ONLINE-STIFTUNGSWOCHE

DATENSCHUTZ-GRUNDVERORDNUNG

DS-GVO

EINE INITIATIVE VON Stifter für Stifter

IN PARTNERSCHAFT MIT Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung; Bundesverband Deutscher Stiftungen; STIFTERVERBAND; Deutsche StiftungsAkademie

PROJEKTTRÄGER Haus des Stiftens – Engagiert für Engagierte

MEDIENPARTNER Fundraiser magazin; DIE STIFTUNG – Magazin für Stiftungswesen und Philanthropie

DS-GVO

Referent

Constantin Meraneos

Rechtsanwalt . Mediator

DSZ Rechtsanwalts GmbH

Deutsches Stiftungszentrum GmbH

Barkhovenallee 1

45239 Essen

Tel. 0201 8401 239

E-Mail constantin.meraneos@stifterverband.de

E-Mail constantin.meraneos@dsz-rechtsanwaelte.de

DS-GVO

Stifterverband für die Deutsche Wissenschaft

- Der Stifterverband ist seit 1920 die Gemeinschaftsinitiative von Unternehmen und Stiftungen, die als einzige ganzheitlich in den Bereichen Bildung, Wissenschaft und Innovation berät, vernetzt und fördert.
- Ein wichtiger Förderer des Stiftungswesen
- Seit 60 Jahren Treuhänder gemeinnütziger Stiftungen und steht Stiftern mit dem Deutschen Stiftungszentrum für die Beratung und Management von Stiftungen zur Seite.

Deutsches Stiftungszentrum

- Das Deutsche Stiftungszentrum berät Stifter in Fragen zur Stiftungserrichtung und hilft gemeinnützigen und mildtätigen Stiftungen bei der Verwirklichung ihrer Satzungszwecke.
- Derzeit werden über 650 rechtsfähige und nichtrechtsfähige Stiftungen mit einem Gesamtvermögen von mehr als 3,1 Milliarden Euro gemanagt.

DS-GVO

Geltungsbereich

DS-GVO

Grundbegriffe

- Personenbezogene Daten
- Verantwortlicher
- Auftragsverarbeiter
- Verarbeitung

Grundsätze

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenrichtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht des Verantwortlichen

Umsetzung

- Bestandsaufnahme
- Datenschutzerklärung
- Verarbeitungsverzeichnis
- Auftragsverarbeitungsvertrag
- Schwachstellenanalyse
- Datensicherheit
- Datenschutzbeauftragter
- Erfüllung der Meldepflichten und Betroffenenrechte

Herausforderungen

- Bedingungen der Verarbeitung personenbezogener Daten
- Nachweispflichten
- Rechtsgrundlagen der Verarbeitung
- Einwilligung des Betroffenen
- Rechte der Betroffenen

DS-GVO

Grundbegriffe
• Personenbezogene Daten • Verantwortlicher • Auftragsverarbeiter • Verarbeitung

DS-GVO

Personenbezogene Daten

- 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.
- 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.
- **Form:** Sprache, Schrift, Zeichen, Bilder oder Ton, digital oder analog; nicht nur das geschriebene Wort und nicht nur elektronische Daten

DS-GVO

Verantwortlicher

- 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.
- **Entscheidungsbefugnis** über das Ob, Wofür und Wieweit einer Datenverarbeitung.
- Die **Stiftung** ist Verantwortlicher
  - rechtsfähige Stiftung: Vorstand
  - nicht rechtsfähige Stiftung: Treuhänder

DS-GVO

Auftragsverarbeiter

- Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (z.B. Dienstleister von Datenbankservern, Cloud-Dienste, Geschäftsbesorger, Adressverwalter, Lettershops u.a.)
- Der Verantwortliche entscheidet weiter über Zweck und Mittel der Datenverarbeitung und delegiert die Verarbeitungstätigkeit an einen Auftragsverarbeiter. Der Auftragsverarbeiter handelt auf Weisung des Verantwortlichen.
- Verantwortlicher und Auftragsverarbeiter müssen einen **Auftragsverarbeitungsvertrag** schließen.

DS-GVO

Verarbeitung

- Praktisch jeder Umgang im Zusammenhang mit personenbezogenen Daten, mit oder ohne technische Hilfsmittel - auch rein manuelle Tätigkeiten.
- **Beispiele:** 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.
- **Beispiele ohne automatisierte Verfahren:** Lesen eines Papierdokuments oder eines Bildschirminhaltes und handschriftliches Notieren personenbezogener Daten.

DS-GVO

Grundsätze
• Grundsatz der Rechtmäßigkeit • Grundsatz der Transparenz • Grundsatz der Zweckbindung • Grundsatz der Datenrichtigkeit • Grundsatz der Speicherbegrenzung • Grundsatz der Integrität und Vertraulichkeit • Grundsatz der Rechenschaftspflicht des Verantwortlichen

DS-GVO

Grundsatz der Rechtmäßigkeit (Art.6 Absatz 1 DS-GVO)

Rechtsgrundlage

Jede Verarbeitung personenbezogener Daten muss durch eine Rechtsgrundlage erlaubt sein (DS-GVO, sonstiges Unionsrecht oder Recht der Mitgliedstaaten). Ohne Rechtsgrundlage dürfen personenbezogene Daten nicht verarbeitet werden.

Wichtige Rechtsgrundlagen aus der DS-GVO:

- Einwilligung
- Vertrag oder vorvertragliche Maßnahme
- Rechtliche Verpflichtung
- Wahrung lebenswichtiger Interessen
- Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt
- Interessenabwägung

DS-GVO

- **Einwilligung**

Freiwillige, spezifisch informierte und eindeutige Handlung der betroffenen Person, mit der sie zu verstehen gibt, dass sie mit der Verarbeitung einverstanden ist (z.B. online durch Anklicken eines Kästchens); **keine stillschweigende Einwilligung** möglich (z.B. bei einem Kästchen, das schon vorab angekreuzt ist).

Der Betroffene muss seine Einwilligung jederzeit ohne Begründung genauso einfach widerrufen können, wie er sie erklärt hat (**Widerrufsmöglichkeit**). Er ist über die Widerrufsmöglichkeit aufzuklären.

Es empfiehlt sich, die Einwilligung schriftlich einzuholen oder elektronisch zu dokumentieren, da der Verantwortliche eine Einwilligung des Betroffenen nachweisen können muss.

DS-GVO

Besondere Datenkategorien (Sonderfall)

Bei besonderen Datenkategorien ist immer eine Einwilligung des Betroffenen nötig und keine andere Rechtsgrundlage möglich.

Besondere Datenkategorien sind rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, genetische oder biometrische Daten, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

DS-GVO

- **Vertrag oder vorvertragliche Maßnahmen**

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

Bespiele:

- **Rechtliche Verpflichtung**

Die Verarbeitung ist erforderlich zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt (z.B. gesetzliche Aufbewahrungspflichten).

- **Wahrung lebenswichtiger Interessen**

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

DS-GVO

- **Im öffentlichen Interesse liegende Aufgabe und Ausübung öffentlicher Gewalt**

Die Verarbeitung ist erforderlich zur Aufgabenwahrnehmung im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde.

- **Interessenabwägung**

Die Verarbeitung ist erforderlich zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten und die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen nicht. Die jeweiligen Interessen sind gegeneinander abzuwägen.

Ist der Betroffene ein **Kind**, überwiegen dessen Rechte grundsätzlich.

DS-GVO

Flexibilität und Unbestimmtheit

Diese allgemeine Interessenabwägungsklausel hält den Datenschutz flexibel, schafft aber auch Probleme in der Rechtssicherheit. Die Norm ist unbestimmt und bedarf künftig der Auslegung. Es gibt keine gesetzlichen Erlaubnistatbestände, die berechtigte Interessen festlegen.

Berechtigte Interessen sind nicht nur rechtliche, sondern können auch tatsächliche, wirtschaftliche und ideelle Interessen sein. Die Erwägungsgründe zur DS-GVO nennen als berechtigte Interessen beispielhaft die Verhinderung von Betrug, die **Direktwerbung**, der Datentausausch innerhalb einer Unternehmensgruppe und die Gewährleitung von IT-Sicherheit.

Der Verantwortliche sollte sein berechtigtes Interesse in der Datenschutzerklärung erläutern.

DS-GVO

z.B. Direktwerbung

Werbung ist jede Äußerung, die darauf zielt, den Absatz von Waren oder Dienstleistungen zu fördern (wettbewerbsrechtlicher Begriff). Direktwerbung wird ausdrücklich in den Erwägungsgründen zugelassen. Daher ist **Spendenwerbung** aus einem berechtigten Interesse der Stiftung grundsätzlich zulässig. Aber im Einzelfall sind die Interessen abzuwägen.

Wichtig: Ein berechtigtes Interesse besteht grundsätzlich nur an jenen Daten, die für eine eindeutige Identifizierung notwendig und ausreichend sind – mehr nicht (z.B. nur Name, Vorname, Anschrift, Geburtsdatum).

Ein berechtigtes Interesse ist auch die Rechtsgrundlage für die Übermittlung von Daten an einen Auftragsverarbeiter.

DS-GVO

Widerspruch des Betroffenen

Betroffene Personen haben das Recht, jederzeit einer Datenverarbeitung durch den Verantwortlichen wegen berechtigter Interessen zu widersprechen. Der Verantwortliche muss die Betroffenen auf dieses Recht hinweisen.

Nach einem Widerspruch ist die Verarbeitung grundsätzlich unzulässig. Der Verantwortliche muss für eine weitere Verarbeitung der Daten wegen eines berechtigten Interesses dann **zwingende schutzwürdige Gründe** nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen oder die weitere Verarbeitung muss der **Geltendmachung, Ausübung oder Verteidigung eigener Rechtsansprüchen** dienen.

DS-GVO

Grundsatz der Transparenz (Informations- und Hinweispflichten)

- Jede betroffene Person ist umfassend darüber zu **informieren**, dass ihre personenbezogenen Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden, über den Umfang der Datenverarbeitung, die Zwecke der Verarbeitung, die Identität des Verantwortlichen, die Risiken der Verarbeitung und die eigenen Rechte (Betroffenenrechte).
- Diese Informationen müssen für den Betroffenen leicht zugänglich und in verständlicher, klarer einfacher Sprache verfasst sein.
- Werden die Daten direkt beim Betroffenen erhoben, ist er zum Zeitpunkt der Erhebung zu informieren; werden sie anders als beim Betroffenen erhoben, ist er in angemessener Frist zu informieren, auch über die Quelle und die Kategorie der erhobenen Daten(spätestens 1 Monat danach).

DS-GVO

Der Verantwortliche kann diese Informations- und Hinweispflichten grundsätzlich in seiner **Datenschutzerklärung** erfüllen.

Aber er darf bei der Information **keinen Medienbruch begehen!**

D.h. er muss die Datenschutzerklärung bei elektronischer Datenverarbeitung elektronisch abgegeben oder zur Verfügung stellen und bei Papierdokumenten auf Papier (Verträge, Kontaktformulare usw.).

Die **Praxis** druckt in Papierdokumenten teilweise nur noch verkürzte Datenschutzerklärungen oder den Link zur Datenschutzerklärung auf der Homepage ab. Dies ist aber noch unzulässig.

DS-GVO

Grundsatz der Zweckbindung

- Personenbezogene Daten dürfen nur für einen eindeutigen rechtmäßigen Zweck erhoben werden. Der Zweck ist bereits bei der Datenerhebung festzulegen. Anschließend kann er nicht mehr einseitig vom Verantwortlichen verändert werden. Der Zweck ist bei jeder weiteren Verarbeitung der Daten zwingend zu beachten.
- Für andere Zwecke dürfen die einmal erhobenen und gespeicherten Daten nicht verwendet werden. Die Verarbeitung bleibt auf den festgelegten Zweck begrenzt.

DS-GVO

- Alle Weiterverarbeitungen, die mit dem Erhebungszweck unvereinbar sind, sind verboten.
- Bei jeder Zweckänderung muss der Verantwortliche den Betroffenen über die neuen Zwecke informieren.

Sonderfall: Weiterverarbeitung für Archivzwecke, wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke, die im öffentlichen Interesse liegen. In diesen Fällen und bei **weiteren bestimmten Voraussetzungen** wäre eine Weiterverarbeitung für die genannten Zwecke auch dann zulässig, wenn sie mit den ursprünglichen Zwecken unvereinbar ist.

DS-GVO

Grundsatz der Datenrichtigkeit

- Die personenbezogenen Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.
- Die sachliche Richtigkeit bezieht sich 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.

DS-GVO

Grundsatz der Speicherbegrenzung

- Die Speicherung personenbezogener Daten muss beendet werden, sobald eine Speicherung für den Verarbeitungszweck nicht mehr notwendig ist (Löschung).
- Um diesem Grundsatz zu entsprechen, sollte der Verantwortliche Fristen für eine Löschung oder eine regelmäßige Überprüfung der personenbezogenen Daten festlegen (Löschfristen).

DS-GVO

Grundsatz der Integrität und Vertraulichkeit (Datensicherheit)

- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Der Verantwortliche muss geeignete **technische und organisatorische Schutzmaßnahmen** treffen, durch die Daten vor dem Risiko unbefugter oder unrechtmäßiger Verbreitung, unbeabsichtigter Zerstörung oder Schädigung und unbeabsichtigtem Verlust geschützt werden.
- 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 und Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen.

DS-GVO

- **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.

DS-GVO

Grundsatz der Rechenschaftspflicht des Verantwortlichen (Neu!)

- Die DS-GVO führt den Grundsatz der Rechenschaftspflicht neu 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, nur das Richtige zu tun, sondern das Richtige ist auch zu dokumentieren und nachzuweisen.

DS-GVO

Umsetzung
• Bestandsaufnahme • Datenschutzerklärung • Verarbeitungsverzeichnis • Auftragsverarbeitungsvertrag • Schwachstellenanalyse • Datensicherheit • Datenschutzbeauftragter • Erfüllung der Meldepflichten und Betroffenenrechte

DS-GVO

Bestandsaufnahme

- Stiftungsvorstand (rechtsfähige Stiftung) oder Treuhänder (nicht rechtsfähige Stiftung) sollten als Verantwortliche für den Datenschutz **alle Prozesse zusammenstellen** und prüfen, mit denen sie personenbezogene Daten verarbeiten (z.B. von Spendern, Stipendiaten, Fördermittelempfängern u.a.)
- Zu den Verarbeitungsprozessen zählen z.B. alle Systeme, mit denen Daten erhoben, gespeichert, genutzt oder in anderer Weise verarbeitet werden (Software, Registrierungstools, Kontaktformulare usw.).
- Eine Bestandsaufnahme verschafft Transparenz über alle Verarbeitungsprozesse und bereitet gleichzeitig ein **Verarbeitungsverzeichnis** vor.
- **Tipp**: Gliedern Sie zur Bestandsaufnahme der Prozesse die einzelnen Bereiche der Stiftung (Förderung, Veranstaltungen, Verwaltung, Rechnungswesen usw.) und den Verlauf der Daten (Erhebung, Speicherung, Nutzung, Weiterleitung, sonstige Verarbeitung, Sperrung, Löschung). Legen Sie dabei fest, welche Daten erhoben werden und zu welchen Zwecken. Hinterlegen Sie am besten dazu auch schon Löschfristen.

DS-GVO

Datenschutzerklärung

- Die DS-GVO erweitert die Informationspflichten wesentlich. Deshalb sollte eine Stiftung jedem Angebot, jedem Vertrag, jedem Kontaktformular usw. grundsätzlich ihre Hinweise zum Datenschutz in Form einer Datenschutzerklärung beifügen. Auch die Webseiten einer Stiftung sollten eine Datenschutzerklärung enthalten.
- Eine Datenschutzerklärung sollte folgenden **(Mindest-)Inhalt** haben:
  - Name und Kontaktdaten der Stiftung als **Verantwortlicher**
  - Wenn erforderlich: Name und Kontaktdaten des **Datenschutzbeauftragten**
  - **Art und Umfang** der verarbeiteten Daten (auch Aktivitäten der Webseite angeben und eventuell beim Dienstleister nachfragen, z.B. Logfiles, Cookies, Registrierungen usw.)

DS-GVO

- **Zwecke** der Datenverarbeitung
- Art der personenbezogenen Daten, die verarbeitet werden (z.B. Angaben zur Identifikation der Person, Auftragsdaten, Daten zum Online-Verhalten u.a.)
- mögliche **Empfänger** der Daten und Hinweis auf Übermittlung der Daten an Drittländer außerhalb der EU (bei Cloud-Diensten eventuell relevant)
- **Löschfristen**
- **Rechte der Betroffenen** auf Auskunft, Berichtigung, Löschung, Sperrung, Widerspruch, Datenübertragbarkeit, Widerruf der Einwilligung und Beschwerde bei einer Datenschutzbehörde

DS-GVO

Verarbeitungsverzeichnis

- Die Stiftung muss ein schriftliches oder elektronisches Verzeichnis von Verarbeitungstätigkeiten führen. Dieses Verzeichnis ist nicht öffentlich und muss Betroffenen nicht offengelegt werden.
- Das Verzeichnis dient zum 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

DS-GVO

- Art der Personen, deren Daten verarbeitet werden
- Art der personenbezogenen Daten, die verarbeitet werden (z.B. Angaben zur Identifikation der Person, Auftragsdaten, Daten zum Online-Verhalten u.a.)
- mögliche **Empfänger** der Daten und Hinweis auf Übermittlung der Daten an Drittländer außerhalb der EU (bei Cloud-Diensten eventuell relevant)
- 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.

DS-GVO

- Stiftungen erfassen und verarbeiten Daten grundsätzlich nicht nur gelegentlich, sondern regelmäßig, weshalb sie ein Verarbeitungsverzeichnis führen müssen, auch bei weniger als 250 Mitarbeitern.
- Als **Verarbeitungstätigkeit** gelten z.B.
  - CRM-Datenbanken und Adressdatenbanken
  - Buchhaltungssoftware
  - E-Mail-Programme
  - Internetauftritt sowie Präsenz in sozialen Netzwerken

DS-GVO

- Im 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 **aktualisiert** werden, da eine Stiftung auf Anforderung der Aufsichtsbehörde nachweisen muss, welche Verarbeitungsprozesse zu einem bestimmten Zeitpunkt aktiv waren.

DS-GVO

Auftragsverarbeitungsvertrag

- 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 keinen Vertrag zur Auftragsverarbeitung mit dem Auftragsverarbeiter schließt, handelt ordnungswidrig.

DS-GVO

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?

DS-GVO

- 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?

DS-GVO

Datensicherheit

- Stiftungen müssen technische und organisatorische Maßnahmen ergreifen, die die Sicherheit der verarbeiteten personenbezogenen Daten gewährleisten (z.B. Verschlüsselung, Stabilität, Wiederherstellbarkeit und regelmäßige Überprüfung der Systeme, ein angemessenes Schutzniveau der Daten).
- Die Maßnahmen zur Datensicherheit sollten dokumentiert werden. Dies kann im Verarbeitungsverzeichnis geschehen.
- **Wichtig:** Die Grundsätze zur Datensicherheit müssen auch beachtet werden, wenn Dritte (z.B. ehrenamtliche Mitglieder) personenbezogene Daten auf eigenen Anlagen (z.B. Zuhause) verarbeiten.

DS-GVO

Datenschutzbeauftragter

Eine Stiftung muss einen Datenschutzbeauftragten bestellen, wenn

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

DS-GVO

Betroffenenrechte

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

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.

DS-GVO

Herausforderungen der DS-GVO
• Bedingungen der Verarbeitung personenbezogener Daten • Nachweispflichten • Rechtsgrundlagen der Verarbeitung personenbezogener Daten • Einwilligung des Betroffenen • Rechte der Betroffenen

DS-GVO

Bedingungen der Verarbeitung personenbezogener Daten

Personenbezogene Daten von Betroffenen dürfen nur unter folgenden Bedingungen verarbeitet werden:

- Die Daten müssen aufgrund einer (eigenen) 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).

DS-GVO

Nachweispflichten

Der Verantwortliche für die Datenverarbeitung muss die Einhaltung der Grundsätze der Datenverarbeitung nachweisen können (Grundsatz der Rechenschaftspflicht). 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 der Betroffene in die Verarbeitung eingewilligt hat, die Verarbeitung der Erfüllung eines Vertrages mit dem Betroffenen dient, eine rechtliche Verpflichtung der Stiftung zur Verarbeitung besteht oder die Verarbeitung einem berechtigten Interesse der Stiftung dient und die Interessen des Betroffenen nicht überwiegen.

DS-GVO

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.

DS-GVO

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 Rechts auf Berichtigung oder Löschung personenbezogener Daten sowie eines Rechts zur Beschwerde bei einer Aufsichtsbehörde
- Recht auf Berichtigung unrichtiger oder unvollständiger Daten

DS-GVO

- Recht zum Widerruf der datenschutzrechtlichen Einwilligungserklärung
- Recht zum Widerspruch gegen die Datenverarbeitung (z.B. bei Wahrung berechtigter Interessen)
- Recht auf Löschung bei Widerruf der Einwilligung, bei Widerspruch gegen die Datenverarbeitung und 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 auf Beschwerde bei einer Aufsichtsbehörde

DS-GVO

Fazit

- Die DS-GVO hat die Brisanz des Datenschutzes verstärkt.
- Bußgelder sollen abschrecken.
- Wer nichts tut wird Probleme bekommen.
- Wer etwas tut und seinen guten Willen dokumentiert, steht besser da.
- Es reicht nicht (mehr) allein das Richtige zu tun, das Richtige muss auch dokumentiert und nachgewiesen werden.

ONLINE-STIFTUNGSWOCHE

VIELEN DANK

EINE INITIATIVE VON Stifter für Stifter

PROJEKTTRÄGER Haus des Stiftens – Engagiert für Engagierte

IN PARTNERSCHAFT MIT Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung; Bundesverband Deutscher Stiftungen; STIFTERVERBAND; Deutsche StiftungsAkademie

MEDIENPARTNER Fundraiser magazin; DIE STIFTUNG – Magazin für Stiftungswesen und Philanthropie