EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Eidgenössisches Justiz- und Polizeidepartement EJPD
Karin Keller-Sutter
Bundeshaus West
3003 Bern

Zustellung per E-Mail an: jonas.amstutz@bj.admin.ch

Zürich, 14. Oktober 2021

Stellungnahme zum Verordnungsentwurf zum Bundesgesetz über den Datenschutz (E-VDSG)

Sehr geehrte Frau Bundesrätin,
sehr geehrte Damen und Herren

Im Rahmen der laufenden Anhörung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (E-VDSG), welche am 23. Juni 2021 vom Bundesrat in die Vernehmlassung geschickt worden ist, möchten wir gerne die Gelegenheit nutzen, zur Vorlage Stellung zu nehmen.

I. Einleitung

EXPERTsuisse – der Schweizer Expertenverband für Wirtschaftsprüfung, Steuern und Treuhand – engagiert sich aktiv für seine rund 10'000 Einzelmitglieder und über 800 Mitgliedunternehmen (mit gut 19'000 Mitarbeitenden) sowie für einen starken Wirtschaftsstandort Schweiz. Die Mitgliedunternehmen von EXPERTsuisse betreuen den Grossteil der Schweizer Wirtschaft.

EXPERTsuisse setzt sich im Digitalisierungszeitalter für einen modernen, zeitgemässen Datenschutz ein, analog der DSGVO, damit Schweizer Recht international anerkannt und insbesondere seitens der EU als äquivalent eingestuft wird. Gleichzeit sollen Innovationen nicht behindert werden.

EXPERTsuisse hat im April 2017 eine Stellungnahme zum Vernehmlassungsentwurf des Bundesgesetzes über den Datenschutz (E-DSG) eingereicht und hatte bereits damals darauf hingewiesen, dass das neue Datenschutzrecht der Schweiz den Vorgaben auf EU-Ebene entsprechen muss, ohne über diese Vorgaben hinauszugehen.

II. Zusammenfassung

Mit der Zunahme digitaler Technologien sind auch die Anforderungen an den Datenschutz gestiegen. Das übergeordnete Ziel ist, die Persönlichkeit und die Freiheiten von Datensubjekten zu schützen. In Anbetracht der europäischen Entwicklungen musste auch die Schweiz ihr Datenschutzrecht revidieren. Dies einerseits, um den internationalen Erwartungen gemäss der künftigen revidierten Europaratskonvention 108 zu genügen und andererseits, um die für die Wirtschaft sehr wichtige Äquivalenz mit der EU-DSGVO zu bewahren. Eng damit verknüpft ist die ePrivacy-Verordnung, die ebenfalls von der EU verabschiedet wurde.

Der Beitritt zur modernisierten Datenschutzkonvention des Europarates hat für die Schweiz sowohl in Bezug auf den Schutz der Privatsphäre als auch für den internationalen Datenverkehr grosse Bedeutung. Die Revision wurde in der Herbstsession 2020 in der Schlussabstimmung angenommen, was den Weg frei macht für die Bewahrung der Anerkennung der Äquivalenz durch die EU. Der Äquivalenzentscheid durch die EU ist jedoch noch hängig.

Der E-VDSG enthält einige verschärfte Bestimmungen, für die gemäss Gesetz keine Grundlage besteht. Dadurch erscheint die Verordnung in gewissen Punkten wie ein Regelwerk mit materiell zusätzlichen Bestimmungen. Dies zeigt sich in dem Verordnungs-Entwurf als auch im Erläuterungsbericht.

Auf zu detaillierte Bestimmungen, die über das Niveau der DSGVO gehen, ist aus wirtschaftsliberaler Sicht zu verzichten. Der Entwurf muss unter der Berücksichtigung des revDSG und der politisch intensiv geführten Diskussionen unbedingt nachgebessert werden.

III. Vorschläge zur Überarbeitung der E-VDSG

In der heutigen digitalisierten Welt muss eine Balance gefunden werden zwischen angemessenem Datenschutz und der Wirtschaftlichkeit. Mit dem revDSG konnte ein modernes Gesetz geschaffen werden, das den aktuellen Anforderungen, mit Blick auf die internationale Ebene, gerecht wird. Insbesondere die Annäherung an die DSGVO der EU macht die Regulierung gut umsetzbar als auch kompatibel mit internationalen Normen.

In der E-VDSG sind zahlreiche Erweiterungen enthalten, die für die Wirtschaft, insbesondere für KMU, einen administrativen Mehraufwand bedeuten. Gewisse Regelungen, welche bereits im politischen Prozess bei der DSG-Revision abgelehnt wurden, wurden nun in der E-VDSG wieder aufgenommen. Zu erwähnen ist hier z.B. die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren (wurde vom Parlament gestrichen). Es ist zu vermuten, dass gerade KMU solche Anforderungen nur mit einem grossen Mehraufwand umsetzen können bzw. die Ressourcen dafür nicht zur Verfügung stehen (Konflikt mit Art. 60ff. revDSG - Strafbestimmungen).

Sinn und Zweck einer Ausführungsverordnung ist es, Gesetzesbestimmungen durch Details genauer zu beschreiben, so dass die Umsetzung des revDSG erleichtert werden sollte. Neue Normen dürfen jedoch nicht geschaffen werden.

Folgendes gilt es im Generellen zu beachten:

- Eine Überarbeitung und Verbindung zum revDSG erscheint zwingend notwendig zur Verhinderung von Swiss Finishes. Auf Einschränkungen, die nicht explizit auf Gesetzesstufe erwähnt sind und über das Niveau der DSGVO hinausgehen, ist zu verzichten. Verschärfungen im Vergleich zum EU-Standards bedeuten für die Wirtschaft zwei unterschiedliche Regelungen und Mehraufwände in der praktischen Umsetzung.
- Widersprüche zum revDSG sind grundsätzlich zu beheben und es wäre sinnvoll, bei einzelnen Verordnungsbestimmungen jeweils auf den Artikel der revDSG zu verweisen.
- Diskussionen, die im politischen Prozess zum revDSG bereits abgewiesen wurden, dürfen nicht auf dem Verordnungsweg wieder eingeführt werden.
- Aufgrund der kurzen Frist schlagen wir eine Übergangsfrist von 1 Jahr vor ab Inkrafttreten des revDSG. Es ist fragwürdig, ob die Wirtschaft ihre Compliance-Projekte rechtzeitig vorantreiben und abschliessen kann.

Konkrete (nicht abschliessende) Aspekte, die wir zur Überarbeitung vorschlagen:

- Grundsätze Art 1, Abs. 2 E-VDSG: Steigt das Risiko für die Rechte der Betroffenen, so soll die Prüfung der Massnahmen regelmässig stattfinden. Ab einem gewissen Risiko empfehlen wir, die Prüfung zu standardisieren (z.B. mittels ISO 27001 als Pflicht). Diese internationale Norm zeigt auf, dass eine Organisation Best-Practice-Prozesse zur Informationssicherheit definiert und umgesetzt hat.

- Schutzziele Art. 2 E-VDSG: Es ist nicht zwingend jedes dieser Schutzziele relevant, jedoch muss begründet werden können, warum nicht. Die Auflistung der Schutzziele sollte durch die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ersetzt werden. Dann wäre die Liste identisch mit Art. 32, Abs. 1 lit. b DSGVO.
- Protokollierung Art. 3 E-VDSG: Der gesamte Artikel soll ersatzlos gestrichen werden aufgrund der fehlenden gesetzlichen Grundlage. Im politischen Prozess hatte das Parlament bereits auf eine Protokollierungspflicht verzichtet.
- Art. 3, Abs. 1 E-VDSG: Das Ergebnis der DSFA ist kein geeigneter Indikator für das Risiko einer Verletzung der Datensicherheit. In den meisten Fällen wird eine DSFA nicht wegen mangelhafter Datensicherheit ein hohes Risiko ausweisen, sondern aufgrund der Art und Weise der Datenverarbeitung. Dies hat jedoch mit Datensicherheit nichts zu tun.
- Bearbeitungsreglement von privaten Personen: Art. 4 E-VDSG: Es fehlt eine gesetzliche Grundlage. Eine Einführung mittels Verordnung ist daher nicht möglich und es ist auch redundant, da die Informationen entweder in einer DSFA oder dann im Verzeichnis der Bearbeitungstätigkeiten enthalten sein werden.
- Modalitäten Art. 6, Abs 2 E-VDSG: Der Sinn und Zweck dieser Bestimmung erscheint unklar, da die Regelung bereits durch die Art. 16 und 17 revDSG abgedeckt ist (Bekanntgabe von Personendaten ins Ausland).
- Beurteilung der Angemessenheit des Datenschutzes eines ausländischen Staates oder eines internat. Organs: Art. 8, Abs 1, 3 E-VDSG braucht eine Präzisierung und könnte falsch verstanden werden. Der Bundesrat muss die Angemessenheit des Datenschutzes in einem Empfängerstaat feststellen (und nicht die verantwortliche Stelle).
- Datenschutzklauseln und spezifische Garantien Art 9. E-VDSG: Die gestellten Anforderungen erreichen ein Detailierungsgrad, der die Komplexität der Datenbearbeitung ineffizient gestaltet. Aus Sicht des Datenschutzes ist diese Regelung zur Erreichung des Datenschutzes zwar konsequent, doch verursacht hohe Aufwände für die Betriebe. Aus diesen Gründen empfehlen wir diese Anforderung auf das Minimum zu reduzieren.
- Verbindliche unternehmensinterne Datenschutzvorschriften Art. 11, Abs. 2: der Artikel geht weniger weit als Art. 47 DSGVO. Die bisherigen Binding Corporate Rules (BCR) wurden regelmässig so formuliert, dass diese auch EU-konform sind.
- Modalitäten der Informationspflichten: Art. 13 E-VDSG beschreibt, dass die Information über die Beschaffung von Personendaten in exakter, verständlicher und leicht zugänglicher Art kommuniziert werden soll. Werden Piktogramme verwendet, müssen diese maschinenlesbar sein. Letzteres soll gemäss dem Erläuterungsbericht einen Vergleich verschiedener Dokumente und allgemein eine gewisse Automatisierung ermöglichen. Es

stellt sich hier die Frage, wie weit dies ein Ziel des Datenschutzes ist. Wir stellen uns ausserdem die Frage, welches die gesetzliche Grundlage ist für diese Bestimmung. Art. 13 Abs. 1 E-VDSG sieht zudem vor, dass der Verantwortliche und der Auftragsbearbeiter die Information über die Beschaffung mitteilen. Das scheint dem Auftragsbearbeiter tatsächlich eine Informationspflicht gegenüber betroffenen Personen aufzuerlegen, was weder im Gesetz (Art. 19 revDSG) vorgesehen noch praktikabel ist. Es ist die Verantwortung des Verantwortlichen, betroffene Personen zu informieren und diese darf nicht auf dem Wege der Verordnung auf den Auftragsbearbeiter ausgedehnt werden. Das könnte auch in der Praxis zu Problemen führen. Zudem sollte man "mitteilen" umformulieren, es geht um die Informationspflicht (die passiv sein kann), nicht eine Mitteilungspflicht (die aktives Handeln min. impliziert).

- Für die «Information bei der Bekanntgabe von Personendaten» gemäss Art. 15 E-VDSG existiert keine gesetzliche Grundlage. Dies ist ein reiner Swiss Finish, der nach EU-Recht, zumindest für private Datenanbieter, nicht vorgeschrieben ist und wirkt und praxisfremd.
- Die in Art. 16 E-VDSG vorgesehene Pflicht des Verantwortlichen, die Empfänger über die Berichtigung, Löschung oder Vernichtung der Bearbeitung von Personendaten zu informieren, wurde vom Parlament bereits im Entwurf des revDSG gestrichen.
- Meldung von Verletzungen der Datensicherheit, Art. 19, Abs. 5: gemäss der DSGVO ist eine Dokumentation vorgesehen, nicht jedoch gemäss revDSG. Selbst die Botschaft zum revDSG sah keine Dokumentationspflicht vor**.** Eine Einführung mittels Verordnung ist daher nicht möglich.
- Modalitäten Art. 20, Abs. 5: Das revDSG sieht keine Dokumentation dieser Art vor. Eine Dokumentationspflicht ist aus diesem Grund zu streichen.
- Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten- Art. 26 E-VDSG: Die Voraussetzungen für die Ausnahme von der Befreiung von der Pflicht zur Führung eines Bearbeitungsverzeichnisses für KMU in Art. 26 E-VDSG ist unpräzis, insbesondere diejenige der "umfangreichen" Bearbeitung von besonders schützenswerten Personendaten. Da schwierig zu beurteilen ist was umfangreich bedeutet, kann dies unter Umständen auch bei KMU schnell vorliegen, insbesondere im Bereich der Bearbeitung von Personalinformationen. Ausserdem ist nicht klar, ob das Bearbeitungsverzeichnis dann nur für diese Bearbeitungen erstellt werden muss oder sich die Pflicht dann auf alle Bearbeitungen bezieht. Dies kann für KMU einen grossen Unterschied ausmachen. Die Anforderungen sind zu präzisieren und die Folgen der Pflicht klarzustellen.

Diese Vernehmlassung wurde in Abstimmung mit anderen Wirtschaftsverbänden erarbeitet. Wir gehen davon aus, dass im Anschluss an das Vernehmlassungsverfahren, das bis zum 14. Oktober dauert, noch Anpassungen der E-VDSG erfolgen werden.

Wie bereits erwähnt, erscheint uns die vorliegende Version als zu restriktiv (unnötige Swiss Finishes generieren keinen Mehrwert). Unternehmen, die bereits die DSGVO- Vorgaben eingeführt haben, werden keine Mühe bekunden bei der Umsetzung des revDSG.

Wir danken Ihnen für die Prüfung und Berücksichtigung unserer Anliegen. Für allfällige Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

EXPERTsuisse

Sergio Ceresola
Ressortleitung Regulatorisches & Fachliches
Mitglied der Geschäftsleitung

Markus Braun
Fachprojektleiter Governance & Regulation