DEUTSCHES STIFTUNGSZENTRUM

FACT SHEET ZUR EUROPÄISCHEN DATENSCHUTZGRUND-VERORDNUNG (DS-GVO)

Seit dem 25. Mai 2018 regelt die neue Datenschutz-Grundverordnung (DS-GVO) die Verarbeitung personenbezogener Daten für die gesamte Europäische Union. Sie gilt auch für Stiftungen und Einrichtungen, die personenbezogene Daten von EU-Bürgern verarbeiten. Stiftungen verarbeiten in vielfältiger Weise personenbezogene Daten von Spendern, Fördermittelempfängern, Stipendiaten, Mitarbeitern, Lieferanten, Nutzern der Webseite, Newsletter-Abonnenten und anderen.

Zwar ist die befürchtete große Abmahnungswelle bisher ausgeblieben, dennoch sollten Stiftungen jetzt das Notwendige tun, um den Anforderungen der DS-GVO auf Dauer zu entsprechen. Datenschutz ist keine einmalige Angelegenheit, sondern ein laufender Prozess. Er stellt komplexe Anforderungen auch an die technischen und organisatorischen Maßnahmen einer Stiftung. Es reicht nicht mehr aus, das Richtige zu tun, sondern das Richtige muss auch dokumentiert werden. Allein die Dokumentationspflichten verursachen großen technischen organisatorischen Aufwand. Bei Verstößen gegen die Vorschriften der DS-GVO kann die Aufsichtsbehörde Bußgelder verhängen.

Damit die komplexe Materie des Datenschutzes besser verständlich wird, erläutern wir in diesem Schreiben wesentliche Grundlagen und Auswirkungen der DS-GVO.

1. HERAUSFORDERUNGEN DER DS-GVO

Leider gibt es im Rahmen der DS-GVO für Stiftungen keine Musterlösungen. Die Anforderungen der DS-GVO unterscheiden sich von Fall zu Fall und Stiftung zu Stiftung. Es gibt aber Grundlagen der DS-GVO, die allgemein gelten und aus denen eine Stiftung ableiten kann, was sie grundsätzlich beachten und gewährleisten muss.

Bedingungen der Verarbeitung personenbezogener Daten

Personenbezogene Daten von Betroffenen dürfen gemäß DS-GVO nur unter folgenden Bedingungen verarbeitet werden:

- Die Daten müssen rechtmäßig aufgrund einer Rechtsgrundlage erhoben werden (Grundsatz der Rechtmäßigkeit).
- Die Daten müssen für festgelegte und legitime Zwecke erhoben werden (Grundsatz der Zweckbindung).
- Die Verarbeitung muss auf das notwendige Maß beschränkt sein (Grundsatz der Datensparsamkeit).
- Die Daten müssen richtig sein (Grundsatz der Datenrichtigkeit).
- Die Daten dürfen nur so lange gespeichert werden, wie es zur Erfüllung des Zwecks erforderlich ist, zu dem sie erhoben und verarbeitet werden (Grundsatz der Speicherbegrenzung).
- Die Daten müssen gegen den Zugriff Unbefugter gesichert werden (Grundsatz der Integrität und Vertraulichkeit).

Nachweispflichten

Der Verantwortliche für die Datenverarbeitung muss die Einhaltung der Grundsätze der Datenverarbeitung nachweisen können (Grundsatz der Rechenschaftspflicht). Dies ist eine zentrale Neuerung der DS-GVO. Die Nachweisdokumente müssen schon im Vorfeld geschaffen werden.

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Jede Verarbeitung personenbezogener Daten braucht eine Rechtsgrundlage, sonst wäre sie unrechtmäßig. Stiftungen verarbeiten personenbezogene Daten grundsätzlich rechtmäßig, wenn die Verarbeitung der Erfüllung eines Vertrages mit dem Betroffenen dient, der Betroffene in die Verarbeitung eingewilligt hat, eine rechtliche Verpflichtung des Verantwortlichen zur Verarbeitung besteht oder die Verarbeitung einem berechtigten Interesse der Stiftung dient und die Interessen des Betroffenen nicht überwiegen.

Einwilligung des Betroffenen

Bei einer Einwilligung des Betroffenen in die Verarbeitung seiner personenbezogener Daten muss der Betroffene ausdrücklich auf die Möglichkeit des Widerrufs seiner Einwilligung hingewiesen und in transparenter, verständlicher, leicht zugänglicher Form und klarer Sprache über die Datenverarbeitung informiert werden (Informationspflicht). Die Einwilligung eines Betroffenen muss eine freiwillige, eindeutig bestätigende Handlung sein. Wegen der Nachweispflichten sollte die Einwilligung schriftlich oder elektronisch eingeholt werden.

Rechte der Betroffenen

Betroffene Personen haben folgende Rechte:

- Auskunftsrecht des Betroffenen über
  - Art der personenbezogenen Daten
  - Zweck der Datenverarbeitung
  - Kategorien von personenbezogenen Daten
  - Empfänger der personenbezogenen Daten
  - Dauer der Datenspeicherung
  - Bestehen eines Rechtes auf Berichtigung oder Löschung personenbezogener Daten sowie eines Rechtes zur Beschwerde bei einer Aufsichtsbehörde
- Recht auf Berichtigung unrichtiger oder unvollständiger Daten
- Recht auf Löschung bei Widerruf der Einwilligung, bei Widerspruch gegen die Datenverarbeitung sowie bei unrechtmäßiger Datenverarbeitung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Unterrichtung anderer Empfänger über die Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten
- Recht auf Datenübertragbarkeit von einem Verantwortlichen (z.B. Serviceanbieter) auf einen anderen
- Recht zum Widerspruch gegen die Datenverarbeitung (z.B. bei Wahrung berechtigter Interessen)
- Recht zum Widerruf der datenschutzrechtlichen Einwilligungserklärung
- Recht auf Beschwerde bei einer Aufsichtsbehörde

2. UMSETZUNG DER DS-GVO

Die DS-GVO erlegt Stiftungen umfangreiche Prüf- und Dokumentationspflichten auf. Um diese Pflichten zu erfüllen, empfiehlt sich folgende Vorgehensweise:

Bestandsaufnahme

Der Stiftungsvorstand sollte als Verantwortlicher für den Datenschutz alle Prozesse zusammenstellen und prüfen, mit denen personenbezogene Daten z.B. von Spendern, Stipendiaten, Fördermittelempfängern u.a. verarbeitet werden. Zu diesen Verarbeitungsprozessen zählen neben allen Systemen, mit denen Daten erhoben, gespeichert, genutzt oder in anderer Weise verarbeitet werden, z.B. auch Kontaktformulare oder Registrierungstools. Mit der Bestandsaufnahme verschafft sich die Stiftung Transparenz über alle Verarbeitungsprozesse und bereitet gleichzeitig ein Verarbeitungsverzeichnis vor.

Datenschutzbeauftragter

Die Stiftung muss einen Datenschutzbeauftragten bestellen, wenn

- bei ihr mindestens zehn Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind und/oder
- ihre Kerntätigkeit in der umfangreichen Verarbeitung besonders schutzbedürftiger Kategorien von Daten besteht.

Erstellung einer Datenschutzerklärung

Da die DS-GVO die Informationspflichten wesentlich erweitert hat, sollten jedem Angebot und jedem Vertrag grundsätzlich die Hinweise zum Datenschutz (Datenschutzerklärung) beigefügt werden. Webseiten einer Stiftung sollten diese Hinweise auch enthalten, insbesondere dann, wenn Google Analytics oder sog. Like Buttons von sozialen Netzwerken eingesetzt werden.

Eine Datenschutzerklärung sollte folgende Inhalte haben:

- Name und Kontaktdaten der Stiftung als Verantwortlicher
- soweit erforderlich: Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten
- Art und Umfang der verarbeiteten Daten (bei Webseiten erweitert um die Aktivitäten der Webseite, z.B. Logfiles, Cookies, Registrierungen usw.)
- Zwecke der Datenverarbeitung
- Art der Personen, deren Daten verarbeitet werden
- mögliche Empfänger der Daten
- Hinweis auf Übermittlung der Daten an Drittländer außerhalb der EU (insbesondere relevant bei Cloud- und Webmail-Diensten)
- Löschfristen
- Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung, Sperrung, Widerspruch, Datenübertragbarkeit, Widerruf der Einwilligung und Beschwerde bei einer Datenschutzbehörde

Auftragsverarbeitung

Stiftungen beauftragen regelmäßig Dienstleister, die für sie personenbezogene Daten verarbeiten (z.B. Geschäftsbesorger, IT-Dienstleister u.a.). Die erbrachten Dienstleistungen sind grundsätzlich Auftragsverarbeitungen, über die ein gesonderter Auftragsverarbeitungsvertrag geschlossen werden muss. Wer diesen Vertrag zur Auftragsverarbeitung nicht schließt, handelt ordnungswidrig.

Erstellung eines Verarbeitungsverzeichnisses

Die Stiftung muss ein schriftliches oder elektronisches Verzeichnis von Verarbeitungstätigkeiten führen. Das Verzeichnis dient dem Nachweis einer datenschutzkonformen Datenverarbeitung in der Stiftung und muss für jede einzelne Verarbeitungstätigkeit folgende Angaben enthalten:

- Name und Kontaktdaten der Stiftung
- Falls erforderlich: Name und Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Art der Personen, deren Daten verarbeitet werden
- Art der verarbeiteten Daten
- Mögliche Empfänger, denen Daten übermittelt werden oder worden sind
- Hinweis auf Übermittlung von Daten in die USA oder in andere Drittstaaten außerhalb der EU (insbesondere relevant bei Cloud- und Webmail-Diensten)
- Löschfristen
- Maßnahmen der Datensicherheit

Grundsätzlich muss eine Stiftung ein Verarbeitungsverzeichnis nur führen, wenn sie 250 oder mehr Mitarbeiter beschäftigt; es sei denn, die Datenverarbeitung erfolgt nicht nur gelegentlich. Da Stiftungen Daten grundsätzlich nicht nur gelegentlich erfassen und verarbeiten, haben sie regelmäßig ein Verarbeitungsverzeichnis zu führen, auch bei weniger als 250 Mitarbeitern.

Als Verarbeitungstätigkeit gelten z.B.

- CRM-Datenbanken und Adressdatenbanken
- Buchhaltungssoftware
- Urlaubslisten
- elektronische Personalakten
- E-Mail-Programme
- Internetauftritt sowie Präsenz in sozialen Netzwerken

In einem Verarbeitungsverzeichnis müssen auch Maßnahmen zur Datensicherheit definiert werden. Deshalb ist zu klären, wie die Datensicherheit funktioniert, die Zugriffsrechte organisiert sind und welche Maßnahmen zur Abwehr von Hackerangriffen oder zum Virenschutz existieren.

Das Verarbeitungsverzeichnis sollte laufend gepflegt werden, da eine Stiftung auf Anforderung der Aufsichtsbehörde nachweisen muss, welche Verarbeitungsprozesse zu einem bestimmten Zeitpunkt aktiv waren.

Erfüllung der Betroffenenrechte

Die Stiftung sollte ein Verfahren einrichten, wie die Rechte von Betroffenen erfüllt werden, sobald sie geltend gemacht werden.

Erfüllung der Meldepflichten

Jeder Datenschutzverstoß muss der zuständigen Datenschutzbehörde innerhalb von 72 Stunden gemeldet werden. Schon ein Verstoß gegen diese Meldepflicht kann ein Bußgeld nach sich ziehen. Die Stiftung sollte daher ein Verfahren einrichten, was bei einer Datenpanne zu tun ist.

Schwachstellenanalyse

Jede Stiftung sollte auf Basis des Verarbeitungsverzeichnisses mögliche Schwachstellen des Datenschutzes analysieren und Folgendes besonders beachten:

- Rechtmäßigkeit: Ist die Datenverarbeitung rechtlich zulässig? Dient sie der Erfüllung eines Vertrages? Gibt es eine Einwilligung des Betroffenen? Besteht eine gesetzliche Verpflichtung zur Datenverarbeitung oder ist die Datenverarbeitung durch ein berechtigtes Interesse der Stiftung gedeckt?
- Datensparsamkeit: Ist die Speicherung und Verarbeitung von Daten tatsächlich notwendig?
- Datenrichtigkeit: Ist gewährleistet, dass die personenbezogenen Daten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
- Löschfristen: Werden personenbezogenen Daten gelöscht, wenn sie nicht mehr notwendig sind?
- Schutz gegen Hacker und Malware: Gibt es eine Firewall? Sind aktuelle Virenscanner installiert?
- Zugangskontrolle: Sind die IT-Anlagen der Stiftung gegen den Zugang durch Unbefugte geschützt?

Datensicherheit

Stiftungen müssen technische und organisatorische Maßnahmen ergreifen, die die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten.

Folgende Maßnahmen sind vorgeschrieben:

- Verschlüsselung: Soweit möglich, sollen personenbezogene Daten verschlüsselt werden.
- Stabilität: Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen.
- Wiederherstellbarkeit: Verarbeitungsprozesse müssen gegen Datenverlust durch eine fachgerechte Datensicherung geschützt werden.
- Regelmäßige Überprüfung: Die Datensicherheit ist regelmäßig zu prüfen.

Notwendig ist ein angemessenes Schutzniveau, das anhand der bestehenden Risiken und des Standes der Technik zu bestimmen ist.

Da die DS-GVO vorschreibt, dass die Maßnahmen zur Datensicherheit dokumentiert sind, ist es wich-

tig, die technischen und organisatorischen Maßnahmen zur Datensicherheit schriftlich festzuhalten. Dies kann im Verarbeitungsverzeichnis geschehen.

3. WESENTLICHE GRUNDBEGRIFFE DER DS-GVO

Was sind „personenbezogene Daten“?

Personenbezogene Daten sind grundsätzlich alle Informationen, die sich im weitesten Sinne auf eine natürliche Person beziehen und diese Person direkt identifizieren oder zusammen mit anderen Informationen identifizierbar machen (betroffene Person). Der Personenbezug ist weit zu verstehen. Zu den Informationen mit Personenbezug zählen z.B. Name, Anschrift, Geburtsdatum, Geschlecht, Größe, Meinungen, Motive, Wünsche, Überzeugungen, Werturteile, Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt. Die Daten können als Sprache, Schrift, Zeichen, Bilder oder Ton sowie digital oder analog vorliegen. Die DS-GVO ist technikneutral und bezieht sich nicht nur auf elektronische Daten, sondern auch auf z.B. Papierakten und Papierarchive.

Wer ist der „Verantwortliche“ für die Verarbeitung personenbezogener Daten?

Verantwortlicher im Sinne der DS-GVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Ein Verantwortlicher hat also die Entscheidungsbefugnis über das Ob, Wofür und Wieweit einer Datenverarbeitung. Verantwortlicher ist die Stiftung selbst. Innerhalb einer rechtsfähigen Stiftung ist dann der Vorstand verantwortlich und innerhalb einer nicht rechtsfähigen Stiftung der Treuhänder. Die Entscheidungsbefugnis über die Mittel der Verarbeitung kann der Verantwortliche auf einen Auftragsverarbeiter übertragen.

Wer ist ein „Auftragsverarbeiter“?

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Verantwortliche entscheidet weiterhin über Zweck und Mittel der Datenverarbeitung, delegiert aber die Verarbeitungstätigkeit an einen Auftragsverarbeiter. Der Auftragsverarbeiter handelt auf Weisung des Verantwortlichen.

Was ist eine „Verarbeitung“ von personenbezogenen Daten?

Unter „Verarbeitung“ ist praktisch jeder Umgang im Zusammenhang mit personenbezogenen Daten zu verstehen, mit oder ohne technische Hilfsmittel. Personenbezogene Daten können auch rein manuell ohne technische Mittel verarbeitet werden. Zu einer Verarbeitung zählen z.B. das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten und andere Formen des Bereitstellens, Abgleichen, Verknüpfen, Einschränken, Löschen oder Vernichten von personenbezogenen Daten. Zu einer Verarbeitung ohne automatisierte Verfahren zählen z. B. das Lesen eines Papierdokuments oder eines Bildschirminhaltes und das handschriftliche Notieren personenbezogener Daten.

4. WESENTLICHE GRUNDSÄTZE DER DS-GVO

Die DS-GVO normiert verschiedene Grundsätze des Datenschutzes, die einen Verantwortlichen unmittelbar verpflichten.

Grundsatz der Rechtmäßigkeit

Nach dem Grundsatz der Rechtmäßigkeit muss jede Verarbeitung personenbezogener Daten durch eine gesetzliche Grundlage erlaubt, also rechtmäßig sein. Ohne Rechtsgrundlage dürfen personenbezogene Daten nicht verarbeitet werden. Rechtsgrundlagen zur Verarbeitung personenbezogener Daten ergeben sich direkt aus der DS-GVO oder auch aus anderen Gesetzen. Die DS-GVO nennt folgende Rechtsgrundlagen:

- **Einwilligung**
  Für eine wirksame Einwilligung braucht es von der betroffenen Person eine freiwillige, spezifisch informierte und eindeutige Handlung, mit der sie zu verstehen gibt, dass sie mit der Verarbeitung einverstanden ist. Online könnte dies z.B. durch Anklicken eines Kästchens erfolgen. Es reicht nicht aus, eine stillschweigende Einwilligung zu unterstellen, wenn z.B. ein Kästchen schon vorab angekreuzt ist. Der Betroffene kann seine Einwilligung jederzeit ohne Begründung widerrufen. Ein Widerruf muss genauso einfach erklärt werden können wie die Einwilligung selbst.

- **Vertrag und vorvertragliche Maßnahmen**
  Die Verarbeitung ist erforderlich zur Erfüllung eines Vertrages mit der betroffenen Person oder erforderlich für vorvertragliche Maßnahmen, die auf Anfrage der betroffenen Person erfolgen.

- **Rechtliche Verpflichtung**
  Die Verarbeitung ist erforderlich zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt.

- **Wahrung lebenswichtiger Interessen**
  Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

- **Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt**
  Die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

- **Interessenabwägung**
  Die Verarbeitung ist erforderlich zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, wenn nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen. Im Einzelfall sind die jeweiligen Interessen gegeneinander abzuwägen.

Grundsatz der Transparenz

Nach dem Grundsatz der Transparenz muss jede betroffene Person umfassend über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Die betroffenen Person muss darüber informiert werden, dass ihre personenbezogenen Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und über den Umfang der Datenverarbeitung, die Zwecke der Verarbeitung, die Identität des Verantwortlichen, die Risiken der Verarbeitung und die eigenen Rechte. Sämtliche Informationen darüber sollten für die betroffene Person leicht zugänglich, verständlich und in klarer einfacher Sprache verfasst sein.

Die Informations- und Hinweispflichten kann der Verantwortliche größtenteils mit seiner Datenschutzerklärung erfüllen. In ihr kann er aufklären, Hinweise geben und die Rechte der Betroffenen erläutern.

Bei der Abgabe der Datenschutzerklärung darf der Verantwortliche grundsätzlich keinen Medienbruch begehen. D.h. im Rahmen elektronischer Datenverarbeitung muss die Datenschutzerklärung auch elektronisch abgegeben oder zur Verfügung gestellt werden und bei Dokumenten auf Papier muss die Datenschutzerklärung auch auf Papier abgegeben werden. Teilweise wird in der Praxis bei Papierdokumenten nur noch auf die Datenschutzerklärung der Homepage verwiesen und der entsprechende Link abgedruckt. Noch dürfte dies ein unzulässiger Medienbruch sein, aber es besteht Hoffnung, dass sich in Zukunft ein praktikabler Weg durchsetzt, der helfen wird, zusätzliches Papier und zusätzlichen Aufwand zu vermeiden.

Grundsatz der Zweckbindung

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für einen eindeutigen rechtmäßigen Zweck erhoben werden. Der Zweck ist schon bei der Erhebung der personenbezogenen Daten festzulegen und kann danach nicht mehr einseitig vom Verantwortlichen verändert werden. Bei jeder weiteren Datenverarbeitung muss dieser Zweck zwingend beachten werden. Die einmal erhobenen und gespeicherten Daten dürfen nicht für andere Zwecke verwenden werden. Der Verantwortliche bleibt an die ursprüngliche Zweckfestsetzung gebunden und die Verarbeitung auf den festgelegten Zweck begrenzt. Deshalb muss z.B. schon bei der Erhebung personenbezogener Daten festgelegt werden, welche Daten verarbeitet werden.

Eine Weiterverarbeitung oder eine Änderung des Verarbeitungszweckes ist nur dann rechtmäßig, wenn der neue (Weiter-)Verarbeitungszweck mit dem ursprünglichen Erhebungszweck vereinbar ist und wenn der neue (Weiter-)Verarbeitungszweck eine eigene Rechtsgrundlage hat. Alle Weiterverarbeitungen, die mit dem Erhebungszweck unvereinbar sind, sind verboten.

Ein Sonderfall gilt nur bei der Weiterverarbeitung für Archivzwecke, wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke, die im öffentlichen Interesse liegen. Unter weiteren bestimmten Voraussetzungen wäre für die genannten Zwecke eine Weiterverarbeitung auch dann zulässig, wenn sie mit den ursprünglichen Zwecken unvereinbar ist.

Bei jeder Zweckänderung muss der Verantwortliche die betroffene Person über die neuen Zwecke informieren.

Grundsatz der Datenrichtigkeit

Nach dem Grundsatz der Datenrichtigkeit müssen die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die sachliche Richtigkeit bezieht sich dabei nur auf Tatsachenangaben und nicht auf Werturteile. Falsche Daten müssen grundsätzlich gelöscht oder berichtigt werden. Ob Daten auf dem neuesten Stand sein müssen, ergibt sich aus dem jeweiligen Verarbeitungszweck.

Grundsatz der Speicherbegrenzung

Nach dem Grundsatz der Speicherbegrenzung muss die Speicherung personenbezogener Daten beendet werden, sobald eine Speicherung für den Verarbeitungszweck nicht mehr notwendig ist. Um diesem Grundsatz zu entsprechen, sollte der Verantwortliche daher Fristen für eine Löschung oder eine regelmäßige Überprüfung der personenbezogenen Daten festlegen.

Grundsatz der Integrität und Vertraulichkeit

Nach dem Grundsatz der Integrität und Vertraulichkeit sind personenbezogene Daten in einer Weise zu verarbeiten, durch die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet wird. Dafür muss der Verantwortliche geeignete technische und organisatorische Schutzmaßnahmen treffen, mit denen die Daten vor bestimmten Risiken geschützt werden. Die Schutzmaßnahmen sollen vor dem Risiko einer unbefugten oder unrechtmäßigen Verbreitung sowie einem unbeabsichtigten Verlust, einer unbeabsichtigten Zerstörung oder einer unbeabsichtigten Schädigung schützen. Die DS-GVO nennt folgende Mindestanforderungen: Pseudonymisierung, Verschlüsselung, Maßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie technische und organisatorische Maßnahmen zur schnellen Wiederherstellung von Systemen bei technischen Zwischenfällen und Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Risiken bestehen grundsätzlich durch Bruch der Vertraulichkeit (intern oder extern), Verbreitung, Veröffentlichung, Veränderung, Löschung, Verlust und Nichtverfügbarkeit.

Der Verantwortliche muss den Stand der Technik, die Umstände und den Zweck der Datenverarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die persönlichen Rechte und Freiheiten angemessen berücksichtigen.

Grundsatz der Rechenschaftspflicht des Verantwortlichen

Die DS-GVO führt den neuen Grundsatz der Rechenschaftspflicht ein. Diese scheinbar kleine Neuerung wirkt sich erheblich auf jeden Verantwortlichen aus und verschärft die Anforderungen an die Organisation des Datenschutzes. Jeder Verantwortliche muss die Organisation des Datenschutzes und die Verarbeitungsprozesse ausreichend dokumentieren und nachweisen können. Es reicht nicht mehr aus, das Richtige zu tun, sondern das Richtige ist auch zu dokumentieren und nachzuweisen.

DEUTSCHES STIFTUNGSZENTRUM

ZUM AUTOR

Rechtsanwalt Constantin Meraneos ist Rechtsanwalt im Bereich „Recht & Consulting“ im Deutschen Stiftungszentrum.

constantin.meraneos@stifterverband.de
www.deutsches-stiftungszentrum.de

DISCLAIMER