Bestandteile beinhaltet und einen Dienstleister zu bitten, dieses zu unterzeichnen. Wenn ein Dienstleister aber gerne seinen Vertrag verwenden möchte bzw. Sie ihm kein Muster vorgeben können, dann sollten Sie die Inhalte des

Auftragsverarbeitungsvertrages bzgl. der Anforderungen der DSGVO ordentlich prüfen und ggfs. Nachbesserungen fordern.

Musterverträge finden Sie beispielsweise hier:

- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https://www.lda.bayern.de/media/muster_adv.pdf

Bitte berücksichtigen Sie auch, dass der AV-Vertrag auch die technischen und organisatorischen Maßnahmen sowie die Subunternehmer enthalten soll. Insbesondere beim Wechsel von Subunternehmern ist der Auftragsverarbeiter verpflichtet, vorab Ihre Zustimmung einzuholen.

Im umgekehrten Fall sind Sie als Auftragsverarbeiter 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. Hierzu gehören sowohl vertragliche Vereinbarungen bzgl. der Rechte und Pflichten als auch Schulungen oder die Bereitstellung von Informationsmaterialien für ein Selbststudium.

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 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.).

Nutzen Sie zur Sensibilisierung anschließend mindestens noch eine der folgenden Maßnahmen:

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

https://www.integrata.de/leistungsangebot-informationstechnologie/eu-dsgvo-gdpr-im-web-based-training-format)

https://www.datakontext.com/datenschutz/shop/mitarbeiterinformation/162/mitarbeiterinformation-datenschutz

Auch hier gilt aufgrund der Rechenschaftspflicht: Halten Sie diese Maßnahmen fest bzw. protokollieren Sie, was Sie und Ihre Mitarbeiter diesbezüglich getan haben.

Dokumentieren

Mit der Rechenschaftspflicht nach Artikel 5 Abs. 2 besitzen Sie die umfangreiche Pflicht, alle Maßnahmen zu dokumentieren und insbesondere nach Artikel 32 Abs. 2 diese permanent zu verbessern.

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.

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

Nutzen Sie alternativ Softwaretools, um diese Themen zu organisieren, z.B.

https://www.2b-advice.com/GmbH-de/Datenschutzsoftware

Ein Datenschutz-Managementsystem einrichten

Ein Datenschutz-Managementsystem umschreibt eine Vorgehensweise sowie Regelungen, um ein Thema zu managen. In diesem Fall hilft dieses Managementsystem bei der Erfüllung der Rechenschaftspflicht nach Artikel 5 Abs. 2 DSGVO, d.h. Sie müssen nachweisen, dass Sie beim Datenschutz etwas gemacht haben. Dazu gehören mindestens folgende Dokumente

- 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 10010
- https://shop.vds.de/de/download/ccb240fd9da9da2ab92f63c27c36cc2c/
- VdS 1000 https://vds.de/fileadmin/vds_publikationen/cyber/V10000_low.pdf

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. Wenn Sie hierzu Unterstützung suchen, dann sprechen Sie uns einfach an.

Wir nehmen gerne alle Prozesse und Systeme auf, mit denen bei Ihnen personenbezogene Daten verarbeitet werden. Dazu gehören neben dem Audit die Umsetzung der

beschriebenen Maßnahmen, die Unterstützung Ihres Datenschutzbeauftragten bei der Umsetzung oder die Beantwortung von Fragen. Gerne sensibilisieren wir auch Ihre Mitarbeiter nach Ihren Vorgaben, erstellen für Sie das erste Verarbeitungsverzeichnis oder die Dokumentation der Datenschutzprozesse. Und wenn Sie selber Auftragsverarbeiter sind dann besitzen Sie weitere Dokumentations- und Informationspflichten, die wir für Sie erledigen.

Und außerdem stellen wir bei Bedarf Vorlagen für die verschiedenen Anwendungsfälle (AV-Vertrag, Verpflichtung Mitarbeiter, Einwilligungserklärungen, etc.) zur Verfügung.

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