EU-Datenschutz-Grundverordnung (DSGVO)
- kurz und bündig informiert -

Rechtlicher Hinweis

Die PiSA sales GmbH übernimmt keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der in diesem Dokument bereitgestellten Informationen. Die Informationen sind insbesondere allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen und Fragen konsultieren Sie bitte unbedingt Ihren Datenschutzbeauftragten bzw. einen Rechtsanwalt.

Die DSGVO und ihre Ziele

Die DSGVO ist eine beschlossene europaweite Verordnung mit dem Ziel,

+ die Datenschutzrechte für EU-Bürger zu stärken und zu vereinheitlichen,
+ in allen EU-Staaten einheitliche Standards zu schaffen,
+ das Datenschutzrecht innerhalb von Europa zu vereinheitlichen,
+ dem einzelnen Bürger mehr Kontrolle über seine Daten zu geben.

Wo und für wen gilt sie?

Die DSGVO wurde bereits am 14. April 2016 vom EU-Parlament beschlossen und trat am 25. Mai 2016 in Kraft. Die verbindliche und unmittelbare Anwendung der DSGVO gilt in allen EU-Mitgliedstaaten seit dem 25. Mai 2018.

Die Verordnung ist eine Weiterentwicklung des inländischen und des europäischen Datenschutzrechtes. Sie schließt Lücken im Datenschutzrecht einzelner EU-Mitgliedsländer und legt EU-weit einen einheitlichen Datenschutzstandard fest. Das deutsche Bundesdatenschutzgesetz erfährt in dem Zusammenhang verschiedene Änderungen und Anpassungen.

Die EU-DSGVO gilt für alle juristischen Personen und Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten. Die Verarbeitung personenbezogener Daten von Nicht-EU-Bürgern unterliegt der EU-DSGVO nur, wenn sich diese Personen in der EU aufhalten.

Hosten und verarbeiten Sie solche Daten außerhalb Europas (z.B. Cloudcomputing außerhalb der EU), so besteht die Gefahr, dass der Datenschutz und die Rechte von EU-Bürgern ausgehebelt werden.

Erweiterte Betroffenenrechte

Mit der Einführung der EU-DSGVO gehen wesentliche Erweiterungen von Betroffenenrechten einher, die auf der Verarbeiterseite neue Informations- und Handlungspflichten erfordern.

Einwilligungserklärung und Kopplungsverbot

Für jede einzelne Nutzung der personenbezogenen Daten muss eine Einwilligung vorliegen. Diese Zustimmung muss freiwillig, spezifisch, informiert, transparent und eindeutig sein.

Die Abfrage der personenbezogenen Daten muss für jeden Verwendungszweck einzeln erfolgen und darf nicht automatisch an andere Dienstleistungen gekoppelt sein.

Beispiel: Max Mustermann übergibt auf einer Messe seine Visitenkarte. Damit stimmt er der Erfassung und Verarbeitung seiner Daten pro forma zu. Aber damit besteht noch keine Einwilligung zur weiteren Nutzung seiner Daten. Es ist zu prüfen:

+ Stimmt er aktiv, freiwillig und ausdrücklich zu, über die auf der Visistenkarte zur Verfügung gestellte E-Mailadresse Newsletter oder Informationsmaterial zu erhalten?

Altersverifizierung

Personenbezogene Daten von unter 16-Jährigen dürfen nicht bzw. nur mit dem Einverständnis der Eltern verarbeitet werden.

Beispiel: Bei der Newsletter-Anmeldung muss u. U. eine Textpassage auf die Altersverifizierung hinweisen: „Mit der Anmeldung bestätige ich, dass ich älter als 16 Jahre bin.“

Auskunftsrecht/Recht auf Berichtigung

Personen haben das Recht, die Daten einzusehen, die pro Verwendungszweck bei einem Unternehmen/Dienstleister über sie gespeichert sind. Diese müssen in einem strukturierten und gängigen technischen Format verfügbar sein. Um schnell auf eine Anfrage zu reagieren, ist zu dokumentieren, welche personenbezogenen Daten im Unternehmen verarbeitet werden, woher diese stammen und ggf. an wen die Daten weitergegeben wurden.

Beispiel: Max Mustermann hat bei PiSA sales die Möglichkeit, alle zu ihm gespeicherten personenbezogenen Daten in einem Report als PDF zu bekommen.

Gleichzeitig hat er das Recht, seine Daten bei Unstimmigkeiten in PiSA sales berichtigen zu lassen.

Recht auf Löschen/Vergessenwerden

Betroffene haben das Recht auf Löschen ihrer personenbezogenen Daten.

Beispiel: Max Mustermann bittet um Löschen seiner Daten bei PiSA sales. Der Eingang der Anfrage muss zeitnah bestätigt werden. Spätestens nach einer Frist von vier Wochen müssen die Daten aus der Datenbank gelöscht werden, was Max Mustermann bestätigt bekommen muss.

Wie geht man mit der DSGVO um?

In der Regel kommen Unternehmen nicht darum herum, die Grundsätze zur Gewährleistung der EU-Datenschutz-Grundverordnung zu beachten (nur streng geregelte Ausnahmen).

Konkret wird die Modernisierung des Datenschutzes durch mehrere Grundsätze gewährleistet, die in Art. 5 der EU-DSGVO festgelegt sind. Die zentralen Prinzipien zur Modernisierung des Datenschutzes in der neuen Verordnung lauten:

Rechtmäßigkeit und Transparenz

Ohne eine Ermächtigungs- bzw. Rechtsgrundlage dürfen keine personenbezogenen Daten erhoben, benutzt und verarbeitet werden.

Zweckbindung

Die personenbezogenen Daten, für die eine Ermächtigungsgrundlage vorhanden ist, dürfen nur zu dem Zweck verwendet werden, für den eben diese Ermächtigung erteilt wurde (siehe auch unten Begrenzung der Speicherung).

Datenminimierung

Die Datenerfassung und Verarbeitung muss auf das notwendigste Maß beschränkt werden.

Richtigkeit von Daten

Bei falschen und unsachlichen Daten hat die betroffene Person sofortigen Anspruch auf Berichtigung bzw. Löschung.

Begrenzung der Speicherung

Die neue Verordnung besagt, dass die Datenspeicherung auf den Zeitraum der Verarbeitung (Zweckbindung) beschränkt ist und unbegrenzte Datenspeicherung vermieden werden muss. Ist der Zweck der Verarbeitung nicht mehr gegeben, so sind die Daten zu löschen oder zu sperren bzw. so zu speichern, dass eine eindeutige Identifizierung der Person nicht ohne Weiteres möglich ist.

Integrität und Vertraulichkeit

Die personenbezogenen Daten müssen angemessen vor Manipulation, Diebstahl oder Fälschung gesichert werden. Vor dem Hintergrund, dass die Zahl der Cyberangriffe auf Datenbanken und Zugangsberechtigungen stetig steigt, hat dieses Prinzip in der EU-Verordnung einen neuen hohen Stellenwert.

Rechenschaftspflicht

Die Einhaltung dieser Grundsätze muss nachgewiesen werden.
Sie sollten in Ihrem Unternehmen solche Punkte prüfen, wie:

+ Gibt es eine Dokumentation zu Tätigkeiten der Verarbeitung personenbezogener Daten im Unternehmen, betroffener Personenkategorien, Art der personenbezogenen Daten und deren Zwecke?
+ Gibt es eine Dokumentation des Datenerhebungsprozesses (Einwilligungserklärung, Altersverifizierung, Dokumentation etc.)?
+ Existieren Unterauftragsverhältnisse, die zu dokumentieren und vertraglich abzusichern sind?
+ Können Sie die Rechte Betroffener gewährleisten (Widerruf der Einwilligung, Löschverfahren, Auskunftspflicht etc.)?
+ Ist der Datenschutz allgemein aktualisiert und angepasst (an DSGVO angepasste Datenschutzerklärung, Zusammenarbeit mit Datenschutzbeauftragtem, angepasste Auftragsverarbeitung etc.)?
+ Sind die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der internen Sicherheit aktualisiert und an die neuen Bedingungen angepasst?
+ Gibt es ein grundsätzliches und informationstechnisches Sicherheitskonzept?
+ Sind die Datenschutz- und Mitarbeiterrichtlinien noch aktuell?

Rechtssichere Prozesse

Des Weiteren muss sichergestellt werden, dass personenbezogene Daten im Unternehmen rechtmäßig verarbeitet werden. Die Erfassung eines Kontaktes sollte mit einem sichtbaren Hinweis zum Erfassungsgrund und der Rechtsgrundlage erfolgen. Darüber hinaus sollte es einen Prozess geben, in dem die Einwilligung zur weiteren Nutzung der Daten (Newsletter, Marketingoffensiven etc.) abgefragt und dokumentiert wird. Das ist eine wichtige Grundlage, um auch zukünftig weiter personalisierte Kampagnen zu versenden.

Verzeichnis der Verarbeitungstätigkeiten zur Dokumentations- und Nachweispflicht

Die DSGVO sieht vor, dass sämtliche Unternehmensprozesse, bei denen die Verarbeitung personenbezogener Daten erfolgt, in einem internen Verzeichnis festgehalten werden. Das dient insbesondere der Zusammenarbeit mit den Aufsichtsbehörden.

Anpassung von Workflows

Einige Änderungen, wie Anpassungen am Anmeldeformular eines Newsletters, lassen sich vielleicht einfach umsetzen. Die Anpassungen und Überarbeitungen von Workflows dagegen sind unter Umständen mit sehr großem Aufwand verbunden. PiSA sales kann Sie beim Umsetzen von

Workflows und Prozessen mit der integrierten Prozessverwaltung technisch unterstützen. Es liegt jedoch in Ihrer Hoheit und Verantwortung, Ihre internen Geschäftsabläufe und Prozesse so zu organisieren, dass den Anforderungen der DSGVO Rechnung getragen werden kann.

Chancen durch die DSGVO

Da die Einzelperson mehr Kontrolle über die Verwendung der eigenen Daten erhält, ergibt sich insbesondere im Kontaktmanagement die Chance, qualifizierte und nicht "beliebige" Daten zu sammeln und "unwichtige" Daten zu entsorgen. Die Datenbasis wird entschlackt, und Auswertungsprozesse werden optimiert. Dadurch lernen Sie den Kontakt besser und tiefgründiger kennen und finden Informationen schneller und gezielter.

Sie können Interessenten und Kunden, die z.B. negativ auf Direktwerbung reagieren, herausfiltern und für diese eine effektivere Kunden-Kommunikation entwickeln - ganz zu schweigen von der Chance, das Vertrauen der Nutzer in Werbung zu stärken.

Interessenten und Kunden, die der Verwendung ihrer Daten ausdrücklich zustimmen, besitzen ein hohes Interesse an Ihren Produkten oder Dienstleistungen. Dadurch ergibt sich eine ideale Ausgangsposition, um Kunden zielgenau anzusprechen, Kundenerlebnisse zu schaffen und die Kundenbindung sowie Ihren Umsatz nachhaltig zu steigern.

Chance und Vertrauen im Wettbewerb

„Privacy by Design“, also ein „ab Werk integrierter“ Datenschutz, der auf Technikgestaltung und datenschutzfreundlichen Voreinstellungen basiert, bietet nun einen enormen Wettbewerbsvorteil.

Die EU-DSGVO schließt Backdoor-Lösungen rigoros aus. Damit gibt sie europäischen Unternehmen einen Vorteil gegenüber dem globalen Wettbewerb, denn in Europa entwickelte Software lässt nach Erfüllung der Vorgaben das Feld des nicht europäischen Mitbewerbers bezüglich Datensicherheit klar hinter sich.

Wettbewerbsverzerrung mit fragwürdigem Datenschutz in Drittländern wie Irland oder Großbritannien ist mit der DSGVO nicht möglich.

Mit gesundem Menschenverstand

Zu den drastisch erhöhten Bußgeldern bei Datenschutzverstößen möchten wir an dieser Stelle keine Bemerkungen machen, um unsere Kunden nicht zu verunsichern und nicht auch noch in die „DSGVO-Panik“ der letzten Zeit einzustimmen.

Aus unserer Sicht ist es wichtig, mit gesundem Menschenverstand (GMV) an die neuen Bedingungen heranzugehen und vor allem das GMV-Prinzip auch in der Kommunikation mit Ihren Mitarbeiterinnen und Mitarbeitern sowie natürlich auch mit Kunden und Interessenten zu vermitteln, damit statt möglicher Angst und Unsicherheit Vertrauen und Zuversicht bleiben.