Vereinigung liechtensteinischer gemeinnütziger Stiftungen e. V. vlgs

BWB Rechtsanwälte AG Attorneys at Law Ltd

Merkblatt

zur Bedeutung der Datenschutzgrundverordnung (DSGVO)

für gemeinnützige Stiftungen

Stand: Mai 2018

1. Einleitung

In Liechtenstein wurde das noch geltende Datenschutzgesetz im Jahr 2002 eingeführt. Die DSGVO gibt dem Datenschutz eine ganz neue Bedeutung. Die DSGVO baut zwar auf dem bestehenden Recht auf, enthält aber auch einige wichtige Änderungen. Dies gilt für alle Unternehmen, die personenbezogene Daten verarbeiten und zwar für Konzerne wie auch für KMUs, in einem allerdings unterschiedlichen Ausmass.

Auch gemeinnützige Stiftungen fallen unter den Anwendungsbereich der DSGVO. Der Vereinigung liechtensteinischer gemeinnütziger Stiftungen e.V. (VLGS) ist die korrekte Handhabung der DSGVO ein grosses Anliegen. Deshalb wurde die BATLINER WANGER BATLINER Rechtsanwälte AG beauftragt, das vorliegende Merkblatt zu erstellen.

In diesem Merkblatt soll die DSGVO im Allgemeinen kurz dargestellt (siehe unten, 2.) und ihre Bedeutung für gemeinnützige Stiftungen erörtert (siehe unten, 3.) werden, ehe am Schluss der mögliche Handlungsbedarf aufgezeigt wird (siehe unten, 4.).

Die DSGVO ist sehr umfassend und komplex. Die Artikel-29-Datenschutzgruppe, der künftige Europäische Datenschutzausschuss, hat wichtige Leitlinien zur Anwendung der DSGVO in der Praxis erstellt.[1] Dieser Prozess ist noch nicht abgeschlossen. Der Datenschutzausschuss, der Ende Mai 2018 seine Tätigkeit aufnimmt, wird diese Arbeit fortsetzen. Aus diesen Gründen ist es nicht möglich, die Bedeutung aller Elemente der DSGVO im Rahmen eines Merkblattes darzulegen. Immerhin sollen die wichtigsten Aspekte im Allgemeinen und für gemeinnützige Stiftungen im Speziellen betont werden.

[1] Siehe http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936

2. Die DSGVO im Allgemeinen

Die DSGVO löst europaweit die bisher bestehende Datenschutzrichtlinie 1995/46/EG und damit das Datenschutzgesetz in Liechtenstein ab. Sie baut sehr stark auf dem bestehenden Recht auf und enthält aber auch wichtige Neuerungen.

Auf die Darstellung des bestehenden Rechts wird hier verzichtet, da eine Kenntnis des Datenschutzgesetzes, das am 1. August 2002 in Kraft getreten ist, vorausgesetzt wird.

Immerhin sei hier an die geltenden Grundsätze erinnert:

- Rechtmässigkeit der Datenverarbeitung
- Treu und Glauben
- Verhältnismässigkeit
- Zweckbestimmung
- Transparenz
- Datenrichtigkeit
- Datentransfer ins Ausland
- Datensicherheit
- Rechte wie das Auskunfts-, Widerspruchs- oder Berichtigungsrecht.

- Zudem müssen verpflichtend alle Unternehmen, die Daten verarbeiten, ihre Datensammlungen aufnehmen.

Weitere Informationen zum geltenden Recht können der Internetseite der liechtensteinischen Datenschutzstelle (DSS) entnommen werden (www.dss.llv.li).

Neu ist zum Beispiel der **extraterritoriale Ansatz**. Dies bedeutet, dass die DSGVO auch ausserhalb der EU massgebend ist, wenn Waren oder Dienstleistungen in der EU angeboten werden. Unter diesen Bedingungen gilt die DSGVO in Liechtenstein schon ab dem 25. Mai 2018. Die Übernahme in das EWR-Abkommen ist für Juli 2018 geplant. Ab diesem Datum wird die DSGVO auch für rein landesinterne Sachverhalte gelten.

Neu ist auch die Harmonisierung in der Rechtsanwendung. Dies bedeutet, dass grenzüberschreitende Fälle in Zukunft nicht mehr nur landesintern gelöst werden können. In Zukunft wird dem gegenüber der sogenannte **One Stop Shop** eingeführt. Dies bedeutet, dass eine betroffene Person mit Wohnsitz z.B. in Deutschland, Österreich oder Italien sich dort an ihre eigene Datenschutzbehörde wenden kann, wenn sie sich wegen eines Unternehmens in Liechtenstein beschweren will. Diese ausländische Datenschutzbehörde nimmt den Ball auf und nimmt dann Kontakt zur Datenschutzstelle in Vaduz auf. So muss zum Beispiel die italienische und die liechtensteinische Behörde darüber befinden, ob die DSGVO eingehalten wurde oder nicht. Dies ist ein zentraler Schritt in der Harmonisierung. Nationale Alleingänge werden somit nicht mehr möglich sein. Kommen diese beiden Behörden nicht zu einer gemeinsamen Schlussfolgerung, entscheidet inskünftig der europäische Datenschutz-

ausschuss. Dieser setzt sich aus den Datenschutzbehörden aller EWR Mitgliedstaaten zusammen (wobei noch nicht klar ist, ob die EFTA/EWR-Länder auch ein Stimmrecht bekommen).

Neu ist ebenfalls der drastisch erweiterte **Sanktionsrahmen**, der Bussen bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens vorsieht. Hierbei ist jedoch zu beachten, dass es sich hier um Maximalstrafen handelt. Die DSGVO erwähnt in diesem Rahmen aber auch explizit, dass Sanktionen verhältnismässig sein müssen.

Neu eingeführt wird ebenfalls eine **Rechenschaftspflicht**. Unternehmen sind somit verpflichtet, alle relevanten Entscheidungen in Bezug auf die Datenverarbeitung festzuhalten und begründet zu dokumentieren. Unternehmen müssen nachweisen können, dass sie den Aufgaben der DSGVO nachgekommen sind (Stichwort: Beweislastumkehr).

Eine weitere Neuigkeit besteht im **risikobasierten Ansatz**. Bisher waren Unternehmen verpflichtet, den Datenschutz überall einzuhalten. Dies führte zum Teil zu einer Bürokratisierung, die nun abgeschafft wird. Unternehmen sind vor allem dort gefordert, wo es um ein grosses Risiko für eine Persönlichkeitsverletzung geht. Dort sind spezifische Massnahmen zu treffen. Nach Erwägungsgrund 75 werden die Folgen eines Risikos zum Beispiel damit umschrieben, dass es zu einem materiellen oder immateriellen Schaden kommen kann insbesondere zu einer Diskriminierung, einem Identitätsdiebstahl, einem finanziellen Verlust, einer Rufschädigung oder wenn etwa Gesundheitsdaten oder Daten über politische, religiöse oder weltanschauliche Überzeugungen verarbeitet werden. Je nach Risiko ist eine Datenschutzfolgenabschätzung (DSFA) vorzunehmen und bei einer Datenpanne die Datenschutzbehörde oder die betroffenen Personen zu informieren (data breach notification).

Die **Datenschutzrechte** werden ausgebaut. Dies gilt vor allem für die Transparenz. Dazu wird ein neues Recht der Datenübertragbarkeit eingeführt.

Wichtig ist schliesslich der Umstand, dass in Zukunft der **Schutz juristischer Personen**, der bisher im DSG gegeben war wegfallen wird.

3. Auswirkungen für gemeinnützige Stiftungen

Auch gemeinnützige Stiftungen verarbeiten personenbezogene Daten, sei es, dass Daten von eigenen Stiftungsräten, Mitarbeitenden, Gesuchstellenden oder Kontaktpersonen bei Geschäftspartnern [2]oder Spendern oder anderen natürlichen Personen betroffen sind.

Eine Verarbeitung von Daten ist *jeder* Vorgang im Zusammenhang mit personenbezogenen Daten, wie bereits das Erheben. Damit reicht es aus, dass eine gemeinnützige Stiftung von einer natürlichen Person per Email, Briefpost oder telefonisch kontaktiert wird, z.B. um eine

[2] Siehe "Einstieg in die EU-Datenschutz-Grundverordnung FAQ", Frage 5: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-einstieg-faq.html#6

Unterstützung zu erhalten, um die Anwendbarkeit der DSGVO auszulösen. Damit ist jedoch noch nichts über das Ausmass der Anwendbarkeit gesagt. In diesem Zusammenhang kann auf das Merkblatt der Datenschutzstelle zu "Anforderungen der Datenschutz-Grundverordnung (DSGVO) an Kleinstunternehmen und kleine und mittlere Unternehmen (KMU) verwiesen werden (www.dss.llv.li).

Wenn zum Beispiel eine natürliche Person direkt betroffen ist, da eine Stiftung

- wissenschaftliche oder kulturelle Tätigkeiten gefördert oder ausgezeichnet
- Arbeiten aus verschiedenen Bereichen oder
- die Lebensqualität benachteiligter Menschen unterstützt

werden, ist der Anwendungsbereich der DSGVO gegeben. Die DSGVO ist dagegen nicht anwendbar, wenn eine andere Einrichtung unterstützt wird, oder wenn natürliche Personen zwar direkt unterstützt werden, diese ihren Wohnsitz aber ausserhalb der EU bzw. des EWR haben (z.B. in Südamerika oder Afrika).

Nach der DSGVO ist derjenige für deren Einhaltung verantwortlich, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies wird in aller Regel der Stiftungsrat sein. Es steht dem Stiftungsrat frei, Aufgaben, auch im Zusammenhang mit Datenschutz, z.B. an ein Mitglied des Stiftungsrates, den Treuhänder, das Treuhandbüro oder eine externe Fachperson zu delegieren. Die Letztverantwortlichkeit für die Einhaltung der Datenschutzgesetzgebung wird aber wohl bei der Stiftung bzw. beim Stiftungsrat verbleiben.

Daten sind neu verpflichtend zu löschen. Bei der Löschung kommt es darauf an, um was für Daten es geht. Es gelten allenfalls unterschiedliche Aufbewahrungsfristen.

4. Handlungsbedarf

Im Folgenden werden die wesentlichen Schritte zur Compliance mit der DSGVO beschrieben:

Schritt 1: Bestandsaufnahme und Erstellung eines Verarbeitungsverzeichnisses

Um personenbezogene Daten gemäss der DSGVO schützen zu können, muss zunächst ermittelt werden, in welchen Fällen personenbezogene Daten erhoben und verarbeitet werden. Sämtliche Prozesse der Stiftung, in denen personenbezogene Daten verarbeitet werden, sollten zunächst identifiziert werden.

Diese und weitere Informationen sind im Verarbeitungsverzeichnis zusammenzuführen, insbesondere Angaben zum Zweck jeder Verarbeitungstätigkeit, eine Beschreibung der betroffenen Datenkategorien, Personen, usw. Das Verarbeitungsverzeichnis ist sehr eng mit der Aufnahme der Datensammlungen gemäss bestehendem Recht verwandt. Ein Muster für ein Verarbeitungsverzeichnis kann zur Verfügung gestellt werden. Die

Datenschutzstelle hat ebenfalls ein Muster erstellt, das auf ihrer Internetseite verfügbar ist.[3]

Schritt 2: Prüfung der Rechtmässigkeitsgrundlagen und Anpassung der Einwilligungserklärungen

Für jeden Verarbeitungsprozess muss neu geprüft werden, ob eine Rechtsgrundlage besteht. Die Rechtsgrundlage ist neu aufzunehmen und im Verzeichnis festzuhalten. Eine Datenverarbeitung ist nur dann erlaubt, wenn sie sich auf eine Rechtsgrundlage abstützt. Dazu zählt insbesondere die rechtliche Verpflichtung nach Gesetz, ein Vertrag oder z.B. auch die Einwilligung. Die Einwilligung gilt als die schwächste Rechtsgrundlage, da sie jederzeit widerrufen werden kann. Das Vorhandensein der Einwilligung ist in Zukunft nachzuweisen. Die Einwilligung gilt als Rechtsgrundlage für den Versand von Newslettern oder Jahresberichten usw.

Schritt 3: Anpassung der Datenschutzerklärungen und der Informationspflichten

Die Transparenz wird in der DSGVO stärker betont als dies bisher der Fall war. So sind betroffene Personen, inklusive Mitarbeitende, im Voraus umfassend zu informieren. Dies hat insbesondere auf der Internetseite der Stiftung zu erfolgen. Die betroffenen Personen können auch direkt angeschrieben werden. Dies kann sehr aufwändig sein. Es empfiehlt sich in jedem Fall, Personen, die in Zukunft eine gemeinnützige Stiftung kontaktieren, zu informieren; sei es über die Internetseite oder einen Datenschutzhinweis am Ende eines Emails.

Schritt 4: Risikoabschätzung

Die DSGVO stellt neu im Wesentlichen darauf ab, ob ein Risiko oder gar ein hohes Risiko für die Verletzung von Rechten betroffener Personen besteht. Diese Risikoabschätzung ist eine Folge des risikobasierten Ansatzes.

Schritt 5: Überprüfung der Vereinbarungen zur Auftragsdatenverarbeitung

In Zukunft muss die Stiftung in dem Fall, in dem sie personenbezogene Daten durch einen Auftragsverarbeiter verarbeiten lässt (z.B. Lohnabrechner, Mailingdienst, Homepageprovider), einen Vertrag über Auftragsdatenverarbeitung schliessen. Dazu bietet es sich an, alle Partner der Stiftung zu erfassen und dann zu überlegen, ob es sich um Auftragsverarbeiter handelt.

Schritt 6: Einführung eines Prozesses zur Erfüllung von betroffenen Rechten

Die Rechte von Betroffenen werden gestärkt. Die Grundidee der DSGVO besteht darin, den Betroffenen ihre Rechte zurück zu geben, die sie aufgrund der zunehmenden Möglichkeiten auf dem Internet inzwischen praktisch verloren haben. Diesen Rechten misst die DSGVO eine zentrale Bedeutung zu, weshalb sich die Einführung eines Prozesses zur Erfüllung solcher Rechte sehr stark empfiehlt. So muss bei der Wahrnehmung von Rechten unverzüglich, in jedem Fall aber innerhalb eines Monats reagiert werden können.

[3] Siehe https://www.llv.li/files/dss/datenschutzerklarung-muster.pdf

Schritt 7: Prüfung der Frage, ob ein Datenschutzbeauftragter zu benennen ist
Ein solcher ist insbesondere zu benennen, wenn die Kerntätigkeit der Stiftung in einer umfangreichen Datenverarbeitung besteht (die Verarbeitung von Mitarbeiterdaten zur Lohnauszahlung ist eine Nebentätigkeit).

Schritt 8: Schulung und Verpflichtung von Mitarbeitern
Mitarbeiter einer gemeinnützigen Stiftung sollten geschult werden. Sie sollten auch zur Einhaltung der DSGVO verpflichtet werden. Das Ganze wird durch ein umfassendes Datenschutzreglement abgerundet.

Schritt 9: Datensicherheit
Die DSGVO erhöht die Anforderungen an die Datensicherheit.

Weitere Informationen zum Datenschutz bei Stiftungen können dem Papier "Das neue Datenschutzrecht – Das müssen Sie jetzt tun" des Bundesverbands Deutscher Stiftungen entnommen werden, welches bei der VLGS erhältlich ist.

BWB Rechtsanwälte AG
Attorneys at Law Ltd

Am Schrägen Weg 2 | 9490 Vaduz | Liechtenstein
T +423 239 78 78 | F +423 239 78 79 | www.bwb.li

Vereinigung liechtensteinischer gemeinnütziger Stiftungen e. V. vlgs

Aeulestrasse 6 | Postfach 882 | LI-9490 Vaduz
Tel +423 399 19 11 | info@vlgs.li | www.vlgs.li