Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht

31. August 2022

Verordnung über Datenschutzzertifizierungen (VDSZ)

Erläuternder Bericht

BJ-D-598A3401/103

Inhaltsverzeichnis

1 Ausgangslage

1.1 Kontext

Aufgrund einer Evaluation des Bundesgesetzes vom 19. Juni 1992[1] über den Datenschutz (DSG) und mit Blick auf die technologischen Entwicklungen und das weiterentwickelte europäische Recht beschloss der Bundesrat, das Datenschutzrecht teilweise zu revidieren. Am 15. September 2017 verabschiedete er die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz[2]. Die Vorlage umfasst einerseits eine Totalrevision des DSG und andererseits eine Teilrevision weiterer Bundesgesetze, womit insbesondere die Richtlinie (EU) 2016/680[3] umgesetzt werden soll. Das Parlament hat die Vorlage des Bundesrates in zwei Etappen aufgeteilt. In der ersten Etappe wurde nur die Schengen-relevante Richtlinie (EU) 2016/680 zum Datenschutz in Strafsachen umgesetzt. Das Bundesgesetz vom 28. September 2018[4] über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (SDSG) ist am 1. März 2019 in Kraft getreten. In einer zweiten Etappe hat das Parlament das neue Datenschutzgesetz (nDSG) beraten und am 25. September 2020 verabschiedet[5].

Als Folge der Totalrevision des DSG müssen auch die dazugehörigen Verordnungen, namentlich die Verordnung zum Bundesgesetz über den Datenschutz (VDSG)[6] und die Verordnung über die Datenschutzzertifizierungen (VDSZ)[7] angepasst werden.

1.2 Änderungen des nDSG im Bereich der Zertifizierung

Artikel 13 nDSG betreffend die Zertifizierung übernimmt Artikel 11 DSG, wobei neu auch Produkte und Dienstleistungen als zertifizierbar erwähnt sind. Tatsächlich ist in materieller Hinsicht nur die Einführung von «Dienstleistungen» neu, da die «Produkte» im aktuellen Recht bereits mit der Verordnung vom 28. September 2007 erfasst werden. Wie bereits im geltenden Recht beauftragt Absatz 2 den Bundesrat zum Erlass von Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens, wobei er das internationale Recht und die international anerkannten technischen Normen berücksichtigt. Überdies kann der private Verantwortliche gestützt auf Artikel 22 Absatz 5 nDSG von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist. Bei Vorliegen einer Zertifizierung erlaubt die «allgemeine» Verordnung zum Datenschutzgesetz in ihrer neuen Version sodann die Bekanntgabe von Personendaten ins Ausland (siehe in diesem Sinn Art. 12 der neuen Verordnung, der sich auf Art. 16 Abs. 3 nDSG stützt).

---

1 SR **235.1**

2 BBl **2017** 6941

3 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016, S. 89.

4 SR **235.3**

5 BBl **2020** 7639

6 SR **235.11**

7 SR **235.13**

1.3 Verfassungsmässigkeit und Vereinbarkeit mit internationalen Verpflichtungen

Die Verordnung über die Datenschutzzertifizierungen ist eine Ausführungsverordnung zum Datenschutzgesetz, das am 25. September 2020 vom Parlament revidiert wurde. Sie erfüllt den dem Bundesrat in Artikel 13 Absatz 2 nDSG erteilten Auftrag. In diesem Sinn entspricht sie dem Gesetz und es kann hinsichtlich der rechtlichen Aspekte auf die Erläuterungen in der Botschaft verwiesen werden (siehe BBl *2017* 6941, insbesondere 7184 ff.).

2 Grundzüge der Vorlage

Die zentralen Neuerungen der neuen VDSZ betreffen verschiedene Punkte. Zunächst waren Vereinfachungen und Vereinheitlichungen in terminologischer Hinsicht notwendig. Beispielsweise wird im nDSG zwischen der Funktion der oder des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten und der Institution unterschieden. Die Abkürzung «EDÖB» meint die Institution, «die oder der Beauftragte» bezeichnet die Leiterin oder den Leiter der Institution. Die entsprechenden Anpassungen werden auch in der neuen VDSZ vorgenommen.

Zur Bezeichnung derjenigen, die eine Zertifizierung anstreben können, übernimmt die neue VDSZ ebenfalls die Begriffe von Artikel 13 nDSG, nämlich die «Hersteller von Datenbearbeitungssystemen oder -programmen», die «Verantwortlichen» und die «Auftragsbearbeiter». Somit wird auf den bis anhin im Rahmen der VDSZ verwendeten Ausdruck «Stelle, die eine Zertifizierung erhalten hat» verzichtet, weil er leicht mit der «Zertifizierungsstelle» verwechselt werden kann. Allerdings sei darauf hingewiesen, dass die Bezeichnung «Hersteller von Datenbearbeitungssystemen oder -programmen» auch Hersteller von Produkten (namentlich Datenbearbeitungssysteme oder -programme [Software] und Hardware), Dienstleistungen und Prozessen umfasst.

Für den Begriff «Systeme» gemäss Artikel 13 Absatz 1 nDSG verwendet die neue VDSZ den Begriff «Managementsysteme». Dies hat jedoch keine materielle Änderung im Verhältnis zum bisherigen Recht zur Folge. Die Begriffe «Organisation und Verfahren» entsprechend der Verordnung von 2007 werden als Präzisierung beibehalten. Die Verordnung verwendet im Weiteren in diesem Zusammenhang nur noch den Begriff «Managementsysteme». Des Weiteren werden, nachdem das nDSG die Möglichkeit der Zertifizierung von Dienstleistungen einführt, die entsprechenden Anforderungen präzisiert. Um den Bedürfnissen aus der Praxis gerecht zu werden, sieht die neue VDSZ zudem die Möglichkeit vor, «Prozesse» zu zertifizieren. Diese werden in Artikel 13 Absatz 1 nDSG zwar nicht aufgeführt, jedoch soll eine entsprechende Anpassung der Gesetzesgrundlage bei der nächsten Gelegenheit erfolgen. Der gewählte Lösungsansatz hat den Vorteil, dass er einerseits der Norm SN EN ISO/IEC 17021-1 (Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen) und andererseits der Norm SN EN ISO/IEC 17065 (Konformitätsbewertung – Anforderung an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren), entspricht. Zudem werden damit insgesamt auch die Zertifizierungsgegenstände besser voneinander abgegrenzt. Obgleich in Artikel 13 Absatz 1 nDSG nicht ausdrücklich vorgesehen, wird insbesondere im Rahmen der Zertifizierung von Produkten und Dienstleistungen auch die Möglichkeit, Datenbearbeitungen zertifizieren zu lassen, berücksichtigt. Dies erlaubt eine Annäherung des Schweizer Zertifizierungssystems an das europäische Recht und sollte es ermöglichen, dass Schweizer Zertifizierungen von Datenbearbeitungen durch die für den Datenschutz zuständigen europäischen Behörden anerkannt werden können.

Eingeführt werden zusätzliche Anforderungen an das Zertifizierungsprogramm (in der Verordnung von 2007 noch als «Kontrollprogramm» bezeichnet), über das die Zertifizierungsstellen verfügen müssen. Auch werden Anforderungen an die Zertifizierung von Dienstleistungen und Prozessen eingeführt. Aktualisiert werden sodann die Anforderungen an die Zertifizierung von Managementsystemen und Produkten sowie die Gültigkeitsdauer der Zertifizierung.

Für private Verantwortliche wird mit dem nDSG eine Ausnahme von der Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung eingeführt. Diese ersetzt die im bisherigen Recht bestehende Möglichkeit, von der Pflicht zur Anmeldung von Datensammlungen entbunden zu werden (ein Konzept, das gemäss dem im September 2020 verabschiedeten Gesetz nicht mehr existiert). Die diesbezüglichen Bestimmungen wurden in der neuen VDSZ entsprechend angepasst.

Schliesslich wurde mit der Erwähnung des Datenschutz-Qualitätszeichens in Artikel 13 Absatz 2 nDSG die bereits im alten Recht vorgesehene Delegationsnorm übernommen. Wie bereits die Verordnung von 2007 enthält auch die neue VDSZ keine Regelung über ein solches Qualitätszeichen. Bisher wurde es nicht als notwendig erachtet, ein allgemeines Qualitätszeichen im Bereich des Datenschutzes einzuführen.

3 Erläuterungen zur neuen VDSZ

3.1 Gliederung der Verordnung

Die neue Verordnung behält die Gliederung der Verordnung von 2007 bei: Der erste Abschnitt ist den Zertifizierungsstellen gewidmet, der zweite betrifft Gegenstand und Verfahren der Zertifizierung, im dritten Abschnitt werden die Sanktionen geregelt, und der letzte Abschnitt behandelt die Schlussbestimmungen.

3.2 1. Abschnitt: Zertifizierungsstellen

Der erste Abschnitt legt den Grundsatz der Akkreditierung von Zertifizierungsstellen fest. Artikel 1 präzisiert die Anforderungen, die von den Stellen erfüllt sein müssen, um akkreditiert zu werden. Artikel 2 nennt die im Rahmen des Akkreditierungsverfahrens zuständigen Institutionen. Schliesslich behandelt Artikel 3 die Frage der Anerkennung von ausländischen Zertifizierungsstellen in der Schweiz.

Art. 1 Anforderungen

Artikel 1 der neuen VDSZ regelt die Anforderungen an die Stellen, die Zertifizierungen durchführen (Zertifizierungsstellen). In erster Linie müssen diese Stellen von der Schweizerischen Akkreditierungsstelle (SAS) akkreditiert sein. Wie bereits unter der Verordnung von 2007 ist eine separate Akkreditierung für jeden Zertifizierungsgegenstand erforderlich.

Im Vergleich zur Verordnung von 2007 wurde Absatz 2 dahingehend ergänzt, dass eine Akkreditierung nunmehr nicht nur für die Zertifizierung der Organisation und der Verfahren im Zusammenhang mit Datenbearbeitungen (Bst. a) sowie von Produkten notwendig ist, sondern auch von Dienstleistungen und Prozessen im Zusammenhang mit Datenbearbeitungen (Bst. b).

Die von den Buchstaben a und b betroffenen Bereiche sind Gegenstand unterschiedlicher Akkreditierungen: Die Akkreditierung nach Buchstabe a erfolgt auf Basis der SN EN ISO/IEC 17021-1 (siehe oben) und SN EN ISO/IEC 27006 (Informationstechnik – IT-

Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten) sowie auf einem entsprechenden Zertifizierungsprogramm. Die Vorgaben für Buchstabe b werden von der SN EN ISO/IEC 17065 (siehe oben) und einem entsprechenden Zertifizierungsprogramm abgedeckt.

Die beiden Ergänzungen (zu Bst. b) der Dienstleistungen und Prozesse sind erforderlich, damit die Verordnung mit Artikel 13 nDSG in seiner im Rahmen der Totalrevision geänderten Version vereinbar ist sowie mit der Praxis und den oben erwähnten ISO-Normen in Übereinstimmung gebracht werden kann. Der Begriff «Dienstleistungen» ist neu. Damit ist beispielsweise die Speicherung von Daten in einer Cloud oder die Sammlung von Daten für einen Wettbewerb gemeint. Der Begriff «Prozesse» wurde ebenfalls ergänzt, um die Übereinstimmung mit den verschiedenen ISO-Normen wie insbesondere der Norm SN EN ISO 9001 (Qualitätsmanagementsysteme – Anforderungen) zu gewährleisten, die im Allgemeinen zwischen dem Prozess («Eingaben, Ausgaben, Aktivitäten») und dem Verfahren («Beschreibung» dieser Elemente) unterscheiden.

Mit der Klammer in Buchstabe a wird der Begriff «Managementsysteme» eingeführt. Diese Formulierung ermöglicht es, dem Gesetz, das neu von «Systemen», «Produkten» und «Dienstleistungen» spricht, zu entsprechen. Der präzisere Ausdruck «Managementsysteme» wird sodann durch den gesamten Verordnungstext hindurch übernommen.

Absatz 3 wird dahingehend geändert, dass er sich nur noch auf das Zertifizierungsprogramm bezieht, dessen Anforderungen in den Artikeln 5 bis 7 der neuen Verordnung geregelt sind. Der Begriff «Zertifizierungsprogramm» ersetzt den Begriff «Kontrollprogramm», um eine den ISO-Normen (beispielsweise SN EN ISO/IEC 17065, siehe oben) entsprechende Terminologie zu verwenden. Im Gegensatz zur Verordnung von 2007 werden die materiellen Anforderungen an das Zertifizierungsprogramm in den neuen Artikel 5 aufgenommen, so dass alle Anforderungen an dieses Programm in einem einzigen Artikel zusammengefasst sind.

Der Inhalt von Absatz 4 der Verordnung von 2007 wird nunmehr in Absatz 3 der neuen VDSZ eingefügt. Die erwähnten Artikel werden angepasst, um der geänderten Nummerierung der neuen Verordnung Rechnung zu tragen. Der Verweis auf die Verordnung vom 17. Juni 1996[8] über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (AkkBV) wird ebenfalls im neuen Artikel 5 aufgenommen.

Absatz 5 der Verordnung von 2007, der die Mindestanforderungen an die Qualifikation des Personals, das Zertifizierungen durchführt, regelt und auf den Anhang verweist, wird zu Absatz 4 in der neuen VDSZ. Der Absatz legt zudem neu normativ fest, dass die Zertifizierungsstellen nachweisen müssen, dass sie über Personal verfügen, welches diesen Kriterien entspricht.

Art. 2 Akkreditierungsverfahren

Im Vergleich zur Verordnung von 2007 wird einzig die Abkürzung «EDÖB» (zur Bezeichnung der Institution des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten) eingeführt. Sie ersetzt den Begriff der oder des «Beauftragten» (der sich neu auf die Leiterin oder den Leiter der Institution bezieht). Zu dieser terminologischen Änderung siehe oben, Ziff. 2.

[8] SR **946.512**

Art. 3 Ausländische Zertifizierungsstellen

Absatz 1 legt die Voraussetzungen fest, welche ausländische Zertifizierungsstellen nachweisen müssen, wenn sie auf schweizerischem Territorium tätig sein wollen. Im Verhältnis zur Verordnung von 2007 wurde die Bestimmung umstrukturiert, um alle Voraussetzungen in der gleichen Bestimmung zu regeln. Neben dem Nachweis, dass sie über eine gleichwertige Qualifikation verfügen, die Anforderungen an das Zertifizierungsprogramm erfüllen sowie die schweizerische Datenschutzgesetzgebung hinreichend kennen, müssen die ausländischen Zertifizierungsstellen neu auch nachweisen, dass sie die Anforderungen an die Qualifikation des Personals, welches Zertifizierungen durchführt, erfüllen (siehe hierzu Erläuterungen zu Art. 1 Abs. 4).

Absatz 2, der entsprechend der Ausführungen zu Absatz 1 im Verhältnis zur Verordnung von 2007 gekürzt wird, legt nunmehr lediglich fest, dass der EDÖB eine ausländische Zertifizierungsstelle nach Rücksprache mit der Schweizerischen Akkreditierungsstelle anerkennt.

Absatz 3 hält fest, dass der EDÖB die Anerkennung befristen und mit Auflagen verbinden kann. Der Begriff «Bedingungen», wie in der Verordnung von 2007 verwendet, wird an dieser Stelle gestrichen, weil eine Anerkennung nur mit Auflagen verbunden werden kann. Im Unterschied zu Bedingungen, welche erfüllt sein müssen, um überhaupt eine Anerkennung zu erhalten, werden Auflagen nach der Anerkennung gemacht, damit diese ihre Rechtsgültigkeit behält.

Hingegen schreibt Absatz 4 vor, dass der EDÖB die Anerkennung entziehen kann, wenn die Bedingungen und Auflagen nicht mehr erfüllt werden.

3.3 2. Abschnitt: Gegenstand und Verfahren

Bevor auf die verschiedenen Zertifizierungen und ihre Anforderungen eingegangen wird, werden in diesem Abschnitt zwei neue Artikel eingeführt. Artikel 4 behandelt den Gegenstand der Zertifizierung, und Artikel 5 regelt die Anforderungen an das Zertifizierungsprogramm. Die Artikel 6–10 der neuen VDSZ übernehmen die Artikel 4–8 der Verordnung von 2007 mit einigen Änderungen.

Art. 4 Gegenstand der Zertifizierung

Zweck dieses neuen Artikels ist es, in einer einzigen Bestimmung darzulegen, was im Datenschutzbereich zertifiziert werden kann. Es sind dies Managementsysteme, Produkte, Dienstleistungen und Prozesse im Zusammenhang mit Datenbearbeitungen (Abs. 1).

Die Zertifizierungsgegenstände werden näher definiert, indem für die Managementsysteme (Abs. 2) Artikel 4 Absatz 1 der Verordnung von 2007 (mit Ausnahme rein formeller Änderungen) übernommen wird.

Die Zertifizierung von Produkten wird in Absatz 3 Buchstabe a geregelt und entspricht der Regelung von Artikel 5 Absatz 1 der Verordnung von 2007. Zu denken ist dabei insbesondere an Internetbrowser, Software für den Betrieb von Webservern, Applikationen zur Betreibung von Websites, aber z.B. auch an Logistiksysteme, die auf RFID- oder GPS-Technologien beruhen. Absatz 3 Buchstabe b präzisiert, dass Dienstleistungen und Prozesse zertifizierbar sind, die hauptsächlich der Bearbeitung von Personendaten dienen oder die Personendaten erzeugen.

Art. 5 Anforderungen an das Zertifizierungsprogramm

Artikel 5 legt die Anforderungen an das Zertifizierungsprogramm fest. Wie bereits weiter oben erwähnt (siehe Art. 1 Abs. 3), wird der Begriff «Kontrollprogramm» durch «Zertifizierungsprogramm» ersetzt und die in Artikel 1 Absatz 3 Buchstaben a und b der Verordnung von 2007 vorgesehenen Vorgaben werden nunmehr in Absatz 1 dieses neuen Artikels verschoben. Die Formulierung wird ohne materielle Änderung leicht angepasst (z.B. Streichung des Begriffs «Begutachtung», weil es ausreicht von «Prüfung» zu sprechen).

Der neue Artikel 5 vervollständigt die bisherigen Anforderungen, indem er in Absatz 2 bestimmte Faktoren aufführt, welche bei der Festlegung des Zertifizierungsprogramms zwingend beachtet werden müssen. So müssen drei Aspekte berücksichtigt werden: erstens die von der Bearbeitung betroffenen Personendaten (dabei handelt es sich um den sachlichen Geltungsbereich), zweitens die für die Bearbeitung der Personendaten verwendete elektronische Infrastruktur (namentlich die technischen Systeme wie Hard- und Software) und schliesslich die organisatorischen Massnahmen im Zusammenhang mit der Bearbeitung von Personendaten. Diese drei Aspekte sind für die Ausarbeitung der Zertifizierungskriterien und der Verfahren massgebend, wobei deren Berücksichtigung je nach Zertifizierungsgegenstand variieren kann.

Als weitere Neuerung wird in Absatz 3 vorgeschrieben, dass das Zertifizierungsprogramm aufzeigen muss, dass die Prüfkriterien mit allen Datenschutzgrundsätzen nach Artikel 6 nDSG übereinstimmen. Bei der Festlegung der Schritte (Prüfkriterien, Verfahren etc.) sind deshalb die datenschutzrechtlichen Grundsätze wie etwa der Rechtmässigkeit, der Verhältnismässigkeit und der Zweckbindung der Bearbeitung sowie der Richtigkeit der Daten zu beachten.

Absatz 4 übernimmt schliesslich Artikel 1 Absatz 4 der Verordnung von 2007 und verweist, wie bereits oben gesagt, auf die Grundanforderungen, die in den im Anhang 2 der AkkBV aufgeführten ISO-Normen festgelegt sind. Dieser Absatz wird zudem ergänzt, um zu verdeutlichen, dass der Anhang 2 der AkkBV nicht abschliessend ist und dass weitere technische Normen zur Anwendung kommen. Für die auf der SN EN ISO/IEC 17065 (siehe oben) basierenden Akkreditierung von Produkten, Dienstleistungen und Prozessen sind für die Erfüllung der Anforderungen Zertifizierungsprogramme vorgesehen, die auf den internationalen Normen SN EN ISO/IEC 17067 (Konformitätsbewertung – Grundlagen für Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme), SN EN ISO/IEC TR 17028 (Konformitätsbewertung – Leitlinien und Beispiele für ein Zertifizierungsprogramm für Dienstleistungen) und SN EN ISO/IEC TR 17032 (Konformitätsbewertung – Leitlinien und Beispiele für ein Zertifizierungsprogramm für Prozesse) basieren können. Diese Zertifizierungsprogramme werden vom EDÖB in Form von Richtlinien erlassen.

Art. 6 Anforderungen an die Zertifizierung von Managementsystemen

Diese Bestimmung übernimmt weitgehend Artikel 4 der Verordnung von 2007. Absatz 1 entspricht materiell im Wesentlichen Artikel 4 Absatz 2. In Buchstabe b wird neu zusätzlich die Dokumentation von Risiken vorgeschrieben. Darüber hinaus wurden formelle Änderungen vorgenommen (zum Beispiel Verwendung des Begriffs «Managementsysteme» oder Streichung des Ausdrucks «Begutachtung»). Der französische Text wurde dahingehend angepasst, dass in Buchstabe a «charte de protection des données» durch «politique en matière de protection des données» ersetzt wurde, damit er dem deutschen Text («Datenschutzpolitik») entspricht.

Artikel 4 Absatz 3 der Verordnung von 2007, der die technischen Normen nennt, die der EDÖB beim Erlass von Richtlinien zu berücksichtigen hat, wird mit wenigen formellen Anpassungen in Artikel 6 Absatz 2 übernommen. Ergänzend wird indes ein neuer Buchstabe c eingefügt, der auf die Norm SN EN ISO/IEC 27701 (IT-Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Schutz der Privatsphäre, Anforderungen und Richtlinien) verweist.

Artikel 4 Absatz 1 der Verordnung von 2007 wird neben einer strukturellen und terminologischen Anpassung in Artikel 4 Absatz 2 der neuen VDSZ übernommen. Deutlicher präzisiert wird, dass die Zertifizierung von Managementsystemen die Gesamtheit des Systems, oder einzelner Teile der Organisation oder einzelne abgrenzbare Verfahren umfassen kann. Hingegen fällt Artikel 4 Absatz 4 der Verordnung von 2007 weg, da Artikel 11*a* Absatz 5 Buchstabe f DSG gestrichen wird (siehe hierzu die nachfolgenden Erläuterungen zu Art. 10).

Art. 7 Anforderungen an die Zertifizierung von Produkten, Dienstleistungen und Prozessen

Dieser Artikel übernimmt weitgehend Artikel 5 der Verordnung von 2007. Allerdings wird er in Bezug auf seinen sachlichen Geltungsbereich ausgeweitet, da er nicht mehr nur Produkte betrifft, sondern auch Dienstleistungen und Prozesse.

Absatz 1 stützt sich auf Artikel 5 Absatz 2 der Verordnung von 2007. In Buchstabe a wird neu das Konzept der Nachvollziehbarkeit vorgesehen, welches in Verbindung mit dem Konzept der Integrität die Authentizität umfasst. Es ist daher nicht mehr notwendig, die Authentizität explizit zu erwähnen. Der Verweis, dass diese Anforderungen im Hinblick auf den Verwendungszweck gewährleistet werden müssen, wird ebenfalls nicht übernommen, da die Anforderungen in jedem Fall und unabhängig vom Zweck der Bearbeitung für den Datenschutz erforderlich sind.

Buchstabe b erfährt dieselbe Anpassung betreffend den sachlichen Geltungsbereich: Dieser gilt neu für Produkte, Dienstleistungen und Prozesse. Zudem wird diese Bestimmung, die den Grundsätzen der Datensparsamkeit und der Datenvermeidung dient, in ihrer Formulierung vereinfacht, was jedoch keine inhaltliche Veränderung zur Folge hat; die Ausdrücke «Generierung» und «Speicherung» von Personendaten sind Aspekte des umfassenderen Begriffs der «Bearbeitung» und werden deshalb gestrichen.

Buchstabe c wird ebenfalls vereinfacht. Der Begriff «Nachvollziehbarkeit» wird in Buchstabe a übernommen und der Hinweis, dass es sich um eine «automatisierte» Bearbeitung handelt, erübrigt sich. Der Grundsatz der Transparenz der Bearbeitung ist auch dann wichtig, wenn die Bearbeitung nicht automatisiert ist (was allerdings wenig wahrscheinlich ist). Entscheidend ist, dass für die Anwenderin oder den Anwender erkennbar ist, welche Personendaten wie bearbeitet werden und insbesondere, welche Daten wohin übermittelt werden. Die Anforderungen definieren sich deshalb je nach Benutzerkreis, für den das Produkt, die Dienstleistung oder der Prozess konzipiert ist; bei einer breiten Anwendung gelten demnach höhere Anforderungen, als wenn es lediglich Spezialistinnen und Spezialisten betrifft. Auch wenn die entsprechende Präzisierung in Buchstabe c gestrichen wurde, ist darauf hinzuweisen, dass die Datenbearbeitung im Rahmen der festgelegten Funktionalität eines Produkts, einer Dienstleistung oder eines Prozesses geprüft wird. Kann das Produkt, die Dienstleistung oder der Prozess für verschiedene Zwecke verwendet werden, so ist darauf zu achten, dass sich Mechanismen zur Gewährleistung der Transparenz nicht ohne Weiteres umgehen oder ausschalten lassen.

Buchstabe d wird mit einem Hinweis ergänzt, wonach insbesondere die Rechte der betroffenen Personen einzuhalten sind.

Wie bereits Artikel 5 Absatz 3 der Verordnung von 2007, sieht schliesslich Absatz 2 vor, dass der EDÖB Richtlinien darüber erlässt, welche weiteren datenschutzrechtlichen Kriterien ein Produkt, eine Dienstleistung oder ein Prozess im Rahmen der Zertifizierung erfüllen muss. Die Bezeichnung der oder des Beauftragten wird durch die Abkürzung EDÖB ersetzt (zu dieser terminologischen Änderung siehe oben, Ziff. 2). Die Aufführung der Zertifizierungsgegenstände wie in der Verordnung von 2007 wird hingegen gestrichen, da sie im Hinblick auf die Überschrift unnötig ist.

Art. 8 Erteilung und Gültigkeit der Datenschutzzertifizierung

Artikel 8 Absatz 1 übernimmt Artikel 6 Absatz 1 der Verordnung von 2007 in gekürzter Fassung, und mit Ausnahme des Zusatzes des Begriffs «Prozesse», ohne materielle Änderung. Mit der Aufführung der Zertifizierungsgegenstände nach Artikel 1 Absatz 2 wird verdeutlicht, dass die Regelung für alle diese Gegenstände gilt. Im letzten Satz wird der Begriff «Bedingungen» gestrichen (siehe hierzu die Erläuterungen zu Art. 3). Dass die Zertifizierung mit Auflagen verbunden werden kann, ermöglicht es dem Hersteller von Datenbearbeitungssystemen oder -programmen, dem Verantwortlichen oder dem Auftragsbearbeiter, sich im Hinblick auf die Zertifizierung eines Managementsystems, eines Produkts, einer Dienstleistung oder eines Prozesses innerhalb einer gewissen Frist auf den neuesten Stand zu bringen.

Absatz 2 wird geändert, damit für alle Gegenstände, die zertifiziert werden können, dieselbe Zertifizierungsdauer von drei Jahren gilt. Neu gilt für Produkte deshalb die gleiche Zertifizierungsdauer wie für die anderen Zertifizierungsgegenstände. Diese Änderung dient insbesondere der Annäherung an das europäische Recht. Wie nach der Verordnung von 2007 muss jährlich eine Prüfung darüber erfolgen, ob die Voraussetzungen für die Zertifizierung weiterhin erfüllt sind. In diesem Zusammenhang wird der Zusatz «summarisch», wie er in Artikel 6 Absätze 2 und 3 der Verordnung von 2007 vorgesehen war, gestrichen, weil der Umfang der Prüfung vom konkreten in Frage stehenden Zertifizierungsgegenstand abhängt.

Art. 9 Anerkennung ausländischer Datenschutzzertifizierungen

Artikel 9 erfährt keine materielle Änderung. Neben wenigen formellen Änderungen im Vergleich zu Artikel 7 der Verordnung von 2007, wird der Begriff der oder des Beauftragten durch denjenigen des EDÖB ersetzt (zu dieser terminologischen Änderung siehe oben, Ziff. 2).

Art. 10 Ausnahme von der Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung

Artikel 4 Absatz 4 der Verordnung von 2007 sieht vor, dass die Ausnahme von der Pflicht zur Anmeldung von Datensammlungen nach Artikel 11*a* Absatz 5 Buchstabe f DSG nur anwendbar ist, wenn sämtliche Datenbearbeitungsverfahren, denen eine Datensammlung dient, zertifiziert sind. Nach der Gesetzesrevision besteht diese Möglichkeit nicht mehr. Gemäss neuem Recht (Art. 22 Abs. 5 nDSG) kann der private Verantwortliche indes «von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist». Artikel 4 Absatz 4 der Verordnung von 2007 ist daher hinfällig geworden und wird gestrichen. Hingegen wird in Artikel 10 der neuen VDSZ eine Anpassung an Artikel 22 Absatz 5 nDSG vorgenommen: Der private Verantwortliche kann von der Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung nur dann absehen, wenn die Zertifizierung die Bearbeitung einschliesst, die im Rahmen der Datenschutz-Folgenabschätzung zu prüfen wäre (siehe

in diesem Sinn die Botschaft des Bundesrates über das neue Datenschutzgesetz, vgl. BBl *2017* 6941, insbesondere 7062). Eine Zertifizierung darf somit nicht zu allgemein sein und sollte die Bearbeitung umfassen, für die der Verantwortliche von der Erstellung einer Datenschutz-Folgenabschätzung befreit werden möchte.

In diesem Zusammenhang wird Artikel 8 der Verordnung von 2007 gestrichen. Diese Bestimmung präzisierte die Bedingungen, unter denen eine Befreiung von der Pflicht zur Anmeldung der Datensammlungen möglich ist, nämlich durch Mitteilung der Zertifizierung an den EDÖB und unter Einreichung der notwendigen Dokumente. Eine erneute Einführung der Pflicht zur Mitteilung an den EDÖB im Fall von Artikel 22 Absatz 5 nDSG wurde als unnötig erachtet, zumal diesem die Ergebnisse der Datenschutz-Folgenabschätzung ebenfalls nicht mitgeteilt werden müssen. Der EDÖB hätte gewünscht, dass der private Verantwortliche dennoch dazu verpflichtet bleibt, vorgängig seine Stellungnahme einzuholen, sofern nach der Risikoanalyse hohe Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person bleiben. Dies würde jedoch dazu führen, dass entgegen dem Willen des Gesetzgebers für die privaten Verantwortlichen wieder eine Informationspflicht an den EDÖB eingeführt wird. Weil die Zertifizierung dem EDÖB nicht mitzuteilen ist, erübrigen sich auch die Absätze 2 und 3 von Artikel 8 der Verordnung von 2007. Die Veröffentlichung eines Verzeichnisses der Stellen, die eine Zertifizierung erhalten haben, wird als unnötig erachtet, da diese Stellen ein Interesse daran haben, direkt darüber zu informieren. Sie brauchen deshalb nicht auf der Website des EDÖB aufgeführt zu sein.

3.4 3. Abschnitt: Sanktionen

Vorbehältlich gewisser punktueller Änderungen übernehmen die Artikel 11 und 12 der neuen VDSZ die Artikel 9 und 10 der Verordnung von 2007.

Art. 11 Sistierung und Entzug der Zertifizierung

Absatz 1 dieses Artikels wird im Vergleich zu Artikel 9 Absatz 1 der Verordnung von 2007 in zwei Punkten geändert. Zunächst wird der interne Verweis gestrichen. Denn aus dem Kontext ergibt sich klar, dass es sich dabei um eine Überprüfung nach Artikel 8 Absatz 2 handelt. Zweitens wird der Buchstabe b leicht umformuliert, ohne eine materielle Änderung zur Folge zu haben.

Anstelle von «namentlich» wie in Artikel 9 Absatz 1 der Verordnung von 2007, wird in Absatz 1 im deutschen Text zudem neu der Begriff «insbesondere» verwendet. Er verdeutlicht, dass es sich lediglich um ein Beispiel handelt und sich auch andere Situationen ergeben können. Beispielsweise kann bei einer besonderen oder spontanen Überprüfung eines mangelhaften Produkts eine Zertifizierung auch dann sistiert oder entzogen werden, wenn der Mangel im Rahmen der jährlichen Überprüfung nicht entdeckt worden ist.

Absatz 2 erfährt lediglich eine formelle Änderung, indem «Stelle, die die Zertifizierung erhalten hat» durch die Terminologie von Artikel 13 nDSG ersetzt wird, ergo «dem Hersteller von Datenbearbeitungssystemen oder -programmen, dem Verantwortlichen oder dem Auftragsbearbeiter, der die Zertifizierung erhalten hat». Damit wird klarer aufgeführt, wer die Personen sind, die von der Möglichkeit einer Zertifizierung Gebrauch machen können (siehe diesbezüglich auch die Erläuterungen oben, Ziff. 2).

Absatz 3 wird gestrichen, weil der Erhalt einer Zertifizierung dem EDÖB nicht mehr mitgeteilt wird. Auch wurde darauf verzichtet, dass der EDÖB ein Verzeichnis über die privaten Verantwortlichen führt, die eine Zertifizierung erhalten haben und von der Pflicht zur Erstellung

einer Datenschutz-Folgenabschätzung befreit sind. Der EDÖB hätte eine Informationspflicht des Zertifizierungsnehmers über die Sistierung oder den Entzug der Sistierung an den EDÖB gewünscht, sofern er von diesem bei Verbleiben hoher Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person eine vorgängige Stellungnahme hätte einholen müssen (siehe hierzu die Erläuterungen zu Art. 10).

Art. 12 Verfahren bei Aufsichtsmassnahmen des EDÖB

Dieser Artikel übernimmt im Wesentlichen Artikel 10 der Verordnung von 2007. Die Sachüberschrift wird dahingehend geändert, dass der Begriff des EDÖB denjenigen der oder des Beauftragten ersetzt (zu dieser terminologischen Änderung siehe oben, Ziff. 2).

Absatz 1 wird in formeller Hinsicht geändert. Der Zusatz in der Verordnung von 2007, dass ein Mangel *bei der Aufsichtstätigkeit des EDÖB* festgestellt wird, wird gestrichen, da er nicht notwendig ist. Denn die Überprüfung fällt auf jeden Fall in die Zuständigkeit des EDÖB nach Artikel 4 sowie 49 bis 51 nDSG. Im Übrigen wird wie bei Artikel 11 Absatz 2 auch hier die Terminologie an Artikel 13 nDSG angepasst.

Absatz 2 wird lediglich formell angepasst, namentlich betreffend den Begriff der oder des Beauftragten und die an Artikel 13 nDSG angepasste Terminologie.

Absatz 3 erfährt ebenfalls nur gewisse redaktionelle Änderungen. Des Weiteren wird aus Gründen der Rechtsklarheit die Dauer der Frist von 30 Tagen zur Behebung von Mängeln erneut explizit erwähnt.

Absatz 4 wird geändert, um auf den betreffenden Artikel des nDSG (Art. 51 Abs. 1) zu verweisen, was zur Folge hat, dass die Begriffe, mit denen das Vorgehen des EDÖB umschrieben wird, anzupassen sind. So kann er nicht mehr lediglich eine Empfehlung aussprechen, sondern er kann vielmehr eine Massnahme anordnen, welche sich an den Hersteller von Datenbearbeitungssystemen oder -programmen sowie den Verantwortlichen oder den Auftragsbearbeiter richtet, der über eine Zertifizierung verfügt. Entsprechend empfiehlt er im letzten Satz der Zertifizierungsstelle nicht mehr, sondern ordnet ihr an, die Zertifizierung zu sistieren oder zu entziehen, wenn diese trotz Weiterbestehen der Mängel, eine Zertifizierung nicht selber sistiert oder entzogen hat. In diesem Fall informiert er, wie in der Verordnung von 2007, die Schweizerische Akkreditierungsstelle darüber.

3.5 4. Abschnitt: Schlussbestimmungen

Artikel 13 regelt die Aufhebung der Verordnung von 2007 und Artikel 14 legt das Datum des Inkrafttretens der neuen VDSZ fest.

3.6 Anhang

Die Überschrift sowie die Ziffern 1 und 2 des Anhangs erfahren lediglich einige formelle Änderungen im Vergleich zur Verordnung von 2007 und werden in gewissen Punkten präzisiert.

1 Zertifizierung von Managementsystemen

Die Sachüberschrift, der Einleitungssatz und der letzte Satz werden der Terminologie der neuen VDSZ angepasst (siehe diesbezüglich auch die Erläuterungen zu Art. 1 Abs. 2 Bst. a). Darüber hinaus werden der Einleitungssatz, die Spiegelstriche und der letzte Satz insofern

geändert, als das Erfordernis des Nachweises, dass das Personal, welches Zertifizierungen durchführt, die Anforderungen erfüllt, nun Teil des Verordnungstexts ist (siehe hierzu die obigen Erläuterungen zu Art. 1 Abs. 5). Der Begriff «gesamthaft» im Einleitungssatz, wie er schon in der Verordnung von 2007 verwendet wird, ist so zu verstehen, dass das gesamte Team, welches Prüfungen durchführt, alle Qualifikationen zu erfüllen hat und nicht jeder Einzelne, da es kaum Spezialisten gibt, die sämtliche Anforderungen erfüllen.

Des Weiteren wird der erste Spiegelstrich zwecks Übereinstimmung mit dem zweiten Spiegelstrich in formeller Hinsicht geändert (Zusatz von «im Bereich»).

Im zweiten Spiegelstrich wird der veraltete Begriff «Informatiksicherheit» durch «Informationssicherheit» ersetzt (siehe in diesem Sinn auch das neue Bundesgesetz über die Informationssicherheit, ISG, vgl. BBl *2020* 9975).

Der dritte Spiegelstrich wird neu eingefügt. Er präzisiert, dass das Personal, das Managementsysteme zertifiziert, nicht nur über durch eine praktische Tätigkeit oder ein Diplom nachgewiesene Kenntnisse in den Bereichen des Datenschutzrechts und der Informationssicherheit verfügen muss, sondern auch die Entwicklungen in diesen beiden Bereichen zu kennen hat, namentlich durch den Besuch von Weiterbildungen.

Der letzte Spiegelstrich wird neu strukturiert und mit zwei zusätzlichen ISO-Normen ergänzt: die Norm SN EN ISO/IEC 17021-3 (Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, Teil 3: Anforderungen an die Kompetenz für die Auditierung und Zertifizierung von Qualitätsmanagementsystemen) und die Norm SN EN ISO/IEC 27006 (siehe oben).

Schliesslich sei darauf hingewiesen, dass sich der Begriff «Bereiche» im letzten Satz – die Verordnung von 2007 in der deutschen Fassung sprach sinngemäss von «Teilbereichen» – auf die beiden Bereiche der zwei ersten Spiegelstriche bezieht, mithin auf den Bereich des Datenschutzrechts und auf denjenigen der Informationssicherheit. Wie in der Verordnung von 2007 wird präzisiert, dass die Prüfung von Managementsystemen durch ein interdisziplinäres Team zulässig ist.

2 Zertifizierung von Produkten, Dienstleistungen und Prozessen

Mit Ausnahme der Verweise im letzten Spiegelstrich auf das Zertifizierungsprogramm, die Richtlinien des EDÖB und die neuen ISO-Normen gelten sämtliche Anpassungen in Ziffer 1 über die Zertifizierung von Managementsystemen auch für diesen zweiten Teil des Anhangs, der die Zertifizierung von Produkten, Dienstleistungen und Prozessen betrifft. Die erwähnten Ergänzungen sind notwendig, weil die bereits in der Verordnung von 2007 aufgeführte ISO-Norm SN EN ISO/IEC 17065 (siehe oben) nicht alle für die Zertifizierung von Produkten, Dienstleistungen und Prozessen notwendigen Anforderungen an die Fachkenntnisse des Personals, welches Zertifizierungen durchführt, beinhaltet. Im Übrigen wird sinngemäss auf die Erläuterungen zu Ziffer 1 verwiesen.