Das neue Datenschutzrecht – Das müssen Sie jetzt tun!

Ab dem 25. Mai 2018 sind die Regelungen der EU-Datenschutz-Grundverordnung (DSGVO) unmittelbar anzuwenden. Die DSGVO regelt den Umgang mit personenbezogenen Daten einheitlich für die gesamte EU und wird durch das neu gefasste Bundesdatenschutzgesetz (BDSG neu) über sogenannte Öffnungsklauseln sowie weitere gesetzliche Anpassungen (z.B. Sozialdatenschutz) ergänzt. Die DSGVO löst das bis dahin gültige Bundesdatenschutzgesetz (BDSG) ab, nach dem Stiftungen auch bisher schon verpflichtet waren, Datenschutz zu betreiben. Insgesamt verschärfen sich die datenschutzrechtlichen Anforderungen für alle Einrichtungen, die mit personenbezogenen Daten umgehen. Ausnahmen für gemeinnützige Stiftungen gibt es nicht!

Welche Daten fallen unter den Schutzbereich der DSGVO?

Im Zentrum des Datenschutzes stehen das Recht jedes einzelnen auf informationelle Selbstbestimmung und der Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Nahezu jede Stiftung besitzt Informationen z.B. zu ihren Spendern oder Sponsoren, ihren Stipendiaten oder ehren- und hauptamtlichen Mitarbeitern. Sie speichert u.a. Name, Adresse, Telefonnummer oder Email in ihren digitalen Datenbanken und nutzt diese Daten, um z.B. zu Spenden aufzurufen oder Projekte zu organisieren. Damit gelten auch Stiftungen als Verantwortliche im Sinne der DSGVO, die ab dem 25. Mai 2018 den verschärften Regelungen der DSGVO unterliegen.

Grundprinzipen des Datenschutzes

Grundprinzipien des Datenschutzes, die auch nach den neuen Regelungen beibehalten werden, und auch für jede Stiftung Geltung haben, soweit sie personenbezogene Daten verwendet, sind Folgende:

- Gebot der Datenvermeidung, Datensparsamkeit und Transparenz
- Verbot mit Erlaubnisvorbehalt: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist verboten, es sei denn, es ist durch Gesetze erlaubt, oder es gibt eine Einwilligung des Betroffenen. Erlaubende Gesetze finden sich u.a. in der DSGVO selbst. Danach ist z.B. die Nutzung der Daten erlaubt, um einen Vertrag zu erfüllen.
- Zweckbindungsgebot: Daten dürfen grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie mit Einwilligung oder Erlaubnis erhoben worden sind
- Zweckentfremdungsverbot: Eine unbefugte Änderung bzw. Erweiterung der Zweckbindung der erhobenen Daten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.
- Direkterhebung: Daten müssen grundsätzlich beim Betroffenen selbst erhoben werden. Werden sie nicht direkt bei ihm erhoben, ist er jedenfalls zu benachrichtigen

Was müssen Stiftungen jetzt konkret tun, um die Anforderungen des neuen Datenschutzrechts zu erfüllen? Welche Maßnahmen müssen Sie zuerst ergreifen? Nachfolgend stellen wir Ihnen anhand von Beispielen einen praxisorientierten Maßnahmenkatalog vor, der die grundlegenden Anforderungen der DSGVO berücksichtigt. Er soll eine Hilfestellung für Stiftungen bieten, um bis zum 25. Mai 2018 die wesentlichen Voraussetzungen für ein sicheres Datenschutzniveau auf Grundlage der neuen Rechtsvorschriften zu erfüllen.

Vorab

Wer ist verantwortlich?

Zu klären ist in der Stiftung zunächst, wer verantwortlich für die Rechtmäßigkeit der Datenverarbeitung ist. Bei Rechtsfähigen Stiftungen ist der Vorstand für den Datenschutz verantwortlich. Dies gilt auch, wenn er nur ehrenamtlich tätig ist. Bei Treuhandstiftungen ist grundsätzlich der Treuhänder als Verantwortlicher anzusehen.

Wann Ist ein Datenschutzbeauftragter zu bestellen?

Das Datenschutzrecht gilt unabhängig von der Frage, ob ein Datenschutzbeauftragter bestellt werden muss. Ein solcher muss bestellt werden, wenn

- in der Stiftung mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftig sind.
- wenn die Kerntätigkeit der Stiftung in der umfangreichen Verarbeitung besonders schutzbedürftiger Kategorien von Daten besteht.

Sind Mitarbeiter auf den Datenschutz zu verpflichten?

Beschäftigte eines Verantwortlichen dürfen personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Wer als Beschäftigter gilt, ist vor dem Hintergrund des Schutzzwecks der DSGVO weit auszulegen. Demnach gehören dazu Angestellte und arbeitnehmerähnliche Personen, insbesondere auch Auszubildende, Praktikanten, Leiharbeiter und ehrenamtlich Tätige.

Tipp: Die entsprechende Verpflichtung des Mitarbeiters sollte schriftlich erfolgen. Ein Muster stellt das Bayerische Landesamt für Datenschutzaufsicht zur Verfügung unter:

www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf .

Auszug

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen1:

Personenbezogene Daten müssen a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden; b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“); d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden; e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter. Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

Ort, Datum Unterschrift des Verpflichteten Unterschrift des Verantwortlichen

Was müssen Stiftungen jetzt tun?

Schritt 1: Bestandsaufnahme

Um personenbezogene Daten nach Maßgabe der DSGVO schützen zu können, muss die verantwortliche Stiftung zunächst ermitteln, in welchen Fällen personenbezogene Daten – z.B. von Spendern, Beschäftigten oder Stipendiaten – erhoben und verarbeitet werden. Besonders schutzbedürftig sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Denkbar sind diese Daten vor allem bei Stiftungen, die soziale Zwecke im weitesten Sinne fördern. Als erster Anhaltspunkt bietet es sich an, alle Systeme bzw. Tools in der Stiftung aufzulisten, in welchen personenbezogene Daten gespeichert werden. Sämtliche Prozesse der Stiftung, in denen personenbezogene Daten erhoben, gespeichert, genutzt oder in sonstiger Weise verarbeitet werden, sollten zunächst identifiziert werden. Dazu gehört bereits z.B. das Auslegen einer Teilnahmeliste anlässlich einer Veranstaltung der Stiftung oder ein Kontaktformular auf der Internetseite der Stiftung.

Eine solche Vorgehensweise ist aus zwei Gründen sinnvoll: Einerseits können dadurch die Datenflüsse in der Stiftung ermittelt und definiert werden. Zusätzlich wird ein erster Grundstein für das Verzeichnis von Verarbeitungstätigkeiten gelegt (Schritt 2). Die Bestandsaufnahme bildet die Grundlage für ein gutes Datenschutzmanagement.

Schritt 2: Erstellung eines Verarbeitungsverzeichnisses

Nach Art. 30 DSGVO ist der Verantwortliche (s.o.) verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Zwar soll diese Pflicht entfallen, wenn in den betreffenden Unternehmen weniger als 250 Mitarbeiter beschäftigt sind. Diese Ausnahme soll aber nur zur Anwendung kommen, soweit die Datenverarbeitung nur gelegentlich erfolgt. Da in einer Stiftung die Erfassung und Verarbeitung von Daten nicht nur gelegentlich erfolgt, ist in der Regel ein Verarbeitungsverzeichnis zu führen. In diesem Verzeichnis sind die wesentlichen Informationen zu Datenverarbeitungstätigkeiten zusammenzufassen, insbesondere also Angaben zum Zweck der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Die neuen Verzeichnisse von Verarbeitungstätigkeiten ähneln inhaltlich den bisherigen internen Verfahrensverzeichnissen nach dem BDSG. Daher dürften den Stiftungen, die bereits jetzt über strukturierte Verfahrensübersichten verfügen, die Vorgaben des Art. 30 DSGVO keine größeren Probleme bereiten.

Ein Muster für ein Verarbeitungsverzeichnis nach der DSGVO finden Sie auf der Internetseite des Bayrischen Landesamts für Datenschutzaufsicht unter

www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf

Schritt 3: Prüfung der Rechtmäßigkeitsgrundlagen

Prüfen Sie, ob Sie für jeden Verarbeitungsprozess eine Rechtsgrundlage haben! Jede Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn dafür eine Rechtsgrundlage besteht. Diese kann in der Einwilligung der betroffenen Person oder in einer gesetzlichen Erlaubnis liegen. Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten dann rechtmäßig, wenn eine

Einwilligung der betroffenen Person vorliegt

oder die Verarbeitung aufgrund einer gesetzlichen Erlaubnis erfolgt.

Eine **gesetzliche Erlaubnis** liegt vor, wenn

- die **Verarbeitung für die Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung **vorvertraglicher Maßnahmen** erforderlich ist, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im **öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt** erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen** oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Es gilt der Grundsatz, dass alles verboten ist, was nicht ausdrücklich erlaubt ist (Verbot mit Erlaubnisvorbehalt). Ferner ist zu beachten, dass nach den neuen Regelungen der DSGVO künftig Stiftungen nachweisen müssen, dass sie die gesetzlichen Anforderungen eingehalten haben. Bisher mussten die zuständigen Behörden die Verstöße nachweisen.

Soweit Sie eine Einwilligung der betroffenen Dateninhaber einholen, sollten Sie diese zum Nachweis dokumentieren, um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten. Hinweise zur Erstellung einer ordnungsgemäßen Einwilligungserklärung finden Sie in Schritt 5.

Bitte beachten Sie, dass eine gesetzliche Verpflichtung bestehen kann, personenbezogene Daten insbesondere zu speichern, d.h. aufzubewahren. So können sich z.B. aus Rechtsvorschriften des Handels- und Steuerrechts umfassende Dokumentations- und Aufbewahrungspflichten ergeben, die erfüllt werden müssen. Dies ist eine ausreichende Rechtsgrundlage für die Datenverarbeitung.

Schritt 4: Anpassung der Datenschutzerklärungen/Informationspflichten

Überprüfen Sie Ihre Datenschutzerklärungen! Die neuen Vorschriften der DSGVO sehen insbesondere verschärfte Informationspflichten vor, die die Stiftung gegenüber dem betroffenen Dateninhaber erfüllen muss. Dies kann am besten über die Datenschutzerklärung geschehen, die dem Dateninhaber bereits bei der Erhebung seiner Daten auf einfache und verständliche Weise zur Kenntnis gegeben wird.

Werden personenbezogene Daten beim Betroffenen erhoben, muss der Verantwortliche nach Art. 13 Abs. 1 DSGVO folgende Informationen mitteilen:

a) Identität des Verantwortlichen

Es ist über den Namen und die Kontaktdaten des Verantwortlichen zu informieren. Gleiches gilt ggf. für Namen und Kontaktdaten des Vertreters des Verantwortlichen nach Art. 27 DSGVO, wenn der Verantwortliche selbst nicht in der EU niedergelassen ist.

b) Kontaktdaten des Datenschutzbeauftragten

Neu ist auch die Verpflichtung zur Mitteilung der Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen, soweit ein solcher bestellt wurde.

c) Verarbeitungszwecke und Rechtsgrundlage

Der Verantwortliche muss auch über die Zwecke der Datenverarbeitung sowie über die Rechtsgrundlage der Verarbeitung informieren. Diese neue Anforderung führt dazu, dass der Betroffene darüber aufgeklärt wird, auf welchen Erlaubnistatbestand (siehe Art. 6 DSGVO, z.B. Einwilligung oder Erfüllung eines Vertrages) der Verantwortliche die Datenverarbeitung stützen möchte.

d) Berechtigtes Interesse

Sollte die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen nach Art. 6 Abs. 1 f DSGVO erforderlich sein, beziehen sich die Informationspflichten auch auf eine Aufklärung über diese Interessen.

e) Empfänger

In allen Fällen, in denen personenbezogene Daten übermittelt werden sollen, sind die Betroffenen grundsätzlich über die konkreten Empfänger zu informieren. Ausnahmsweise reicht auch eine Information über Kategorien von Empfängern, wenn konkrete Empfänger noch nicht bezeichnet werden können.

f) Übermittlung in Drittstaaten

Sollte der Verantwortliche eine Übermittlung personenbezogener Daten in Drittstaaten beabsichtigen, ist darüber ebenfalls zu informieren. Um diese Pflicht zu erfüllen, ist mitzuteilen, auf welcher besonderen Bedingung nach Art. 44 ff. DSGVO die Übermittlung beruht und welche Maßnahmen ergriffen wurden, um beim Empfänger ein angemessenes Datenschutzniveau herzustellen.

Nach Art. 13 Abs. 2 DSGVO muss der Verantwortliche dem Betroffenen darüber hinaus weitere Informationen mitteilen, die insbesondere notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) Dauer der Speicherung

Es ist konkret anzugeben, für wie lange personenbezogene Daten gespeichert werden. Nur ausnahmsweise, wenn die Angabe einer konkreten Zeitspanne dem Verantwortlichen nicht möglich ist, reichen Kriterien für die Festlegung der endgültigen Dauer der Speicherung aus.

b) Rechte der Betroffenen

Die Betroffenen sind auf ihre Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung sowie Datenübertragbarkeit hinzuweisen.

c) Widerrufbarkeit von Einwilligungen

Soweit die Verarbeitung auf einer Einwilligung des Betroffenen beruht, ist auch darauf gesondert hinzuweisen. Die entsprechende Informationspflicht ist nur erfüllt, wenn gleichzeitig darüber aufgeklärt wird, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt.

d) Beschwerderecht bei der Aufsichtsbehörde

Der Betroffene ist darüber aufzuklären, dass er sich gemäß Art. 77 DSGVO bei einer Aufsichtsbehörde beschweren kann, wenn er der Ansicht ist, dass die Verarbeitung seiner personenbezogenen Daten rechtswidrig erfolgt.

e) Verpflichtung zur Bereitstellung personenbezogener Daten

Der Verantwortliche muss den Betroffenen darüber informieren, ob die Bereitstellung seiner personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben, für einen Vertragsschluss erforderlich ist oder eine sonstige Verpflichtung besteht und welche Folgen eine Nichtbereitstellung hätte.

f) Automatisierte Entscheidungsfindung und Profiling

Sobald der Verantwortliche Verfahren der automatisierten Entscheidung nach Art. 22 DSGVO oder andere Profiling-Maßnahmen nach Art. 4 Nr. DSGVO durchführt, muss der Betroffene über die besondere Tragweite und die angestrebten Auswirkungen solcher Verfahren informiert werden. Diese Informationspflicht erstreckt sich auf Angaben zu der dazu verwendeten Logik oder des Algorithmus.

Schritt 5 Anpassung der Einwilligungserklärungen

Die Einwilligung des Betroffenen ist selbstverständlich nach wie vor eine Möglichkeit, um eine rechtmäßige Verarbeitung personenbezogener Daten zu gewährleisten. Die Einwilligung muss in erster Linie

- freiwillig,
- bestimmt,
- in informierter Weise,
- ausdrücklich und unmissverständlich

erklärt werden.

Wie eine rechtskonforme Einwilligungserklärung grundsätzlich auszusehen hat, beschreibt Art. 4 Nr. 11 DSGVO. Demnach sind die folgenden sieben Punkte besonders zu beachten.

1. Form der Einwilligung

Die Einwilligungserklärung bedarf nicht zwingend der Schriftform. Diese kann ebenfalls mündlich, elektronisch – aktives Setzen eines Hakens (opt-in) oder etwa in Textform erfolgen. Jede Form bringt jedoch eigene Vor- und Nachteile mit sich, insbesondere was die Nachweisbarkeit betrifft. Wichtig ist jedoch, dass die Einwilligungserklärung klar verständlich und eindeutig formuliert sein muss. Optisch muss die Einwilligungserklärung klar von anderen Sachverhalten abgegrenzt werden.

2. Informiertheit bei der Einwilligung

Der Betroffene muss klar erkennen können, worauf er sich einlässt. Der Betroffene muss also vor Erklärung der Einwilligung darüber informiert werden, auf welche konkreten personenbezogenen Daten sich die Einwilligung bezieht und was der vorgesehene Zweck der Erhebung, Verarbeitung oder Nutzung ist. Die Einwilligungserklärung muss ebenfalls zum Ausdruck bringen, ob die Daten gegebenenfalls an Dritte weitergegeben werden. Dieser Hinweis muss deutlich erfolgen und darf nicht versteckt oder unter erschwerten Bedingungen, etwa durch mehrfache Verweise, zugänglich sein.

3. Freiwilligkeit der Einwilligung

Die Einwilligung muss auf dem freien Willensentschluss des Betroffenen beruhen. Der Betroffene muss eine echte Wahlfreiheit haben und muss die Einwilligung ohne zu erleidende Nachteile verweigern können. Der Betroffene ist darauf hinzuweisen, dass die Einwilligung verweigert werden darf.

4. Bestimmtheit und Zweck in der Einwilligung

Aus der Erklärung muss eindeutig hervorgehen, wer genau welche Daten zu welchem konkreten Zweck erhebt, verarbeitet oder nutzt. Eine pauschale und generelle Erklärung ist nicht ausreichend. Eine Verwendung erhobener Daten zu anderen Zwecken, als in der Einwilligung angegeben, ist unzulässig.

5. Unmissverständlichkeit der Einwilligungserklärung

Dem Betroffenen muss bei Abgabe einer Einwilligungserklärung klar sein, dass es sich hierbei um eine solche handelt. Dies kann etwa dadurch erfolgen, dass die Erklärung die Überschrift „Einwilligung“ trägt oder der Inhalt wiedergibt, dass man etwas „zustimmt“ oder in etwas „einwilligt“.

6. Widerrufsmöglichkeit der Erklärung

Der Betroffene muss seine erklärte Einwilligung jederzeit widerrufen können. Dies ist in der Einwilligungserklärung klar zum Ausdruck zu bringen. Ein Widerrufsverzicht ist unzulässig. Der Widerruf muss dabei nicht zwingend in derselben Form der Einwilligung abgegeben werden. Entscheidend ist jedoch, dass die Erklärung des Widerrufs nicht schwieriger sein darf als die Erklärung der Einwilligung. Die Widerrufserklärung darf also keine zusätzlichen Hürden oder erschwerte Bedingungen mit sich bringen. Insbesondere sind Anschrift und Kontaktinformationen mitzuteilen, an welche der Widerruf zu adressieren ist.

Beispiel

Einwilligungserklärung zur Datenverarbeitung

Ich willige ein, dass die Stiftung XYZ die erhobenen Daten zu dem Zwecke der Aufnahme in Spenderdatei/Einladung zu Veranstaltung/Übersendung von Information über die Stiftung/…. verarbeitet.

[Ort, Datum] ……[Unterschrift des Betroffenen]

Widerspruchsrecht

Sie können jederzeit ohne Angabe von Gründen von Ihrem Widerspruchsrecht Gebrauch machen und die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen. Sie können den Widerruf entweder postalisch, per E-Mail oder per Fax an die Stiftung übermitteln.

Exkurs:

Gibt es besondere Anforderungen bei der Einwilligung von Kindern?

- Soweit es einer Einwilligung bedarf (s.o.), dann sieht das Gesetz grundsätzlich eine Altersgrenze von 16 Jahren vor, anderenfalls bedarf es einer Eltern Einwilligung der Eltern. Zudem bleiben die Regelungen zur Geschäftsfähigkeit unberührt.

Ist eine Einwilligung freiwillig, wenn die Gewährung einer Leistung davon abhängt?

- Oftmals machen Stiftungen die Gewährung einer Leistung von der Abgabe der Einwilligung abhängig. Auch in diesem Fall bleibt die Einwilligung freiwillig, wenn sie für die Gewährung der Leistung erforderlich ist.

Schritt 6: Überprüfung der Vereinbarungen zur Auftragsdatenverarbeitung

Gemäß Art. 28 Abs. 3 DSGVO muss die Stiftung in dem Fall, in dem sie personenbezogene Daten durch einen Dienstleister (z.B. Lohnabrechner, Mailingdienst, Homepageprovider) verarbeiten lässt, einen Vertrag über Auftragsdatenverarbeitung schließen. Es empfiehlt sich, alle von der Stiftung eingesetzten Dienstleister in einer Liste zusammenzufassen – dies zunächst unabhängig davon, ob sie personenbezogenen Daten verarbeiten oder nicht. Im nächsten Schritt hat die Stiftung zu prüfen,

- ob durch den Dienstleister personenbezogene Daten erhoben, genutzt, übermittelt oder verarbeitet werden,
- ob eine Vereinbarung zur Auftragsdatenverarbeitung erforderlich ist und
- ob diese bereits abgeschlossen wurde.

Im Anschluss kann die Stiftung prüfen, welche Verträge nach den Vorgaben der DSGVO angepasst bzw. geändert werden müssen.

Ein Muster für einen solchen Vertrag finden Sie hier:
www.lda.bayern.de/media/muster_adv.pdf

Schritt 7: Einführung eines Prozesses zur Erfüllung von Betroffenenrechten

Wie oben bereits dargestellt, fließen die Betroffenenrechte insbesondere in die Datenschutz- und die Eiwilligungserklärung ein. Die Betroffenen einer Datenverarbeitung haben folgende Rechte:

- Informationsrecht
- Auskunfts- und Widerspruchsrecht
- Recht auf Berichtigung, Löschung und Einschränkung
- Recht auf Datenübertragbarkeit

Mit der Datenschutz-Grundverordnung vervielfachen sich die von Verantwortlichen zu berücksichtigenden Pflichten in Bezug auf die Information von Betroffenen. Die Betroffenen sollen wissen, wer welche Daten zu welchem Zweck über sie erhebt und in die Lage versetzt werden, die Datenerhebung, -verarbeitung bzw. –nutzung zu prüfen.

Diese Anforderung kann nur dann erfüllt werden, wenn die verantwortliche Stiftung die Betroffenen ausreichend über die Datenverarbeitungsvorgänge informiert. Um die Betroffenen informieren zu können, müssen in der Stiftung wiederum die Sachverhalte ermittelt werden, in welchen Informationspflichten bestehen (beispielsweise Anmeldung zum Newsletter oder zu einer Veranstaltung, Spendeneinnahme etc.).

Des Weiteren sollte definiert werden, wie zu reagieren ist, falls ein Betroffener (Kunde, Interessent oder Mitarbeiter) von seinen Rechten Gebrauch macht: An wen und in welcher Frist soll die E-Mail, der Brief oder das Telefonat des Betroffenen weitergeleitet werden und wer ist für die Bearbeitung des Anliegens zuständig? Was ist dabei zu beachten (Stichwort: „Vertraulichkeit“)? Wer sind die Ansprechpartner für verschiedene Systeme, um beispielsweise die Löschung von Kundendaten überall im Unternehmen gewährleisten zu können (falls der Löschungsanspruch begründet ist)?

Weiterführende Hinweise:

Informationen zu den Anforderung der Datenschutzgrundverordnung und deren Umsetzung finden Sie auch unter nachfolgenden Links:

EU-Datenschutz-Grundverordnung: Das müssen Sie wissen
www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung

Broschüre der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=34

Mustervorlagen und Leitfäden
www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/EU-DSGVO/Datenschutzkonforme-Datenverarbeitung.html

Hinweisblatt zur Auftragsverarbeitung nach der EU-Datenschutz-Grundverordnung
www.lda.bayern.de/media/muster_adv.pdf

Muster einer Vereinbarung zur Auftragsverarbeitung
www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf