

per Mail: danielle.schneider@bj.admin.ch / jonas.amstutz@bj.admin.ch

Frau Bundesrätin
Karin Keller Sutter
Eidgenössisches Justiz- und Polizeidepartement
CH-3003 Bern

Basel, 6. Oktober 2021

Vernehmlassung zum Vorentwurf zur Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

Sehr geehrte Frau Bundesrätin

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz, vertritt gesamtschweizerisch die Interessen *gemeinnütziger Stiftungen und Vereine* aller Tätigkeits- und Finanzierungsformen. Dem Gemeinnützigkeitswesen kommt in der Schweiz eine sehr grosse Bedeutung zu. Die über 13'000 gemeinnützigen Stiftungen und die zahlreichen gemeinnützigen Vereine üben im Interesse und zum Wohl der Allgemeinheit wichtige Funktionen aus, etwa in den Bereichen Soziales, Gesundheitswesen, Forschung und Wissenschaft, Bildung und Erziehung, Jugendförderung, Kunst, Kultur, Entwicklungszusammenarbeit etc.

Gerne machen wir von der Möglichkeit Gebrauch, zum Vorentwurf der Verordnung zum Bundesgesetz über den Datenschutz (VE-VDSG) eine Vernehmlassung einzureichen.

Vorbemerkung

Zahlreiche gemeinnützige Stiftungen und Vereine werden vom totalrevidierten Datenschutzgesetz und entsprechend von der Verordnung betroffen sein. Im Vordergrund stehen namentlich Aktivitäten im Zusammenhang mit dem Fund-raising (Spenderdaten) sowie die Förderung (Daten von Destinatären) und – für Vereine – den Mitgliederdaten. In diesen Bereichen werden Personendaten bearbeitet.

Beim Gros der gemeinnützigen Stiftungen und Vereine handelt es sich um kleinere und mittlere Organisationen ohne nennenswerte Personalressourcen. Nach wie vor ist die Ehrenamtlichkeit, d. h. unentgeltliches Engagement, weit verbreitet, namentlich in den Leitungsgremien (Stiftungsrat und Vereinsvorstand). Der Grossteil der gemeinnützigen Stiftungen und Vereine verfügt auch über sehr begrenzte finanzielle

Mittel. Deshalb ist es erforderlich, dass die Umsetzung des Datenschutzgesetzes auch für solche Organisationen machbar bleibt.

Zu den einzelnen Bestimmungen in dem VE-VDSG (Auswahl)

Zu Art. 1

Die Angemessenheit der Massnahme ist nicht nur nach den Implementierungskosten (Art. 1 lit. d VE-VDSG), sondern auch nach dem sonstigen Implementierungsaufwand zu beurteilen. Hierzu sind sämtliche Aufwendungen zu berücksichtigen, wie auch personelle Aufwendungen, deren Kosten nicht ausschliesslich der Implementierung hinzugerechnet werden können.

Die Ausführungen im erläuternden Bericht sind widersprüchlich, wenn ausgeführt wird, dass der Verantwortliche oder Auftragsbearbeiter sich nicht von der Pflicht einer angemessenen Datensicherheit mit dem Verweis auf übermässige Kosten befreien könne, die Implementierungskosten aber zu berücksichtigen sind. Offenkundig sind die Kosten als Kriterium der Angemessenheit heranzuziehen.

Gerade bei kleineren und mittleren Stiftungen und Vereinen ist es existenziell, dass sämtliche Aufwendungen, die im Zusammenhang mit der Sicherstellung der Datensicherheit getätigt werden, für die Beurteilung der Angemessenheit der Datensicherheit berücksichtigt werden. Ziel des Heranziehens des Kostenaspekts ist es ja nicht, sich den datenschutzrechtlichen Anforderungen zu entziehen, sondern diese für kleinere und mittlere Organisationen auch tatsächlich umsetzbar zu machen. Hier ist also behördliches Augenmass gefragt. Die Bestimmung ist zu präzisieren.

Zu Art. 4

Das Erstellen eines Bearbeitungsreglements, wenn umfangreiche besonders schützenswerte Daten bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird, ist gesetzlich nicht vorgesehen. Für diese zusätzliche, nicht unbedeutende Pflicht fehlt es somit an einer gesetzlichen Grundlage.

Eine Vielzahl gemeinnütziger Stiftungen und Vereine bearbeiten besonders schützenswerte Daten, sei dies namentlich im Sozial-, Gesundheits- oder im Wissenschaftsbereich. Es ist nicht einzusehen, weshalb diese Organisationen nun durch die Hintertür mit einer Anmeldepflicht einer Datensammlung konfrontiert werden, obwohl der Gesetzgeber diese Anmeldepflicht durch das Führen eines Bearbeitungsverzeichnisses ersetzt hat. Der Umstand, dass Art. 11a DSG keinen Einzug in das neue DSG (nDSG) gefunden hat, ist ja auch dem erläuternden Bericht zu entnehmen. Umso unverständlicher ist der vorliegende Versuch, dies wiedereinzuführen. Die Bestimmung ist daher zu streichen.

Zu Art. 6

Art. 6 Abs. 1 VE-VDSG sieht vor, dass der Verantwortliche bei einer Datenbearbeitung durch einen Auftragsbearbeiter sicherstellen muss, dass die Daten vertrags- oder gesetzesgemäss bearbeitet werden.

Dazu muss es genügen, wenn der Verantwortliche dem Auftragsbearbeiter die gesetzlichen Pflichten vertraglich überbindet und ihn damit zu einer gesetzeskonformen Datenbearbeitung anhält.

Gerade kleinere und mittlere Stiftungen, Vereine und NPO geben gewisse Datenbearbeitungen extern (bspw. im Rahmen des Fundraising). Diese haben in aller Regel weder die Möglichkeit noch die Ressourcen eine umfassende Kontrolle vorzunehmen. Daher ist vorzusehen, dass der Verantwortliche die Auftragsbearbeitung vertraglich so auszugestalten hat, dass sie gesetzeskonform ist.

Zu Art. 13

Vorneweg ist festzuhalten, dass die Informationspflicht nach Art. 19 nDSG dem Verantwortlichen auferlegt ist. Auf welcher Grundlage der VE-VDSG nun auch für den Auftragsbearbeiter eine solche Pflicht begründen will, ist nicht ersichtlich. Es fehlt an einer gesetzlichen Grundlage. Die Bestimmung ist entsprechend zu korrigieren, d.h. die Pflicht für den Auftragsbearbeiter zu streichen.

Gemäss dem erläuternden Bericht muss die Information stets auf der ersten Kommunikationsstufe erfolgen. Was damit genau gemeint ist, ist dem Bericht nicht zu entnehmen. Reicht der Verweis auf der Entry Page auf eine Datenschutzerklärung?

Auch ist nicht klar, was damit gemeint ist, dass es "eine gute Praxis wäre", wenn alle Informationen auf "einen Blick verfügbar" wären. Ist das eine gestalterische Vorgabe? Muss ein Inhaltsverzeichnis erstellt werden?

Die Ausführungen im erläuternden Bericht sind insbesondere dann gänzlich unklar, wenn der Verantwortliche nicht im digitalen Bereich seiner Informationspflicht nachzukommen hat. Muss bei einer Anfrage am Telefon einer gemeinnützigen Organisation die u.U. mehrseitige Datenschutzerklärung vorgelesen werden? Muss im Rahmen des Fundraising bei jedem ersten Briefkontakt die Datenschutzerklärung mitgesendet werden? Dies wäre klar unverhältnismässig!

Leider verpasst es der VE-VDSG und der erläuternde Bericht, hier Klarheit zu schaffen. proFonds vertritt die Ansicht, dass es genügen muss, wenn der Datenbearbeiter über seine Website seiner Informationspflicht nachkommt. Es ist zumutbar, dass sich Betroffene (gegebenenfalls nach einem ausdrücklichen Verweis auf die Website) dort informieren.

Die Regelung in Art. 13 VE-VDSG ist nach dem Gesagten unklar. Durch die unpräzise Formulierung schafft diese Bestimmung Rechtsunsicherheiten. Es wäre zu wünschen, dass sich der Ordnungsgeber den praktischen Bedürfnissen der Verantwortlichen und der Betroffenen annimmt und einen praktikablen Umgang vorsieht.

Zu Art. 15

Vorneweg ist festzuhalten, dass auch in Art. 15 VE-VDSG neben den Verantwortlichen wiederum die Auftragsbearbeiter verpflichtet werden sollen. Diese haben aber keine Informationspflicht.

Des Weiteren fehlt es auch dieser weitergehenden Pflicht an einer gesetzlichen Grundlage. Sie ist auch nicht umsetzbar. Der Verantwortliche wird ohne unverhältnismässigen Aufwand nicht ununterbrochen über die Aktualität, Zuverlässigkeit und

Vollständigkeit informieren können. Diese zusätzliche Regelung ist auch nicht notwendig.

Im Gegenteil: Es gelten die Grundsätze nach Art. 6 nDSG. Gemäss Art. 6 Abs. 5 nDSG muss sich der Datenbearbeiter über die Richtigkeit der von ihm bearbeiteten Daten vergewissern. Dies umfasst bereits eine Prüfung der Aktualität und Vollständigkeit und mit der Sicherstellung der Richtigkeit der Daten sind diese auch zuverlässig. Die Interessen des Betroffenen sind damit ausreichend geschützt. Er darf gestützt auf Art. 6 nDSG davon ausgehen, dass die über ihn erhobenen Daten korrekt sind. Eine zusätzliche Informationspflicht geht über die gesetzlichen Anforderungen hinaus und plustert den ohnehin reichhaltigen Pflichtenkatalog nur unnötig auf.

Art. 15 VE-VDSG ist aus diesem Grund ersatzlos zu streichen.

Zu Art. 16

Art. 16 VE-VDSG entspricht Art. 19 lit. b VE-DSG. Dieser wurde nach der Vernehmlassung gestrichen. Entsprechend kann es nicht sein, dass diese Pflicht nun auf Verordnungsebene wiedereingeführt wird. Der Wille des Gesetzgebers ist zu respektieren und Art. 16 VE-VDSG ist ersatzlos zu streichen.

Zu Art. 18

Die Datenschutz-Folgenabschätzung sollte mit Blick auf die strenge bundesverwaltungsgerichtliche Auslegung des Begriffs der Schriftlichkeit gemäss Art. 14 OR (BVerwGer A-3548/2018 vom 19. März 201, E. 4.8) nicht "schriftlich" festgehalten werden. Vielmehr sollte der Nachweis durch Text genügen.

Zu Art. 19

Art. 19 Abs. 5 VE-VDSG stipuliert die Dokumentationspflicht von Datenschutzverletzungen. Die Anforderung, wonach "alle mit den Vorfällen zusammenhängenden Tatsachen" dokumentiert werden müssen, ist gerade für mittlere und kleinere Stiftungen, Vereine und NPO nicht umsetzbar. Diese Pflicht geht viel zu weit und generiert einen unverhältnismässigen Aufwand.

Des Weiteren ist die Aufbewahrungsfrist – im Gleichlauf zu Art. 18 VE-VDSG – auf zwei Jahre zu reduzieren.

Zu Art. 20

Die Erteilung der angeforderten Auskunft sollte in irgendeiner Textform (also auch digital) möglich sein. Das Schriftlichkeitserfordernis geht zu weit und ist auch nicht praktikabel.

Für die Frage, ob die Auskunft für die betroffene Person verständlich ist (Art. 20 Abs. 3 VE-VDSG), ist ein objektivierter Massstab heranzuziehen. Persönliches Unvermögen der betroffenen Person darf nicht zur Annahme einer Pflichtverletzung des Verantwortlichen führen. Des Weiteren ist auch hier die Aufbewahrungsfrist – im Gleichlauf zu Art. 18 VE-VDSG – auf zwei Jahre zu reduzieren.

Zu Art. 26

proFonds begrüsst ausdrücklich die Regelung in Art. 26 VE-VDSG, wonach eine privatrechtliche Organisation, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigt, von der Pflicht befreit ist, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, es sei denn, es werden umfangreich besonders schützenswerte Personendaten bearbeitet oder es wird ein Profiling mit hohem Risiko durchgeführt.

Stiftungen unterstehen der Revisionspflicht (Art. 83b ZGB). In Übereinstimmung mit Art. 727 OR, wonach eine ordentliche Revision vorzunehmen ist, wenn in zwei aufeinander folgenden Geschäftsjahren 250 Vollzeitstellen im Jahresdurchschnitt überschritten werden, sollte in Art. 26 VE-VDSG ebenfalls auf 250 Vollzeitstellen im Jahresdurchschnitt abgestellt werden. Damit sind Stiftungen und Vereine, die aufgrund ihrer Mitarbeiteranzahl zur ordentlichen Revision verpflichtet sind, auch zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Damit wird eine gesetzliche Kohärenz geschaffen.

Zusammenfassende Betrachtung

Es ist Sache der VDSG, die datenschutzrechtlichen Anforderungen gemäss dem neuen Gesetz so zu präzisieren, dass sie einerseits praktikabel und umsetzbar sind, andererseits aber auch dem gesetzgeberischen Willen entsprechen. Diesen Spagat schafft die VDSG an zahlreichen Stellen nicht.

Wir danken Ihnen für die aufmerksame Prüfung unserer Standpunkte. Wir hoffen, dass unsere Vorschläge bei der weiteren Bearbeitung der Vorlage Berücksichtigung finden. Für eine Vertiefung spezifischer Fragen steht proFonds jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen

proFonds, Dachverband gemeinnütziger Stiftungen der Schweiz



Dr. Christoph Degen
Geschäftsführer



Sebastian Rieger
Recht und Steuern