universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO im Bildungsbereich“

verfasst von / submitted by

Mag. Florian Novotny

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2024 / Vienna 2024

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Dr. Matthias Schmidl

Danksagung

Ich möchte mich an dieser Stelle bei allen Personen bedanken, die mich bei der Fertigstellung dieser Master Thesis unterstützt haben.

Zunächst darf ich meinem Betreuer, Herrn Dr. Schmidl meinen Dank für die professionelle Anleitung und Expertise im gesamten Betreuungsprozess bis zur Einreichung meiner Master Thesis aussprechen.

Ein besonderer Dank ergeht an das Bundesministerium für Bildung, Wissenschaft und Forschung als meinen Dienstgeber, welches mich bei der Erreichung meiner akademischen Ziele neben der Erfüllung meiner beruflichen Verpflichtungen maßgeblich unterstützt hat.

Ich möchte mich auch ganz herzlich bei meiner Familie und meiner Verlobten bedanken, deren Unterstützung und Rückhalt die Realisierung meines Studienvorhabens erst möglich gemacht haben.

Disclaimer

Im Sinne eines diskriminierungsfreien Sprachgebrauchs bei der Verwendung personenbezogener Bezeichnungen gilt die jeweils gewählte Form für alle Geschlechter, wenngleich einschlägige Gesetzestexte mitunter das generische Maskulinum verwenden. Bezeichnungen aus dem Englischen wie zB „privacy by design“ oder „friendly Audit“ werden in ihrer ursprünglichen Form verwendet.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Anm	Anmerkung
Art	Artikel
Abs	Absatz
BilDokG	Bildungsdokumentationsgesetz
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
BSI	deutsches Bundesamt für Sicherheit in der Informationstechnologie
BVerG	Bundesvergabegesetz
DAkkS	Deutsche Akkreditierungsstelle
DSB	österr. Datenschutzbehörde
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DSK	Datenschutzkonferenz (Deutschland)
DSGVO	Datenschutzgrundverordnung
DSMS	Datenschutzmanagementsystem
EDSA	Europäischer Datenschutzausschuss
EdTech Hub	Educational Technologies Hub
EK	Europäische Kommission
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
ErwG	Erwägungsgrund
EWR	Europäischer Wirtschaftsraum
ex ante	im Voraus
ex lege	nach dem Gesetz
FISA	Foreign Intelligence Surveillance Act
gem	gemäß
GRC	Charta der Grundrechte der Europäischen Union
IKT	Informations- und Kommunikationstechnologie
IoT	Internet of Things
iSd	im Sinne der/des

ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Normungsorganisation
iVm	in Verbindung mit
leg cit	legis citate / zitierte Gesetzesstelle
lit	litera
NGO	Non-Governmental Organisation
NIS	Netz- und Informationssicherheit
PH	Pädagogische Hochschule
Rn	Randnummer
SchUG	Schulunterrichtsgesetz
SSO	Single Sign-On
TKG	Telekommunikationsgesetz
TOM	technische und organisatorische Maßnahmen
Z	Ziffer
zB	zum Beispiel
ZeStAkk-V	Zertifizierungsstellen-Akkreditierungs-Verordnung
ZLM	Zentrum für Lernmanagement

1. Einleitung

Die fortschreitende Digitalisierung stellt den österreichischen Bildungsbereich vor aktuelle Herausforderungen wie etwa den rechtskonformen Umgang mit künstlicher Intelligenz.[1] Der Datenschutz soll jedenfalls „keinen Hemmschuh für digitalen Fortschritt" darstellen, wobei auf die technologieneutrale Ausgestaltung der DSGVO[2] verwiesen werden kann.[3]

Die bestehenden Untersuchungs- und Aufsichtsbefugnisse der DSB[4] sowie die beiden rezenten Entscheidungen des EuGH zur Haftung für schuldhaftes Verhalten jeglicher unternehmerischer Tätigkeit im Namen einer juristischen Person sowie zurechenbarer Verarbeitungsvorgänge von Auftragsverarbeitern[5] verdeutlichen die Notwendigkeit der nachweislichen Erfüllung datenschutzrechtlicher Pflichten.

Die Einhaltung normativer Vorgaben kann auf verschiedene Weise reguliert werden, weshalb zwischen den Ansätzen der imperativen Regulierung, der regulierten Selbstregulierung sowie der autonomen Selbstregulierung differenziert wird. Diese Ansätze unterscheiden sich dahingehend voneinander, ob staatliche Vorgaben zur Durchsetzung vorliegen oder ob lediglich ein verbindlicher Rahmen für die Einhaltung gewisser Rechtsschutzziele vorgegeben wird, dessen Umsetzung die Normadressaten jedoch selbst durchführen. Schließlich kann den Normadressaten auch die Implementierung von Mechanismen zur Erstellung und Einhaltung eines eigenen Regelwerkes freigestellt werden.

Die imperative Regulierung gilt als überwiegender Anwendungsfall regulatorischer Modelle, da staatliche Gesetzgeber den Normadressaten einseitige, von deren Partizipation unabhängige Pflichten auferlegen und Kontroll- und Sanktionsmechanismen festlegen. Als prominentes Beispiel imperativer Regulierung kann hier grundsätzlich die DSGVO genannt werden. Das Prinzip der regulierten Selbstregulierung stellt auf die staatlich vorgesehene Einsetzung von Regulierungsinstanzen ab, die über festgelegte Durchsetzungsmechanismen

[1] https://www.bmbwf.gv.at/Themen/schule/zrp/ki.html (abgerufen am 10.12.2023).

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

[3] Dr. Matthias Schmidl im Zuge des Rechtspanoramas am Juridium zur künstlichen Intelligenz in *Aichinger*, Wie Hermann Nitsch Chat-GPT-Nutzern hilft, Die Presse 2023/21/01.

[4] *Schmidl*, Die Datenschutzbehörde am 25. 5. 2018 - Funktion und Stellung der DSB nach der DS-GVO und dem DSG (2018), jusIT 2017/79, 191.

[5] EuGH 05.12.2023, C-683/21 d; EuGH 05.12.2023, C-807/21.

verfügen. Eine autonome bzw tatsächliche Selbstregulierung ist schließlich durch fehlende staatliche Vorgaben gekennzeichnet, wobei privatwirtschaftliche Instanzen ein entsprechendes Regelwerk und Instrumentarium zu dessen Einhaltung als Ausfluss der Privatautonomie aufstellen.

Die datenschutzrechtliche Zertifizierung nach Art 42 DSGVO fällt mit den vorgesehenen, zu akkreditierenden Zertifizierungsstellen als Regulierungsinstanz in den Anwendungsbereich der regulierten Selbstregulierung, solange die DSB als staatlich vorgesehene Aufsichtsbehörde im jeweiligen Anwendungsfall nicht selbst als Zertifizierungsstelle tätig wird. Wie auch im Zusammenhang mit Verhaltensregeln gem Art 40 DSGVO erfolgt die Unterwerfung der Zertifizierungswerber unter diese Regulatorien freiwillig und ohne staatlichen Zwang. Aufgrund des imperativen Regelungscharakters der DSGVO ist es jedoch strittig, ob ein erhöhtes Schutzniveau über die vorgesehenen Standards der DSGVO hinaus durch selbstregulatorische Mechanismen zulässigerweise erreicht werden kann.[6]

In Ermangelung einer allgemeingültigen Legaldefinition des Begriffes der Zertifizierung kann zunächst auf die Ansicht der Internationalen Normungsorganisation (ISO) zurückgegriffen werden. Eine Zertifizierung ist demnach die schriftliche Garantie einer unabhängigen Stelle, dass bestimmte Anforderungen erfüllt werden. Die Begriffe der Konformitätsbewertung durch unabhängige Stellen lassen sich auch aus einschlägigen technischen Normen ableiten.[7] Im Kontext der datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO bezieht sich der Begriff der Zertifizierung den Leitlinien des EDSA zufolge auf eine Bescheinigung durch unabhängige Dritte im Zusammenhang mit Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern.[8]

Während die Notwendigkeit einer Zertifizierung, die bloß das grundlegende Datenschutzniveau der DSGVO abbildet, aufgrund der ohnehin bestehenden normativen Vorgaben kritisch in Abrede gestellt werden könnte, lässt sich aus den Erwägungsgründen

[6] *Mertens,* Accountability im europäischen Datenschutzrecht Kapitel B.

[7] DIN EN-ISO/IEC 17000:2004 Konformitätsbewertung - Begriffe und allgemeine Grundlagen (ISO/IEC 17000:2004), abrufbar unter: https://www.beuth.de/de/norm/din-en-iso-iec-17000/73222448; vgl auch ÖVE/ÖNORM EN ISO/IEC 17000 Konformitätsbewertung - Begriffe und allgemeine Grundlagen (ISO/IEC 17000:2020), abrufbar unter: https://shop.austrian-standards.at/action/de/public/details/684592/OEVE_OENORM_EN_ISO_IEC_17000_2020_10_15;jsessionid=072D271F0DEC3965F965F5BAF38D99ED (abgerufen am 30.11.2023).

[8] EDSA Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, 1.3.1.

ableiten, dass die DSGVO von einer inhomogenen Ausgestaltung der jeweiligen datenschutzrechtlichen Schutzniveaus innerhalb der Mitgliedsstaaten ausgeht.[9]

Die lückenlose Umsetzung sämtlicher Vorgaben der DSGVO geht in der Praxis bekanntlich mit gewissen Herausforderungen einher. Demzufolge gilt es zu berücksichtigen, dass Verantwortliche und Auftragsverarbeiter durch die Erlangung einer derartigen datenschutzrechtlichen Zertifizierung nach dem Durchlaufen eines komplexen Zertifizierungsverfahrens eine hohe Bereitschaft zur Einhaltung bestmöglicher Datenschutz – Compliance signalisieren. Während die attestierte Einhaltung eines DSGVO-Grundniveaus bei der Verarbeitung personenbezogener Daten im Zusammenhang mit diversen, auf dem Vormarsch befindlichen Clouddienstleistungen[10] im Sinne der Rechtssicherheit vorteilhaft erscheint, obliegt es hingegen einer Einzelfallbetrachtung, ob die Einhaltung höherer datenschutzrechtlicher Standards einer Zertifizierung sinnvollerweise zuträglich ist.[11]

Zertifizierungen im Datenschutzrecht bergen ein hohes Potential, um datenverarbeitende Akteure im Sinne eines selbstregulatorischen Ansatzes zur Einhaltung des geforderten Datenschutzniveaus anzuhalten. Sobald akkreditierte Zertifizierungsstellen die ersten Konformitätsbewertungen durchführen können, wird sich herausstellen, in welchem Ausmaß die für Datenverarbeitungsvorgänge unmittelbar bzw. für Produkte und Dienstleistungen bloß mittelbar zulässige Zertifizierung in Anspruch genommen wird. [12]

[9] ErwG 100 DSGVO, vgl. auch *Bergt/Pesch* in Kühling/Buchner, DS-GVO[3] Art 42 Rz 15.

[10] https://de.statista.com/infografik/22671/nutzung-von-cloud-computing-in-unternehmen-in-deutschland/ (abgerufen am 30.11.2023).

[11] *Strohmaier* in Knyrim, DatKomm Art 42 DSGVO Rn 28/4 – 28/6.

[12] *Kröpfl*, Datenschutzrechtliche Zertifizierungen, Jahrbuch Datenschutzrecht 2019, 163 (221).

1.1 Aufbau der Masterthesis

Der Aufbau der Masterthesis gliedert sich in einen Grundlagenteil sowie in einen Praxisteil. Die folgenden Themenkomplexe werden anhand der zugrundeliegenden Forschungsfragen abgehandelt:

Zu Beginn des Grundlagenteiles werden jene Bestimmungen des risikobasierten Ansatzes der DSGVO näher umrissen, die einen direkten normativen Konnex zur datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO aufweisen. In weiterer Folge wird ein Überblick über Zertifizierungen im Allgemeinen sowie über die gängigsten internationalen und nationalen Normen und Standards gegeben, bevor eine Gegenüberstellung von Zertifizierungsmöglichkeiten im Bereich von Managementsystemen der Informationssicherheit und des Datenschutzes erfolgt. Der Kernbereich des Grundlagenteils beleuchtet die einzelnen Facetten der datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO und grenzt diese schließlich von bisher etablierten Zertifizierungsverfahren ab.

Der Praxisteil bildet datenschutzrechtliche Prozesse innerhalb des BMBWF ab und soll anhand alltäglicher Fallbeispielen aus dem Schulunterricht vor Augen führen, was es hierbei aus datenschutzrechtlicher Sicht zu beachten gilt. In weiterer Folge werden die im Schulrechtsvollzug einschlägigen Normen für die Verarbeitung von personenbezogenen Daten angeführt und Initiativen zur Förderung des Bewusstseins von Schülerinnen und Schülern für den Bereich des Datenschutzes und der Datensicherheit vorgestellt. Daraufhin folgt die eingehende Behandlung technisch denkbarer Ansätze, um dem Spannungsfeld des Einsatzes privater Clouddiensteanbieter sowie Aspekten des Datenschutzes und der digitalen Souveränität im Bildungsbereich zu begegnen.

Hierdurch wird schließlich der Bogen zur angestrebten Zertifizierung nach Art 42 DSGVO im Bildungsbereich und dem derzeit stattfindenden, datenschutzrechtlichen Beratungsaudit zweier Lernplattformen des BMBWF gespannt, bevor eine abschließende Zusammenfassung der aufgestellten Thesen erfolgt.

2. Grundlagen

2.1 Der risikobasierte Ansatz der DSGVO

Die DSGVO zielt auf den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ab, wobei Verarbeitungsvorgänge stets im Dienste der Menschheit erfolgen sollen.[13] Die Verarbeitung personenbezogener Daten geht jedoch unweigerlich mit Risiken für die betroffenen Personen einher, da eine vollständig risikofreie Datenverarbeitung nicht möglich ist. Das Grundrecht auf Schutz personenbezogener Daten[14] besteht nicht uneingeschränkt und bedarf einer verhältnismäßigen Abwägung unter der Berücksichtigung seiner gesellschaftlichen Funktion.[15]

Bereits der Ratsentwurf zur DSGVO lies darauf schließen, dass Angemessenheits- und Risikoerwägungen eine wichtige Rolle im Bereich eines harmonisierten Datenschutzrechts des europäischen Binnenmarktes zukommt. In diesem Zusammenhang erfolgte auch eine Stellungnahme der Artikel 29 – Datenschutzgruppe als Vorgängerin des Europäischen Datenschutzausschusses, in der sie für die Einheitlichkeit und Skalierbarkeit des eingeräumten Schutzniveaus plädierte.[16]

Sobald Verarbeitungsvorgänge personenbezogene Daten enthalten, ist eine kritische Risikobewertung unter der Berücksichtigung von Verhältnismäßigkeitsgesichtspunkten vorzunehmen, obwohl hierfür keine systematische Zuordnung zu den allgemeinen Grundsätzen nach Art 5 DSGVO vorliegt. Der geforderte Sorgfaltsmaßstab knüpft somit an der Schutzwürdigkeit von betroffenen Daten an.[17] Im Zuge der Rechenschaftspflicht nach Art 5 Abs 2 leg cit müssen Verantwortliche die Einhaltung ihrer datenschutzrechtlichen Vorgaben nachweisen können. Die Verhältnismäßigkeit erforderlicher Maßnahmen ist zur Sicherstellung von grundlegenden, rechtsstaatlichen Prinzipien sowie einer unbeschränkten Nachweispflicht nach dem risikobasierten Ansatz zu beurteilen [18]

[13] ErwG 4 DSGVO.
[14] Art 8 GRC, vgl auch Art 8 EMRK.
[15] *Bergauer/Jahnel*, Das neue Datenschutzrecht[3] 17.
[16] *Veil*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD 2015, 347 f.
[17] *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] 146.
[18] *Hötzendorfer/Kastelitz/Tschohl* in Knyrim (Hrsg), DatKomm Art 24 DSGVO Rz 35.

Das Konzept des risikobasierten Ansatzes ermöglicht datenverarbeitenden Akteuren eine strukturierte Überprüfung auftretender Risiken sowie ein geeignetes Mittel zur Abwägung von Maßnahmen im Rahmen ihrer gesetzlichen Pflichten.[19] Die DSGVO kennt jedoch keine allgemeine Legaldefinition des Risikobegriffs. Die deutsche Datenschutzkonferenz des Bundes und der Länder leitet den Risikobegriff als möglichen Eintritt eines schädigenden Ereignisses her.[20] Als Ausgangspunkt für eine objektivierte Bewertung kann die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen herangezogen werden.[21]

Der Verantwortliche hat die Bewertung unter der Berücksichtigung aller in diesem Zeitpunkt vorliegenden Informationen ex-ante vorzunehmen. Falls eine Datenschutzfolgenabschätzung zwingend vorgesehen ist, erfolgt die Risikobewertung anhand deren Ergebnis.[22] In Bezug auf die Art, den Umfang, die Umstände sowie die Zwecke der Verarbeitung ist zwischen „Risiko“ und „hohem Risiko“ zu unterscheiden, die DSGVO sieht jedoch keine Legaldefinition dieser Begrifflichkeiten vor.[23] In der Praxis hat sich die Verwendung einer Risikomatrix zur Abschätzung und besseren Visualisierung für eine Abbildung der Eintrittswahrscheinlichkeit etabliert. Der risikobasierte Ansatz stößt aufgrund seiner Unanwendbarkeit im Zusammenhang mit Betroffenenrechten der DSGVO schließlich an seine Grenzen, da diese keiner Risikoabwägung zuträglich sind.

Der risikobasierte Ansatz umfasst neben den Bestimmungen der Art 24, 25 sowie 32 DSGVO auch die Bestimmung zur Datenschutz-Folgenabschätzung nach Art 35 leg cit, die grundsätzlich nur die Einhaltung genehmigter Verhaltensregeln nach Art 40 DSGVO und nicht die Durchführung einer datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO vorsieht. In weiterer Folge werden jene Bestimmungen der DSGVO näher erläutert, die auf risikobasierte Gesichtspunkte abstellen und eine Möglichkeit zur Durchführung einer Zertifizierung nach Art 42 DSGVO zum Nachweis obliegender Rechenschaftspflichten ex lege vorsehen. [24]

[19] *Piltz* in Gola/Heckmann (Hrsg), DS-GVO Art 24 Verantwortung des für die Verarbeitung Verantwortlichen[3] 597 f.
[20] DSK, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen.
[21] ErwG 76 DSGVO.
[22] ErwG 84 DSGVO.
[23] ErwG 94 DSGVO.
[24] *Schröder*, Der risikobasierte Ansatz in der DS-GVO, ZD 2019/11, 503.

2.1.1 Artikel 24 DSGVO: Verantwortung des für die Verarbeitung Verantwortlichen

Als zentrale Bestimmung des risikobasierten Ansatzes normiert Art 24 DSGVO die Haftung des Verantwortlichen für die Einhaltung der ihm obliegenden datenschutzrechtlichen Pflichten. Der Begriffsdefinition in Art 4 Z 7 DSGVO zufolge handelt es sich bei Verantwortlichen um natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Die Pflicht zur rechtmäßigen Datenverarbeitung ergibt sich systematisch bereits aus den Grundsätzen der DSGVO[25]. Der weite Regelungsumfang des Art 24 DSGVO umfasst darüber hinaus auch die Prozessverantwortung sowie die Sicherstellungspflicht des Verantwortlichen zur Einhaltung datenschutzrechtlicher Anforderungen. Aufgrund der Rechenschaftspflicht gilt es Informationspflichten nachzukommen und die Einhaltung bestehender Pflichten nachzuweisen, da der Verantwortliche über die Zwecke und Mittel der Datenverarbeitung entscheidet.[26]

In Abgrenzung zu den nachfolgenden Bestimmungen in Art 25, 32 DSGVO kann der abstrakte Regelungsgehalt des Art 24 DSGVO als lex generalis mit der Funktion eines Auffangtatbestands angesehen werden. Der Grundsatz der Rechenschaftspflicht sowie seine Ausgestaltung in Art 24 DSGVO richtet sich dabei unmittelbar an den Verantwortlichen als Normadressaten. Spezifische Regelungen wie etwa die Rechenschaftspflicht gegenüber der Aufsichtsbehörde sowie die Verpflichtung, geeignete Unterlagen und Aufzeichnungen zu führen, gelten jedoch auch gegenüber Auftragsverarbeitern.[27]

Im Hinblick auf die Auswahlverantwortlichkeit des Verantwortlichen bei der Beauftragung von Auftragsverarbeitern nach Art 28 Abs 1 DSGVO kann diesen gegenüber mittelbare Bindungswirkung entstehen.[28] Der Verantwortliche hat adäquate Maßnahmen zu implementieren und umzusetzen, um die Vorgaben der DSGVO zu erfüllen sowie Datenschutzverletzungen vorzubeugen.[29] Die DSB vertritt die Rechtsmeinung, dass

[25] Art 5 Abs 1 lit a iVm Abs 2 DSGVO.

[26] *Schmidt/Brink* in Wolff/Brink/Ungern-Sternberg (Hrsg), BeckOK Datenschutzrecht DS-GVO[44] Art 24 Rn 13-18.

[27] EDSA Leitlinie 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO Rn 9.

[28] *Hötzendorfer/Kastelitz/Tschohl*, DatKomm Art 24 DSGVO Rz 13.

[29] DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018.

Betroffene nicht die Umsetzung spezifischer Maßnahmen aus der DSGVO verlangen können, der Verantwortliche entscheidet daher selbst über die Eignung und Angemessenheit seiner Maßnahmen.[30]

Unter der Berücksichtigung der jeweiligen Umstände eines Verarbeitungsvorganges gilt es die Erforderlichkeit und Eignung von Maßnahmen grundsätzlich im Zuge einer Einzelfallentscheidung zu beurteilen. Die Anordnung zur Vornahme einer Verhältnismäßigkeitsabwägung durch den Verantwortlichen bei der Auswahl seiner Maßnahmen lässt sich unmittelbar aus Art 52 Abs 2 GRC[31] ableiten. In diesem Zusammenhang sind auch die Grundrechte des Verantwortlichen wie etwa das Recht auf Erwerbsfreiheit und die Privatautonomie zu berücksichtigen.[32]

Datenschutz ist stets als ein fortlaufender Prozess über das Setzen einmaliger Maßnahmen hinaus zu betrachten. Der Verantwortliche muss die ergriffenen Maßnahmen daher beispielsweise im Rahmen seines DSMS regelmäßig evaluieren und anpassen, wobei die DSGVO keine spezifischen Fristen für die Vornahme dieser Überprüfungen festlegt. Auftretende Änderungen der Rahmenbedingungen einer Verarbeitungstätigkeit können zu einer abweichenden Risikobewertung führen, die jedenfalls eine Anpassung der bisherigen Maßnahmen indiziert.[33]

Die DSB kann im Zuge ihrer Untersuchungsbefugnis festgestellte Verstöße gegen Art 24 DSGVO sanktionieren, indem sie in Ausübung ihrer Abhilfebefugnis nach Art 83 Abs 6 leg cit eine Geldbuße gegen den Verantwortlichen verhängt.[34] Das Konzept der regulierten Selbstregulierung gem Art 24 Abs 3 DSGVO ermöglicht es dem Verantwortlichen, die Erfüllung seiner datenschutzrechtlichen Pflichten durch Zertifizierungsverfahren einzelner Verarbeitungsvorgänge gem Art 42 DSGVO nachzuweisen.[35]

[30] DSB 13.9.2018, DSB-D123.070/0005-DSB/2018.
[31] Charta der Grundrechte der Europäischen Union, ABl. C 202 vom 7.6.2016, S. 389–405.
[32] DSB 23. 7. 2019, DSB-D123.822/0005-DSB/2019.
[33] *Schmidt/Brink* in BeckOK Datenschutzrecht [44] Art 24 Rn 22-24.
[34] *Hötzendorfer/Kastelitz/Tschohl* in DatKomm Art 24 DSGVO Rn 9.
[35] *Schmidt/Brink* in BeckOK Datenschutzrecht [44] Art 24 Rn 32-35.

2.1.2 Artikel 25 DSGVO: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Der Aspekt der Rechenschaftspflicht des Verantwortlichen ist konsequenterweise auch in den Prinzipien Datenschutz durch Technikgestaltung sowie Datenschutz durch datenschutzfreundliche Voreinstellungen in Art 25 DSGVO verankert. Der Verantwortliche hat demnach nicht nur zum Zeitpunkt der Festlegung seiner Verarbeitungsmittel, sondern auch im tatsächlichen Zeitpunkt der Verarbeitungstätigkeit sicherzustellen, dass die bestehenden Anforderungen der DSGVO erfüllt werden.[36]

Der normative Inhalt dieser Bestimmung richtet sich unmittelbar an den Verantwortlichen, eine mittelbare Wirkung gegenüber Auftragsverarbeitern wird jedoch gem Art 28 Abs 1 DSGVO begründet.[37] Unter diesen Gesichtspunkten entfaltet die Bestimmung auch faktische Wirkung gegenüber Herstellern von Softwareprodukten und sieht die Berücksichtigung datenschutzfreundlicher Voreinstellungen ebenso im Zuge öffentlicher Ausschreibungen vor.[38]

Im Auswahlprozess von Verarbeitungsmitteln wie Softwareprodukten, Dienstleistungen und Anwendungen, hat der Verantwortliche geeignete Maßnahmen und notwendige Garantien im Sinne dieser beiden abstrakt formulierten Prinzipien von Privacy by Design und Privacy by Default einzuhalten. Die zu implementierenden Maßnahmen können von der Minimierung personenbezogener Daten im Zuge von Verarbeitungsvorgängen bis zur Verbesserung bestehender DSMS und ihrer Sicherheitsfunktionen reichen.

Das Prinzip Privacy by Design gem Art 25 Abs 1 leg cit setzt auf eine möglichst frühe technische Integration der DSGVO, um Software unter der Einhaltung datenschutzrechtlicher Anforderungen gestalten und vertreiben zu können. Die Technik fungiert hier als Regulierungsmittel und gibt Schranken für die Handlungsmöglichkeiten von Nutzerinnen und Nutzern vor. In der Softwareentwicklung gilt es daher bereits bei der Planung eines Projektes datenschutzrechtliche Aspekte wie die Anwendung automatischer Löschkonzepte oder zeitgemäßer Verschlüsselungsmethoden zu berücksichtigen und entsprechende Strategien

[36] DSB 23.7.2019, DSB-D123.822/0005-DSB/2019.
[37] *Hötzendorfer/Kastelitz/Tschohl*, DatKomm Art 25 DSGVO Rz 17.
[38] ErwG 78 DSGVO.

umzusetzen. Durch diese Vorgehensweise soll der Schutz personenbezogener Daten ohne weitere, zu einem späteren Zeitpunkt erforderliche Handlungen erreicht werden.[39]

Der Verantwortliche hat die Pflicht, geeignete technische und organisatorische Maßnahmen im Zusammenhang mit seiner konkreten Verarbeitungstätigkeit unter der Berücksichtigung des aktuellen technischen Fortschrittes auf dem Mark festzulegen. Die fehlende Adaption an eine neue technische Veränderung kann eine Verletzung dieses Grundsatzes darstellen. Zur Erfassung des jeweiligen Stands der Technik bedarf es einer kontinuierlichen und dynamischen Betrachtungsweise.[40] Der Verantwortliche hat stets zu evaluieren, ob seine Verpflichtungen durch den Einsatz datenschutzfreundlicher Technologien eingehalten werden können oder weitere Maßnahmen erforderlich sind.

Das Prinzip Privacy by Default gem Art 25 Abs 2 leg cit zielt durch die Konkretisierung des Grundsatzes der Datenminimierung iSd Art 5 Abs 1 lit c DSGVO auf eine datenschutzfreundliche Voreinstellung der bereitgestellten Hardware, Software und Services ab. Aufgrund datenschutzfreundlicher Voreinstellungen sollen nur jene personenbezogenen Daten von Nutzerinnen und Nutzer verarbeitet werden, die für den vorliegenden Verarbeitungszweck zwingend erforderlich sind. Ein bewusstes Abweichen von diesem Schutzniveau darf ausschließlich durch ein aktives Optieren und nicht bereits aufgrund von Voreinstellungen erfolgen. [41]

Der Verantwortliche hat hier über die Konfiguration von Werten und Optionen innerhalb eines Systems zur Verarbeitung personenbezogener Daten zu entscheiden, um die erforderlichen Daten einer rechtmäßigen Verarbeitung aufgrund von Art 6 DSGVO zu definieren. Vor der Verwendung von Standardsoftware oder Individualsoftware von Drittherstellern hat der Verantwortliche eine umfassende Risikobewertung durchzuführen, um sicherzustellen, dass alle angewandten Funktionalitäten dem angestrebten Verarbeitungszweck entsprechen. Im Sinne der Zugänglichkeit erforderlicher Daten soll auch

[39] *Pollirer*, DSGVO und Informationssicherheit in Knyrim (Hrsg), Praxishandbuch Datenschutzrecht[4] Rn 10.41-10.45.

[40] EDSA Leitlinien 04/2019 zu Artikel 25 DSGVO, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[2] Rn 18f.

[41] *Pollirer*, DSGVO und Informationssicherheit in Knyrim (Hrsg), Praxishandbuch Datenschutzrecht[4] Rn 10.46-10.48.

der jeweilige Personenkreis im Vorfeld durch entsprechende Voreinstellungen definiert werden, der auf die personenbezogenen Daten der betroffenen Personen zugreifen darf.[42]

Am Beispiel der nationale Umsetzung der e-Privacy Richtlinie[43] sind datenschutzfreundliche Voreinstellungen in der Gestalt aktiver Informations- und Zustimmungspflichten bei der Verwendung von Cookies vorgesehen. Cookie-Kennungen können mit digitalen Geräten, Softwareanwendungen oder Protokollen natürlicher Personen in Verbindung gebracht werden und diese im Regelfall dadurch identifizieren.[44]

Unter Berücksichtigung der jeweiligen Umstände im Einzelfall, kann die Aufsichtsbehörde bei Verstößen gegen Art 25 DSGVO Geldbußen gem Art 83 Abs. 4 lit. a leg cit verhängen. Ein solcher Verstoß begründet jedoch keine zwingende Verletzung der betroffenen Personen in ihrem Grundrecht auf Datenschutz oder in ihren sonstigen subjektiven Rechten.[45] Das Vorliegen einer Zertifizierung nach Art 42 DSGVO kann gem Art 25 Abs 3 leg cit als Indiz zum Nachweis der Einhaltung der erforderlichen datenschutzrechtlichen Pflichten herangezogen werden.

2.1.3 Artikel 28 DSGVO: Auftragsverarbeiter

Der Begriffsdefinition in Art 4 Z 8 DSGVO zufolge, kann es sich bei Auftragsverarbeitern neben natürlichen Personen auch um juristische Personen, Behörden, Einrichtungen oder andere Stellen handeln, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

Zahlreiche Geschäftsprozesse und damit einhergehende Verarbeitungsvorgänge erfordern aus Gründen der Arbeitsteiligkeit und Spezialisierung oftmals die Beiziehung externer Auftragnehmer. Unter den Voraussetzungen des Art 28 DSGVO können Auftragsverarbeiter zur Durchführung datenschutzrechtlicher Verarbeitungstätigkeiten im Interesse des Verantwortlichen ausgewählt werden. Die Entscheidung über die Heranziehung und konkrete Auswahl von Auftragsverarbeitern obliegt stets dem Verantwortlichen und erfordert keine Einwilligung der Betroffenen.[46] In Abgrenzung zur gemeinsamen datenschutzrechtlichen

[42] EDSA Leitlinien 04/2019 zu Artikel 25 DSGVO Rn 41f.
[43] Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002.
[44] DSB 19.9.2023, 2023-0.632.875; ErwG 30 DSGVO.
[45] DSB 22.2.2021, 2020-0.833.281, ZVers 2021, 69.
[46] DSB 16.11.2018, DSB-D213.692/0001-DSB/2018.

Verantwortlichkeit nach Art 26 DSGVO, ist keine Zulässigkeitsprüfung der Datenübermittlung an Auftragsverarbeiter nach Art 5 f DSGVO erforderlich.

Das Auftragsverarbeitungsverhältnis wird durch den Abschluss eines Auftragsverarbeitungsvertrages begründet. Der Abschluss eines derartigen Vertrages zwischen Verantwortlichen und Auftragsverarbeitern erfolgt aufgrund einer individuell verhandelten Vereinbarung oder unter Gebrauch von Standardvertragsklauseln. Das bloße Rezitieren von Bestimmungen der DSGVO innerhalb des Vertrages ist jedoch zu vermeiden. Beide Varianten stellen gleichwertige Optionen dar und haben gem Art 28 Abs 3, 4 DSGVO Regelungen im Zusammenhang mit dem Verarbeitungsgegenstand, der Verarbeitungsdauer, Rechten und Pflichten des Verantwortlichen, der Art und dem Zweck sowie der betroffenen Datenkategorien der zugrundeliegenden Verarbeitungstätigkeiten aufzuweisen.[47]

Standardvertragsklauseln zur Auftragsverarbeitung werden durch die EK im Prüfverfahren gem Art 93 Abs 3 DSGVO oder nach erfolgter Annahme durch eine nationale Aufsichtsbehörde im Kohärenzverfahren gem Art 63 DSGVO festgelegt. Standardvertragsklauseln können zum Gegenstand von Verarbeitungsvorgängen werden, die einer datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO zuträglich sind.[48] Die getroffenen Datensicherungsmaßnahmen zur Einhaltung der erforderlichen Maßnahmen nach Art 32 DSGVO durch den Auftragsverarbeiter sind verpflichtend in den Auftragsverarbeitungsvertrag aufzunehmen. Auf diese Weise kann der Verantwortliche Kenntnis über technisch-organisatorische Maßnahmen seiner Auftragsverarbeiter zur Einhaltung seiner eigenen Nachweispflicht gem Art 24 DSGVO erlangen. [49]

Der Verantwortliche hat bei der Auswahl geeigneter Auftragsverarbeiter sicherzustellen, dass diese hinreichende Garantien für die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen aufweisen können. Als Kriterien für das Erfordernis der Eignung können etwa betriebliche Ressourcen, fachliche Kenntnisse sowie die Zuverlässigkeit der Auftragsverarbeiter herangezogen werden.[50] Diese Verpflichtung des Verantwortlichen beschränkt sich jedoch nicht auf den bloßen Auswahlzeitpunkt, sondern besteht konsequenterweise in Form einer fortlaufenden Prüfpflicht für die gesamte Dauer des Auftragsverarbeitungsverhältnisses. Bei rechtswidriger Überschreitung eingeräumter

[47] *Jahnel*, Kommentar zur Datenschutz-Grundverordnung Art 28 DSGVO Rn 1-3, 7-14.
[48] EDSA Leitlinien 07/2020 Rn 93 ff.
[49] *Jahnel*, Datenschutz-Grundverordnung Art 28 DSGVO Rn 22.
[50] ErwG 81 DSGVO.

Befugnisse sowie eigenmächtiger Entscheidung über Zwecke und Mittel liegt ein Auftragsverarbeitungsexzess vor. Auftragsverarbeiter gelten im Zusammenhang mit den betroffenen Datenverarbeitungsvorgängen sodann selbst als Verantwortliche. Bei Vorliegen eines materiellen oder immateriellen Schadens aufgrund eines Verstoßes gegen die DSGVO durch weisungswidrige Datenverarbeitung können Auftragsverarbeiter gem Art 82 DSGVO nach zivilrechtlichen Gesichtspunkten haftbar werden.

Die DSB ist bei Verstößen gegen die Pflichten nach Art 28 DSGVO zur Verhängung von Geldbußen gem Art 83 Abs. 4 lit a DSGVO gegen Auftragsverarbeiter legitimiert, wobei Auftragsverarbeiter auch für die Einhaltung bestehender Pflichten durch etwaige Sub-Auftragsverarbeiter haften.[51] Die Einhaltung eines genehmigten Zertifizierungsverfahrens nach Art 42 DSGVO kann gem Art 28 Abs 5 DSGVO als Indiz zum Nachweis hinreichender Garantien durch Auftragsverarbeiter herangezogen und von der DSB als Aufsichtsbehörde zur Bestimmung der Strafzumessung im Zuge von Geldbußeverfahren berücksichtigt werden.[52]

2.1.4 Artikel 32 DSGVO: Sicherheit der Verarbeitung

Die zunehmende Anzahl an Vorfällen von Cyberkriminalität[53] sowie das rasant ansteigende Aufkommen an vernetzten, über das Internet kommunizierenden Geräten[54] verdeutlichen das Erfordernis von Maßnahmen zur Einhaltung der Informationssicherheit.

Verantwortliche und Auftragsverarbeiter müssen auf der Grundlage einer risikobasierten Abwägung geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Schutzniveau für die vorzunehmenden Verarbeitungsvorgänge garantieren zu können. Hierbei gilt es den jeweiligen Stand der Technik, die Eintrittswahrscheinlichkeit eines Risikos sowie näheren Umstände der Verarbeitung wie etwa den Verarbeitungszweck zu berücksichtigen.[55]

Artikel 32 Abs 1 DSGVO enthält eine demonstrative Aufzählung technischer und organisatorischer Maßnahmen, die dazu geeignet sind, ein angemessenes Schutzniveau

[51] *Geuer/Reinisch*, Haftung des Auftragsverarbeiters nach der DSGVO, Dako 2019/47, 82–85.
[52] *Bogendorfer* in Knyrim, DatKomm Art 28 DSGVO Rn 56 – 57.
[53] Sophos Ransomware Report 2023, Stand: Mai 2023, abrufbar unter: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.
[54] Internet of Things (IoT), siehe dazu: https://findstack.de/resources/internet-of-things-statistics/ (abgerufen am 21.10.2023).
[55] *Pollirer* in Knyrim, DatKomm Art 32 DSGVO Rn 3.

personenbezogener Daten sicherzustellen. An dieser Stelle werden die Pseudonymisierung und Verschlüsselung der Daten neben der Möglichkeit zur Datenwiederherstellung binnen angemessener Zeit genannt. Die DSGVO legt keine Kategorien von Verarbeitungstätigkeiten für den erforderlichen Einsatz von Verschlüsselungsmethoden fest, dies liegt im Ermessen des jeweiligen Verantwortlichen.[56]

Die entsprechenden technischen Systeme sind auf ihre Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit zu überprüfen, wobei Prozesse zur regelmäßigen Evaluierung und Überprüfung der getroffenen Sicherheitsmaßnahmen zu implementieren sind.[57] Die zu berücksichtigenden Risiken im Zusammenhang mit personenbezogenen Daten durch Vernichtung, Verlust, Veränderung, unbefugte Weitergabe und unberechtigten Zugang werden in Art 32 Abs 2 leg cit demonstrative aufgezählt. Betroffene Personen haben gegenüber Verantwortlichen keinen durchsetzbaren Rechtsanspruch auf die Implementierung spezifischer Maßnahmen.[58]

Verantwortliche und Auftragsverarbeiter haben gem Art 32 Abs 4 leg cit als organisatorische Maßnahme sicherzustellen, dass Mitarbeiterinnen und Mitarbeiter in datenschutzrechtlichen und sicherheitstechnischen Fragen geschult und entsprechende Maßnahmen wie geeignete Zugriffsberechtigungen und Passwortrichtlinien ergriffen werden.

Angesichts des fortschreitenden technologischen Fortschrittes, wie beispielsweise im Zusammenhang mit künstlicher Intelligenz und Large Language Models[59], werden immer größer werdende Datenmengen benötigt.[60] Zur datenschutzkonformen Verarbeitung derartiger Datenmengen stellen Anonymisierungsverfahren eine interessante und aufwändige Lösung zugleich dar. Daten weisen nach erfolgter Anonymisierung keinen Bezug zu natürlichen Personen mehr auf und fallen aufgrund mangelnder Identifizierbarkeit nicht in den Anwendungsbereich der DSGVO.[61]

Im Zuge absoluter Anonymisierungen erfolgt die Neutralisierung aller Identifikationskriterien, wodurch keine Rekonstruktion von Einzelangaben mehr möglich ist.

[56] *Pollirer* in Knyrim, DatKomm Art 32 DSGVO Rn 45.
[57] EuGH 14.12.2023, C-340/21.
[58] DSB 13.09.2018, DSB-D123.070/0005-DSB/2018.
[59] https://datasolut.com/was-ist-ein-large-language-model/ (abgerufen am 11.10.2023).
[60] Anm: In diesem Zusammenhang kommt es vermehrt zum Einsatz von Datenmengen im Bereich von Petabyte (1 Petabyte ≙ 1.000 Terrabyte ≙ 1.000.000 Gigabyte ≙ in etwa 500 Milliarden Dokumentseiten), https://www.ionos.at/digitalguide/websites/web-entwicklung/was-ist-ein-petabyte/ (abgerufen am 11.10.2023).
[61] ErwG 26 DSGVO.

Diese Form der Anonymisierung ist aus datenschutzrechtlicher Sicht jedoch nicht immer erforderlich. Im Bereich faktischer Anonymisierungen wird anhand von Risikoprognosen nur eine bestimmte Anzahl an Datenmerkmalen entfernt. Eine verlässliche Identifizierung kann dann nach dem jeweils aktuellen Stand der Technik mit vernünftigerweise zu erwartendem Aufwand nicht mehr erreicht werden. Die sog. probabilistische Anonymisierung ist ein faktisches Anonymisierungsverfahren und stellt auf eine Ausgeglichenheit zwischen der Anonymität und dem jeweiligen Informationsgehalt der Daten ab. Die hierbei angewandten Methoden der „K-Anonymität" sowie „Differential Privacy" verändern in einer Einzelbetrachtung die zugrundeliegenden Datensätze oftmals stärker, als es unbedingt erforderlich ist. Eine Kombination aus beiden Methoden kann den erforderlichen Anonymisierungsgrad durch das kontrollierte Hinzufügen eines zufälligen Rauschens nach mathematischen Grundsätzen jedoch sicherstellen.[62]

Pseudonymisierte Daten gem Art 4 Z 5 DSGVO können unter der Heranziehung zusätzlicher Informationen natürlichen Personen zugeordnet werden und unterliegen somit der DSGVO, da zugrundeliegende Identifikationsmerkmale nicht vollständig beseitigt werden. Bei der Beurteilung der Identifizierbarkeit natürlicher Personen gilt es, objektivierbare Faktoren wie die Mittel, den erforderlichen Zeitaufwand sowie die damit verbundenen Kosten zu berücksichtigen. Um ein hohes Schutzniveau durch Pseudonymisierungsmethoden gewährleisten zu können, bedarf es entsprechender Zuordnungsregeln.[63]

Als Pseudonymisierungsmethode im Bereich der Kryptographie kann eine effektive Verschleierung von Identitäten durch sog. multi-party Computation erreicht werden.[64] Es handelt sich dabei um eine gesicherte Methode der Zugriffskontrolle für verteilte Datenanalysen. Mehrere Teilnehmerinnen und Teilnehmer arbeiten an gemeinsamen Berechnungen, wobei jede Person nur über einen Teil der entsprechenden Daten verfügt und diese während des gesamten Vorganges stets geheim bleiben.[65]

---

[62] *Heiler/Ciarnau*, Datenanonymisierung der Schlüssel zum Erfolg, ecolex 2022/114, 166-167.

[63] ErwG 26 DSGVO.

[64] *Tschohl, Kastelitz, Hospes, Rothmund-Burgwall*, Datenschutzrechtliche Fragestellungen beim Einsatz von Clouddienste-Anbietern 82.

[65] vgl zur Zugriffskontrolle bei Multi-party Computation: https://technology.a-sit.at/zugriffskontrolle-fuer-verteilte-datenanalyse-mittels-secure-multi-party-computation/ (abgerufen am 18.10.2023).

In der Rechtssache Breyer[66] judizierte der EuGH, dass es sich bei dynamischen IP-Adressen unter bestimmten Voraussetzungen um personenbezogene Daten handeln kann. Dies betrifft auch jene Anwendungsfälle, in denen Webseitenbetreiber die Bestimmbarkeit einzelner Personen mit vernünftigerweise einzusetzenden Mitteln erwirken können. Serverseitiges Tracking stellt hier im Vergleich zu klassischem clientseitigen Tracking eine geeignete technische Möglichkeit dar, um die datenschutzkonforme Übertragung personenbezogener Daten mit Hilfe von Proxyservern sicherzustellen.[67] Unter Heranziehung der in ErwG 26 DSGVO verankerten Zweck-Mittel-Abwägung kann durch die ausschließliche Zurverfügungstellung pseudonymisierter Datensätze bei der Übermittlung an Datenverarbeitende eine anonymisierende Wirkung herbeigeführt werden.[68]

Datenschutzrechtliche Vorgaben für die sichere Verarbeitung personenbezogener Daten werden durch Rechtsakte aus dem technischen Bereich der Cybersecurity flankiert.[69] Hierzu zählt unter anderem die zurzeit im parlamentarischen Gesetzgebungsprozess befindliche, nationale Umsetzung der NIS 2-Richtline[70] sowie der Digital Operation Resilience Act - Dora[71].

Bei einem Verstoß gegen die Bestimmungen gem Art 32 DSGVO kann die DSB als Aufsichtsbehörde gem Art 83 Abs 4 lit a DSGVO eine Geldbuße gegen Verantwortliche und Auftragsverarbeiter verhängen. Zur Minderung des bestehenden Haftungsrisikos sowie zum Nachweis der getroffenen Maßnahmen empfiehlt sich eine gesamtheitliche Betrachtungsweise sowie der Aufbau eines performanten ISMS innerhalb der jeweiligen Organisation.[72]

---

[66] EuGH 19.10.2016, C-582/14.

[67] https://dr-dsgvo.de/serverseitiges-tracking-was-bedeutet-das-und-wie-sieht-es-mit-dem-datenschutz-aus/ (abgerufen am 18.10.2023).

[68] *Hofer*, Überlegungen zur anonymisierenden Wirkung der Pseudonymisierung im Außenverhältnis am Beispiel von Cloud-Computing, jusIT, 5/2022, 173-176.

[69] *Stadler/Drolz*, Pflicht und Kür bei der Abwehr von Cybercrime, Die Presse 2023/09/03.

[70] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnungen(EG) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.

[71] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) 2026/1011.

[72] *Pollirer* in Knyrim, DatKomm Art 32 DSGVO Rn 27.

Die Einhaltung eines genehmigten Zertifizierungsverfahrens nach Art 42 DSGVO kann gem Art 32 Abs 3 DSGVO als Faktor zum Nachweis der Einhaltung von Datensicherheitsmaßnahmen herangezogen werden.

2.1.5. Artikel 24, 25 und 32 DSGVO: Genüberstellung und Wechselwirkungen

Die DSGVO zielt mit ihren Bestimmungen zum risikobasierten Ansatz auf die Ermittlung eines kohärenten Systems zum Schutz natürlicher Personen und ihrer personenbezogenen Daten ab. Der normative Regelungsgehalt der Artikel 24, 25 und 32 DSGVO überschneidet sich teilweise, wobei sich einzelne Bestimmungen jedoch grundlegend unterscheiden.[73]

Während sich die Pflichten gem Art 24, 25 DSGVO unmittelbar an den Verantwortlichen und nur mittelbar durch Art 28 DSGVO an Auftragsverarbeiter als Normadressaten richten, adressiert Art 32 DSGVO die beiden datenschutzrechtlichen Akteure gleichermaßen.[74]

Die Artikel 25 und 32 DSGVO beinhalten speziellere Regelungen gegenüber Art 24 DSGVO, der dem Verantwortlichen als zentrale Norm die grundlegende Verantwortung und Haftung für Verarbeitungsvorgänge personenbezogener Daten auferlegt. Die Pflichten des Verantwortlichen werden etwa durch die Einhaltung technischer und organisatorischer Maßnahmen durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu einem möglichst frühen Zeitpunkt gem Art 25 DSGVO konkretisiert.

Diese allgemeinen Pflichten werden mit Art 32 DSGVO schließlich um Aspekte der sicheren Datenverarbeitung durch die Einhaltung von TOMs weiter konkretisiert. Das Kriterium der Beachtung unterschiedlicher Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen durch Verantwortliche und Auftragsverarbeiter vollendet den risikobasierten Ansatz um die Ausrichtung auf TOMs.[75] Es ist kein Abgehen von Maßnahmen nach Art 32 DSGVO mittels Einwilligung möglich, da die Vorgaben der DSGVO zwingend einzuhalten sind.[76]

[73] EDSA Leitlinien 04/2019 Rn 29 - 32.
[74] Pollirer in Knyrim, DatKomm Art 32 DSGVO Rn 19.
[75] *Pollirer* in Knyrim, DatKomm Art 32 DSGVO Rn 26.
[76] DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018.

2.2 Zertifizierungen

In Ermangelung einer allgemeingültigen Legaldefinition, kann die Durchführung von Zertifizierungen als formeller Vorgang angesehen werden, um die Einhaltung von Normen und Qualitätskriterien zu belegen. Als Zertifizierungsgegenstand kommen Personen, einzelne Prozesse, Produkte sowie Managementsysteme, die nach spezifizierbaren Normen oder technischen Regulatorien eingeführt wurden, in Frage. Managementsysteme in den Bereichen des Datenschutzes und der Informationssicherheit werden nach dem aktuellen Stand der Technik zunehmend komplexer, weshalb ein erhöhter Bedarf an objektivierbaren Maßstäben für diese Prozesse und Strukturen vorliegt. Im freien Wettbewerb können Unternehmen bestehende Zertifizierungen nicht nur zum Nachweis der Einhaltung ihrer Pflichten und dadurch zur Reduzierung ihrer eigenen Haftung, sondern auch als Wettbewerbsvorteil gegenüber Mitbewerbern einsetzen.[77]

Die verpflichtende Vornahme von Zertifizierungen kann in einzelnen Geschäftszweigen wie etwa in der Luftfahrt oder im Bauwesen zur Einhaltung einschlägiger Vorschriften erforderlich sein. Darüber hinaus können Zertifizierungen effektive Compliance – Tools zur Vertrauensbildung, Risikominimierung sowie zur nachweislichen Anpassung an Wünsche und Anforderungen von Kundinnen und Kunden eingesetzt werden. Um ein möglichst hohes Maß an Transparenz und Sicherheit durch die Zertifizierung zu ermöglichen, ist diese von einer unabhängigen, von der zertifizierungswerbenden Organisation unterschiedlichen Stelle durchzuführen. Diese Stelle führt Audits im Rahmen des Zertifizierungsgegenstands anhand festgelegter Kriterien sowie unter der Berücksichtigung branchenüblicher Standards und Gegebenheiten durch.

Die erste Phase einer Zertifizierung beginnt zumeist mit der Evaluation der Ziele und Anforderungen einer geplanten Zertifizierung mit der zu zertifizierenden Organisation. In weiterer Folge werden Unterlagen, Dokumentationen und Informationen zusammengetragen, um in einer zweiten Phase verlässlich beurteilen zu können, ob das zu prüfende Managementsystem den Anforderungen der für die Konformitätsprüfung einschlägigen Normen entspricht. Im Zuge der dritten Phase erfolgt schließlich die Bewertung der

[77] https://www.din-iso-zertifizierung-qms-handbuch.de/zertifizierung/ (abgerufen am 28.10.2023).

ermittelten Ergebnisse im Zertifizierungsaudit sowie die Entscheidung über die Ausstellung des entsprechenden Zertifikats.

Zertifizierungen stellen eine Beurteilung zu einem bestimmten Stichtag dar und weisen eine zeitlich begrenzte Gültigkeitsdauer auf. Je nach Ausgestaltung des jeweiligen Zertifizierungsverfahrens sind jährliche Überwachungsaudits und periodische Rezertifizierungen erforderlich, um die Gültigkeit des Zertifikats aufrecht zu erhalten. Zertifikate akkreditierter Zertifizierungsstellen genießen aufgrund der vorangegangenen Prüfung und Anerkennung ihrer Kompetenzen und der Eignung zur Durchführung von derartigen Zertifizierungen eine hohe Aussagekraft.[78]

Als Vorbereitung auf die tatsächliche Zertifizierung können sog. friendly Audits durchgeführt werden. Der Ablauf eines solchen Vorbereitungsaudits entspricht weitestgehend den einzelnen Phasen des Zertifizierungsverfahrens, einen wesentlichen Bestandteil stellt jedoch die sog. Gap-Analyse dar. Der zu zertifizierenden Organisation werden in diesem Rahmen bestehende Schwachstellen und Dokumentationslücken ihres Managementsystems aufgezeigt, bevor ein entsprechendes Audit zu Testzwecken durchgeführt wird. Die daraus gewonnenen Erkenntnisse können für Organisationen einen wertvollen Beitrag für die Vorbereitung auf die angestrebte Zertifizierung leisten.[79]

In weiterer Folge wird zwischen technischen Zertifizierungen von Informationssicherheitsmanagementsystemen, nationalen Standards für Datenschutz-managementsysteme, privaten Datenschutzzertifikaten sowie datenschutzrechtlichen Zertifizierungen gem Art 42 DSGVO unterschieden.[80]

2.2.1 Technische Zertifizierungen von Informationssicherheitsmanagementsystemen

Die fortschreitende Digitalisierung erfordert die Einhaltung hoher Standards im Bereich der Informationssicherheit, um eine erfolgreiche und sichere Arbeitsweise gewährleisten zu können.[81]

Informationssicherheitsmanagementsysteme kommen in zahlreichen Organisationen zum Einsatz, um Standards und Anforderungen im Bereich der Informationssicherheit

[78] https://www.dqsglobal.com/de-de/ueber-uns/zertifizierung/was-ist-eine-zertifizierung (abgerufen am 28.10.2023).
[79] https://www.dqsglobal.com/de-de/wissen/blog/was-ist-eine-gap-analyse (abgerufen am 28.10.2023).
[80] *Novotny/Menzel*, Datenschutz in der Schule, Dako 2023/4, 7-9.
[81] *Löffler*, Cyber Security in der Risikoberichterstattung, Dako 2021, 118.

sicherzustellen. Im Sinne einer ganzheitlichen Betrachtungsweise sind hierbei Ansätze des Risikomanagements, interner Kontrollsysteme sowie des Compliance Managements vertreten. Bereits im Zeitpunkt der Implementierung eines geeigneten ISMS gilt es, individuelle Sicherheitsziele und Sicherheitsmaßnahmen zu definieren sowie auch geeignete Prozesse zur periodischen Evaluierung der definierten Parameter einzuführen.[82]

Technische Normen werden durch anerkannte Normungsorganisationen akkreditiert und betreffen allgemeingültige Standards, Leitlinien und Merkmale für abgegrenzte Tätigkeitsbereiche. Derartige Normen erlangen im Regelfall eine hohe Verkehrsgeltung und dienen oftmals als Maßstab dafür, ob bestimmte Maßnahmen dem Stand der Technik entsprechen. Die Anwendung und Einhaltung dieser Empfehlungen erlangt schließlich Verbindlichkeit, sobald dies vertraglich vereinbart wird oder der jeweilige Gesetzgeber eine Norm für verbindlich erklärt.[83]

Die technische Norm ISO/IEC 27701[84] der internationalen Organisation für Standardisierung ist die konsequente Weiterentwicklung der Vorgängerbestimmungen ISO/IEC 27001 und ISO/IEC 27002 und beinhaltet als technische Antwort auf die DSGVO erstmals Leitlinien für Verantwortliche und Auftragsverarbeiter. Terminologisch wurde die datenschutzrechtliche Nomenklatur jedoch ohne die bedeutende Vornahme inhaltlicher Neuerungen in dieser Norm angepasst. Im Bereich von ISMS gibt die Norm international gültige Standards für die Implementierung von Sicherheitsmerkmalen und Prozessen anhand eines generisch prozessorientierten Ansatzes vor. Die getroffenen Spezifikationen betreffen, über die erstmalige Einrichtung hinaus, auch die praktische Umsetzung und Weiterentwicklung geeigneter Anforderungen in der jeweiligen Organisation.[85]

Eine Zertifizierung nach einschlägigen technischen Normen kann im Wirtschaftsleben sowie gegenüber Aufsichtsbehörden zu einem erheblichen Wettbewerbsvorteil sowie zur Minimierung von Geschäfts- und Haftungsrisiken beitragen.

[82] *Niederbacher*, Datenschutz und Informationssicherheitsmanagementsysteme , GRCaktuell 2018, 122.

[83] https://www.wko.at/ce-kennzeichnung-normen/grundlagen-normung-oesterreich (abgerufen am 04.11.2023).

[84] Internationale technische Standards im Bereich der Informationssicherheit, Cybersicherheit, Datenschutz-Informationsmanagementsyseme und Anforderungen, ICS – Klassifikation: 03.100.70, 35.030.

[85] https://www.beuth.de/de/norm/din-en-iso-iec-27701/339507443 (abgerufen am 04.11.2023).

Die wesentlichen Normen, Standards und Entwicklungen im Bereich der IKT – Sicherheit werden regelmäßig im IKT – Sicherheitsportal[86] sowie auf der Webseite des BSI[87] angeführt.

2.2.2 Datenschutzmanagementsysteme – ÖNORM A 2017

Jeder Verantwortliche ist zur Einhaltung gesetzlicher Datenschutzanforderungen verpflichtet und hat eine ganzheitliche Datenschutzkultur durch die sorgfältige Überprüfung betroffener Datenflüsse und Verarbeitungstätigkeiten im Zuge seiner Rechenschaftspflicht nach Art 5 DSGVO nachweisen können.[88] Die Einhaltung datenschutzrechtlicher Pflichten war bereits vor dem Inkrafttreten der DSGVO aufgrund diverser Rechtsakte vorgesehen. Diese sieht jedoch eine Vielzahl an Neuerungen im Zusammenhang mit Prozessen und technischen Sicherheitsmaßnahmen als Ausgangsgrundlage für die Organisation des Datenschutzmanagements vor.[89]

Datenschutzmanagementsysteme beziehen sich in gesamtheitlich strukturierter Form auf alle Tätigkeiten zur Einhaltung des Datenschutzes und adressieren in diesem Zusammenhang überwiegend steuernde Tätigkeiten.[90] Angesichts der grundsätzlich vorzunehmenden Abgrenzung von DSMS zu anderen Managementsystemen, können mithilfe einer interdisziplinären Betrachtungsweise jedenfalls Wechselwirkungen und Überschneidungen einzelner Prozesse innerhalb einer Organisation genutzt werden.[91]

Das Datenschutzmanagement dient der systematischen Analyse, Planung und Umsetzung von erforderlichen Maßnahmen zur Einhaltung datenschutzrechtlicher Vorgaben. Dabei handelt es sich um keine in sich geschlossene Softwarelösung, sondern vielmehr um dynamische Aspekte innerhalb eines beweglichen Systems, das sich im Zeitverlauf verändern kann. Es besteht keine einheitliche Dokumentationspflicht eines DSMS, da die datenschutzrechtlich relevanten Vorgänge einer Organisation auch einzeln betrachtet werden können. Eine transparente und nachvollziehbare Dokumentation erscheint jedenfalls vorteilhaft, da die entsprechenden Unterlagen der jeweiligen Aufsichtsbehörde dadurch fristwahrend und ohne

[86] https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Normen-und-Standards.html (abgerufen am 04.11.2023).
[87] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html (abgerufen am 04.11.2023).
[88] *Pachinger*, Zeit wird knapp: Sechs Monate bis zum neuen Datenschutz, Die Presse 2017/47/05.
[89] *Lamprecht*, Cyber-Security: Das unterschätzte Risiko?, DJA 2018/9, 28.
[90] *Schefzig* in Moos/Schefzig/Arning, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap. 10 Rn 4.
[91] *Roth*, Die systemische Umsetzung von Organisationspflichten des Verantwortlichen am Beispiel des Art. 30 DSGVO, DSB 2023, 230.

weiteren, erheblichen Arbeitsaufwand vorgelegt werden können. Einzelne Prozesse können dadurch besser abgebildet und im Sinne der „Plan – Do – Check –Act“ Methode optimiert werden[92]:

• In der Planungsphase werden datenschutzrechtliche Grundlagen durch die Durchführung eines Soll-Ist-Vergleichs evaluiert.
• In der Umsetzungsphase sollen bestehende Pflichten mit den bisher implementierten Prozessen und Abläufen abgeglichen und auf ihre Umsetzbarkeit geprüft werden.
• Im Zuge der Evaluationsphase erfolgen periodische Überprüfungen,
• die schließlich in der Korrekturphase genutzt werden können, um das DSMS weiter zu verbessern und aktuell zu halten.

Die Intensität und Ausgestaltung eines DSMS richtet sich nach dem individuellen Risikoprofil einer Organisation, das aus einer Vielzahl von Faktoren wie den Kategorien und dem Umfang verarbeiteter, personenbezogener Daten sowie dem damit einhergehenden Risiko betroffener Personen resultiert. Die auf ein Risikoprofil abgestimmten Maßnahmen unterliegen stets einer Einzelfallbetrachtung und sollen durch eine möglichst effiziente Abstimmung von Synergieeffekten profitieren.[93]

Als Unterfall des Technologiebegriffes „Legal Tech“ stellen Anwendungen aus dem Bereich des „Privacy Tech“ Lösungen zur technikorientierten Umsetzung datenschutzrechtlicher Pflichten zur Verfügung. In Abgrenzung zu „Privacy Enhancing Technologies“ bei technischen Lösungen wie im Zusammenhang mit den Prinzipien Privacy by Design und Privacy by Default, handelt es sich bei „Privacy Tech“ Lösungen um eigenständige Anwendungen durch neue Technologien.[94]

Normen und Standards sind in beinahe allen Lebensbereichen vertreten und lassen sich nicht auf die bereits genannten technischen ISO - Standards beschränken. Darüber hinaus bestehen

[92] https://www.ensecur.de/datenschutzberatung/datenschutzlexikon/technik-organisation/datenschutzmanagementsystem/ (abgerufen am 04.11.2023).

[93] *Schefzig* in Moos/Schefzig/Arning, Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle[2] Kap. 10 Rn 46.

[94] *Struck/ Aßhoff*, Privacy Tech als Anwendungsfall für Legal Tech Applikationen Technologiegestütztes Datenschutzmanagement - neue Anwendungsfälle treiben die Digitalisierung und Integration voran, LTZ 2022, 224 – 225.

Europäische Normen (EN), die in das österreichische Normenwerk übernommen wurden (ÖNORM EN) sowie rein nationale Standards (ÖNORM). In Österreich ist der Verein Austrian Standards für die Entwicklung nationaler Standards zuständig.[95] Die Voraussetzungen zur Erteilung der Befugnis als Normungsorganisation, sowie die damit verbundenen Aufgaben und Pflichten, werden in Österreich im NormG 2016 geregelt.[96]

Der Aufbau und die Gestaltung nationaler ÖNORMEN sowie die Festlegung unterschiedlicher Verbindlichkeitsgrade innerhalb der jeweiligen Anforderungen („müssen – sollen – dürfen – können") werden durch eine Richtlinie der Austria Standards vorgegeben.[97]

Wenn der Stand einer neuartigen, in einem engen zeitlichen Kontext zu vollziehenden Entwicklung dokumentiert werden soll, kommen sog. „ONR" zur Anwendung. Hierbei handelt es sich um normative Dokumente, die im Zuge ihres raschen Entwicklungsprozesses nicht jede Anforderung einer ÖNORM im klassischen Sinn erfüllen und daher als eine Mittellösung zwischen Normen und Spezifikationen angesehen werden kann, die innerhalb einer Organisation entwickelt wurden.[98]

Die ÖNORM A 2017[99] legt innerhalb Österreichs einen nationalen Standard für die Organisation von DSMS fest. Anhand der Buchstabenkombination in der Kennnummer kann diese ÖNORM dem Fachbereich allgemeiner Normen zugewiesen werden.[100] Durch die festgelegten Anforderungen können Organisationen spezifische Maßnahmen für die Implementierung und fortlaufende Verbesserung ihres DSMS umsetzen. Im direkten Vergleich zur technischen Norm ISO/IEC 27701, wurden die Kontrollmechanismen im

[95] https://www.oesterreich.gv.at/themen/dokumente_und_recht/normen/Seite.2560002.html (abgerufen am 05.11.2023).

[96] Bundesgesetz über das Normenwesen (Normengesetz 2016 – NormG 2016), BGBl. I Nr. 153/2015.

[97] Richtlinie 1 Teil 1: Aufbau und Gestaltung von nationalen Regelwerken von Austrian Standards International, https://www.austrian-standards.at/dokumente/footer-links/rechtliches-agb/Richtlinie%201-1_2022-11.pdf (abgerufen am 05.11.2023).

[98] https://www.austrian-standards.at/de/standardisierung/warum-standards/grundbegriffe/onr (abgerufen am 05.11.2023).

[99] https://shop.austrian-standards.at/action/de/public/details/730065/OENORM_A_2017_2023_06_01 (abgerufen am 05.11.2023).

[100] Anm: Die darüber hinaus weit verbreitete Buchstabenkombination „B" steht für den Fachbereich „Bau", die Buchstabenkombination „D" steht für den Fachbereich „Dienstleistung".

Bereich des Datenschutzmanagements auf dieser normativen Ebene grundlegend überarbeitet.[101]

Inhaltlich setzt die ÖNORM A 2017 auf das primäre Verständnis der eigenen Organisation durch die Bestimmung relevanter Themen, Anforderungen sowie betroffener Parteien in Bezug auf den Datenschutz. Dieses Vorgehen ermöglicht im Hinblick auf das DSMS eine dokumentierte Festlegung von Anwendungsbereichen und Grenzen. In weiterer Folge werden die Pflichten der obersten Leitung einer Organisation zur Sicherstellung geeigneter Datenschutzziele und deren fortlaufender Verbesserung aufgezeigt. Verantwortlichkeiten und Befugnisse über die Konformität eines DSMS mit den Vorgaben der gegenständlichen ÖNORM müssen den obersten Organen zugewiesen werden. Berichte über die Entwicklung des Managementsystems sind in periodischen Abständen erforderlich. [102]

Darüber hinaus muss eine Organisation wirksame Maßnahmen zur Bestimmung von Chancen und Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten sowie geeignete Prozesse für die Durchführung einer Datenschutzrisikobeurteilung implementieren. Als wesentliche Punkt sind an dieser Stelle die Verfügbarkeit ausreichender Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die kontinuierliche Verbesserung eines DSMS genannt. Jede Organisation hat sicherzustellen, dass ihre Mitarbeiterinnen und Mitarbeiter im Bereich des Datenschutzes ausreichend geschult werden, an regelmäßigen Fortbildungen teilnehmen können sowie ausreichende personelle Ressourcen durch die Anstellung und Beauftragung geeigneter Personen vorhanden sind. Diese Vorgaben werden durch Bewusstseinsbildung für die jeweilige Datenschutzpolitik sowie durch eine Dokumentation des DSMS in angemessenem Ausmaß abgerundet. Neben entsprechenden Maßnahmen im Zusammenhang mit Betroffenenrechten unter Berücksichtigung datenschutzrechtlicher Grundsätze werden auch verpflichtende Vorgaben bei Datenschutzvorfällen angeführt.[103]

Zur Überwachung der Wirksamkeit bestehender Maßnahmen sind Mess- und Bewertungsmethoden sowie die Durchführung interner Audits in regelmäßigen Abständen vorgesehen. In den normativen Anhängen A und B der ÖNORM findet sich schließlich eine

[101] https://www.austrian-standards.at/de/newsroom/pressemeldungen/datenschutz-management-so-profitieren-kmu-von-der-neuen-oenorm-a-2017 (abgerufen am 05.11.2023).
[102] ÖNOM A 2017:2023-06, 4-8.
[103] ÖNOM A 2017:2023-06, 10 f.

Auflistung von Maßnahmenzielen und Maßnahmen sowohl für Verantwortliche als auch für Auftragsverarbeiter.[104]

2.2.3 EuroPriSe – European Privacy Seal

Das private Unternehmen EuroPriSe Cert GmbH bietet seit dem Jahr 2007 eine Datenschutzzertifizierung auf der Grundlage eines ursprünglich von der Europäischen Kommission geförderten Projektes an. Diese Zertifizierung mit dem EuroPriSe-Siegel kann sowohl für IT-Produkte als auch für IT-basierte Dienste ausgestellt werden, wenn die gesamte Datenverarbeitung DSGVO – konform erfolgt.[105] Die Zertifizierungskriterien werden in einem umfangreichen Kriterienkatalog beschrieben und stellen hauptsächlich auf die Grundsätze der Datenverarbeitung, risikobasierte Ansätze sowie auf die Wahrung von Betroffenenrechten ab.[106]

Die zuständige deutsche Aufsichtsbehörde genehmigte die eingereichten Kriterien der EuroPriSe Cert GmbH als Zertifizierungsstelle zur Durchführung datenschutzrechtlicher Zertifizierungen nach Art 42 DSGVO im Oktober 2022 als erstes Unternehmen innerhalb der EU.

Die Akkreditierung zur Zertifizierungsstelle durch die DAkkS war zum Bearbeitungszeitpunkt dieser Arbeit jedoch noch ausständig.[107] Das Unternehmen scheint die zukünftige Durchführung der datenschutzrechtlichen Zertifizierungen nach Art 42 DSGVO speziell auf Verarbeitungstätigkeiten personenbezogener Daten von Auftragsverarbeitern auszurichten.[108]

[104] ÖNORM A 2017:2023-06, 18, 21-28.

[105] https://www.euprivacyseal.com/de/certification-schemes/scheme-for-products-and-services/ (abgerufen am 06.11.2023).

[106] https://www.euprivacyseal.com/wp-content/uploads/2023/01/EuroPriSe-Criteria-v201701_final.pdf (abgerufen am 06.11.2023).

[107] https://www.euprivacyseal.com/de/europrise-cert-gmbh-is-the-first-private-company-in-the-eu-with-certification-criteria-approved-by-the-competent-supervisory-authority/ (abgerufen am 06.11.2023).

[108] https://www.euprivacyseal.com/de/certification-schemes/scheme-for-processors/ (abgerufen am 06.11.2023).

2.2.5 Die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO

Der Wortlaut von Artikel 42 DSGVO lautet

„(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

(2) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 5 des vorliegenden Artikels genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

(3) Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.

(4) Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, die gemäß Artikel 55 oder 56 zuständig sind.

(5) Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde anhand der von dieser zuständigen Aufsichtsbehörde gemäß Artikel 58 Absatz 3 oder — gemäß Artikel 63 — durch den Ausschuss genehmigten Kriterien erteilt. Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen.

(6) Der Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 43 oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.

(7) Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden. Die Zertifizierung wird gegebenenfalls durch

die Zertifizierungsstellen nach Artikel 43 oder durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

(8) Der Ausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register auf und veröffentlicht sie in geeigneter Weise."

Der Wortlaut des korrespondierenden Erwägungsgrundes 100 zur DSGVO lautet

„Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen."

2.2.5.1 Einordnung und Anwendungsbereich

Die datenschutzrechtliche Zertifizierung nach Art 42 DSGVO stellt auf einzelne Verarbeitungsvorgänge personenbezogener Daten ab und soll zu einem erhöhten Maß an Transparenz im Zusammenhang mit datenschutzrechtlichen Vorgaben beitragen. Sie weist das Potential für die Etablierung einer harmonisierten datenschutzrechtlichen Konformitätsbewertung mit unionsweiter Anwendbarkeit und Akzeptanz auf, wodurch betroffenen Personen ein möglichst niederschwelliger und leicht zugänglicher Überblick über das jeweilige Datenschutzniveau[109] ermöglicht werden soll.

In Abgrenzung zu datenschutzrechtlichen Verhaltensregeln nach Art 40 DSGVO, die verstärkt auf sektorenspezifische Harmonisierungs- und Standardisierungsbestrebungen abstellen, zielt die Zertifizierung nach Art 42 DSGVO auf die Erbringung eines Nachweises für die Einhaltung der DSGVO ab. Diese beiden selbstregulatorischen Mechanismen sollen dem Ansatz der EK zufolge dazu beitragen, den Anforderungen schnelllebiger technischer Entwicklungen im Wirtschaftsleben gerecht zu werden.[110]

Verantwortliche können diese Zertifizierung als Nachweis zur Erfüllung ihrer Rechenschaftspflicht im Sinne des risikobasierten Ansatzes nutzen und im Zusammenhang mit der Auswahl ihrer Auftragsverarbeiter eine rechtskonforme Verarbeitung nach dem jeweils aktuellen Stand der Technik bescheinigen. Eine Zertifizierung nach Art 42 DSGVO stellt dennoch ebenso für Auftragsverarbeiter ein geeignetes Tool zum Nachweis des

[109] ErwG 100 DSGVO.
[110] *Kröpfel*, Konformitätsbewertung im Datenschutzrecht, Jahrbuch Datenschutzrecht 2020, 221-225.

erforderlichen Sorgfaltsmaßstabes dar, auch wenn diese im direkten Vergleich mit Verantwortlichen nicht dasselbe Ausmaß an Sorgfaltspflichten trifft.[111]

Datenschutzrechtliche Akteure wie Verantwortliche und Auftragsverarbeiter sowie ein DSMS in seiner Gesamtheit stellen keinen geeigneten Zertifizierungsgegenstand dar, Produkte und Dienste sind durch die zugrundeliegenden Verarbeitungsvorgänge nur mittelbar umfasst. Der Anreiz zur Vornahme von datenschutzrechtlichen Zertifizierungen wird explizit im Verordnungstext der Bestimmungen zu Art 24 Abs 3, Art 25 Abs 3, Art 28 Abs 5 und Art 32 Abs 3 DSGVO sowie in ErwG 100 DSGVO angeführt.

Aufgrund der Einstufung als Compliance – Tool sieht der Verordnungstext in Art 42 Abs 3 DSGVO vor, dass die Durchführung einer solchen datenschutzrechtlichen Zertifizierung ausschließlich freiwillig erfolgt und nicht verpflichtend vorgeschrieben werden darf. Die Möglichkeit zur Erbringung eines Nachweises, dass bestehende datenschutzrechtliche Verpflichtungen eingehalten werden, kann jedoch aus unterschiedlichen Beweggründen relevant sein. Einerseits können datenschutzrechtliche Verstöße zu Schadenersatzforderungen nach Art 82 DSGVO sowie zur Verhängung von Geldbußen durch die Aufsichtsbehörde nach Art 83 DSGVO führen. Andererseits kann die Einhaltung hoher Datenschutzstandards als Qualitätsmerkmal angesehen werden und zu einer vertrauens- und wettbewerbsfördernden Wirkung einer Organisation gegenüber Dritten beitragen. Das Vorliegen einer Zertifizierung mindert Art 42 Abs 4 DSGVO zufolge jedoch nicht das Ausmaß bestehender, datenschutzrechtlicher Pflichten und kann auch nicht als Haftungsbefreiung datenschutzrechtlicher Akteure angesehen werden.[112]

Eine Zertifizierung kann gem Art 42 Abs 2 DSGVO auch als Nachweis für das Vorliegen geeigneter Garantien für den Export von personenbezogenen Daten an Verantwortliche oder Auftragsverarbeiter in Drittländern gem Art 46 Abs 2 lit f DSGVO herbeigezogen werden. Der räumliche Anwendungsbereich der DSGVO kann somit durch die Vornahme von Zertifizierungen erweitert werden, sobald die nationale Aufsichtsbehörde des datenexportierenden Mitgliedsstaates die zugrundeliegenden Zertifizierungskriterien nach

[111] *Trieb*/*Kröpfl*, Datenschutzzertifizierungen in greifbarer Nähe, Dako, 2020/32, 52 - 54.
[112] *Strohmaier* in Knyrim, DatKomm Art 42 DSGVO Rn 1, 7 – 8, 12.

erfolgter Stellungnahme des EDSA genehmigt hat. Diese Einschränkung entfällt jedoch bei der Verwendung von Zertifizierungskriterien, die durch den EDSA genehmigt wurden.[113]

Zertifizierungen können durch akkreditierte Zertifizierungsstellen sowie durch die nationale Aufsichtsbehörde nach Art 58 Abs 3 lit f DSGVO iVm Art 42 Abs 5 leg cit erteilt werden. Zertifizierungsstellen sind in diesem Zusammenhang als von der zertifizierungswerbenden Stelle unterschiedliche, unabhängige Dritte zu verstehen, die eine entsprechende Konformitätsbeurteilung anhand festgelegter Zertifizierungskriterien durchführen.[114] Die Ausübung dieser Befugnis zur Ausstellung von Zertifizierungen durch die Aufsichtsbehörde obliegt ihrem eigenen Ermessen, wodurch kein Wahlrecht für die Einbringung eines Zertifizierungsantrages bei der Aufsichtsbehörde besteht.[115]

Die Liste aller in Österreich akkreditierten Zertifizierungsstellen ist auf der Webseite der Datenschutzbehörde öffentlich einsehbar.[116] Die einzelnen Mitgliedsstaaten, nationalen Aufsichtsbehörden sowie der EDSA und die EK unterliegen gem Art 42 Abs 1 DSGVO einer Förderpflicht für die Einführung datenschutzrechtlicher Zertifizierungsverfahren. Der EDSA gibt hier etwa fortlaufende Stellungnahmen über Akkreditierungsanforderungen nationaler Aufsichtsbehörden ab und veröffentlicht Leitlinien über Zertifizierungskriterien, während die EK eine umfassende Studie[117] in diesem Bereich durchgeführt hat.

2.2.5.2 Abgrenzung zu bisherigen Zertifizierungen

Bereits vor Inkrafttreten der DSGVO gab es eine Vielzahl privatwirtschaftlicher Anbieter für Konformitätsbewertungen und datenschutzrechtliche Zertifizierungen. Zugrundeliegende Prüfungskriterien werden hier überwiegend ohne behördliche Akkreditierung durch die prüfenden Organisationen selbst festgelegt. Dieser Umstand kann sich negativ auf die Effektivität und Akzeptanz dieser Verfahren auswirken. Diese Zertifizierungen waren oftmals an nationale Datenschutzrichtlinien gebunden und wiesen im Zusammenhang mit den zugrundeliegenden Prüfungsmodalitäten teilweise intransparente Abweichungen auf,

[113] *Strohmaier* in Knyrim, DatKomm Art 42 DSGVO Rn 19 – 20.

[114] *Kröpfl*, Datenschutzrechtliche Zertifizierungen, Jahrbuch Datenschutzrecht 2019, 186.

[115] *Strohmaier* in Knyrim, DatKomm Art 42 DSGVO Rn 24/4 – 24/5.

[116] https://www.dsb.gv.at/aufgaben-taetigkeiten/Zertifizierungen.html#Frage_11, im Zeitpunkt der Verfassung dieser Arbeit war an dieser Stelle noch keine akkreditierte Zertifizierungsstelle angeführt (abgerufen am 17.11.2023).

[117] *Kamara/Leenes/Lachaud/Stuurman/van Lieshout/Bodea*, Data Protection Certification Mechanisms, final report of the European Commission study on Articles 42 and 43 of the Regulation (EU) 2016/679, abrufbar unter: data_protection_certification_mechanisms_study_publish_0.pdf (europa.eu).

wodurch ein transnationaler Vergleich des attestierten Datenschutzniveaus erschwert wurde.[118]

Im Gegensatz dazu sieht die datenschutzrechtliche Zertifizierung nach Art 42 DSGVO ein harmonisiertes, unionsweit anerkanntes Verfahren mittels unabhängiger Bescheinigungen durch Dritte vor. Bestehende Konformitätsbewertungen dürfen parallel weiterverwendet werden. Dies setzt jedoch ein gewisses Maß an Abgrenzbarkeit zur datenschutzrechtlichen Zertifizierung nach Art 42 DSGVO voraus, damit keine Verwechslungsgefahr entstehen kann.[119]

Darüber hinaus gilt es zu beachten, dass in Österreich mittlerweile mehr als fünf Jahre nach Inkrafttreten des DSGVO bisher noch keine akkreditierte Zertifizierungsstelle besteht, die Zertifizierungen nach Art 42 DSGVO vornehmen kann.

2.2.5.3 Das Europäische Datenschutzsiegel – European Data Protection Seal

Artikel 42 Abs 5 DSGVO sieht vor, dass durch den EDSA genehmigte Zertifizierungskriterien in weiterer Folge zu einem Europäischen Datenschutzsiegel führen können. Der EDSA veröffentlichte Empfehlungen für informelle sowie formalisierte Verfahren zur Genehmigung eingereichter, nationaler Zertifizierungskriterien zur Etablierung eines europäischen Datenschutzsiegels. [120]

Wenn Zertifizierungskriterien transnationale Verarbeitungsvorgänge innerhalb von Mitgliedstaaten der EU adressieren, sind diese in einem ersten Schritt den jeweiligen, nationalen Aufsichtsbehörden vorzulegen. Diese prüfen die eingereichten Kriterien im Kohärenzverfahren gem Art 63 DSGVO und stellen bei vorliegender Eignung einen Antrag auf Genehmigung an den EDSA. Die eingereichten Kriterien können schließlich unter der Berücksichtigung nationaler Regelungen im Zusammenhang mit vorgesehenen Öffnungsklauseln der DSGVO unionsweit angewendet werden, sobald der EDSA seine Genehmigung dafür erteilt hat.

Die Vorteile eines einheitlichen europäischen Datenschutzsiegels liegen in der Vereinheitlichung nationaler Zertifizierungsverfahren, die zu einer höheren Marktakzeptanz

[118] *Hofmann*, Dynamische Zertifizierung, Datenschutzrechtliche Zertifizierung nach der Datenschutzgrundverordnung am Beispiel des Cloud Computing 162 – 164.

[119] *Kröpfl,* Datenschutzrechtliche Zertifizierungen, Jahrbuch Datenschutzrecht 2019, 163 – 167.

[120] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals adopted on February 14th 2023.

der Zertifizierung wie bisher bereits im Bereich technischer ISO – Normen in der Informationssicherheit führen kann. Im öffentlichen Bereich kann ein unionsweites Datenschutzsiegel die Eignung von Bietern in Verfahren nach dem Bundesvergabegesetz[121] und damit zur Rechtsicherheit beitragen. Mitgliedsstaatenübergreifend operierende Unternehmen können in wirtschaftlicher Hinsicht von derartigen Harmonisierungsbestrebungen durch die Umsetzung erforderlicher Prozesse anhand von einheitlichen Vorgaben profitieren.[122]

Der EDSA hat die Zertifizierung nach Europrivacy als erstes unionsweit anerkanntes Datenschutzsiegel gem Art 42 Abs 5 DSGVO aufgrund der genehmigten Zertifizierungskriterien anerkannt.[123] Dieses Zertifizierungsprogramm wurde im Rahmen eines Forschungsprogrammes der EU entwickelt und kann nunmehr in allen Mitgliedsstaaten zur Konformitätsbeurteilung von datenschutzrechtlich relevanten Verarbeitungsvorgängen herangezogen werden.

Das Europrivacy Zertifizierungssystem wurde teilweise in Anlehnung an ISO -Zertifizierungsmodelle entwickelt, weshalb es mit technischen Zertifizierungen im Zusammenhang mit der Sicherheit von ISMS nach dem ISO/IEC 27001 Standard kombiniert werden kann. Ein internationales Expertengremium aus dem Bereich des Datenschutzes überwacht und aktualisiert dieses Zertifizierungssystem kontinuierlich, um dem Stand der Technik sowie regulatorischen Gegebenheiten zu entsprechen. [124]

2.2.5.4 Zertifizierungsstellen und das Akkreditierungsverfahren nach Art 43 DSGVO

Während das Zertifizierungsverfahren in Art 42 Abs 5 DSGVO in Grundzügen skizziert wird, enthält Art 43 DSGVO Vorgaben im Zusammenhang mit der Akkreditierung von Zertifizierungsstellen. Bevor eine Stelle die datenschutzrechtliche Zertifizierung erteilen darf, ist zunächst ein formalisiertes Akkreditierungsverfahren zu durchlaufen:[125]

[121] Bundesvergabegesetz 2018 (BVerG 2018), BGBl. I Nr. 65/2018.

[122] *Herold*/*Tober*, DSGVO-Zertifizierung - Das Europäische Datenschutzsiegel, CB 2023, 361.

[123] https://www.europrivacy.org/en/news/2022-10-14/europrivacy-gdpr-european-data-protection-seal-approved-eu-new-era-privacy-and-data (abgerufen am 07.11.2023); https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en?field_edpb_lsa_target_id=All&field_edpb_certification_transf_value=All (abgerufen am 18.11.2023).

[124] https://europrivacy.com/ (abgerufen am 07.11.2023).

[125] https://www.dsb.gv.at/aufgaben-taetigkeiten/Zertifizierungen.html#Frage_1 (abgerufen am 12.11.2023).

- Sobald die Akkreditierung als Zertifizierungsstelle anstrebt wird, hat die akkreditierungswerbende Stelle einen Antrag an die nationale Aufsichtsbehörde oder jene Stelle zu richten, die nach nationalem Recht für Akkreditierungen genannt wird. Dazu sind geeignete Unterlagen zum Nachweis der geforderten Akkreditierungsvoraussetzungen einzureichen. Die DSB fungiert in Österreich gem § 24 Abs 3 DSG als Akkreditierungsstelle iSd Art 43 Abs 1 DSGVO.

- Die erforderlichen Akkreditierungsvoraussetzungen werden in Art 43 Abs 2 DSGVO allgemein formuliert und stellen überwiegend auf das Vorliegen einer fachlichen Eignung und Unabhängigkeit sowie organisatorischen Struktur ab, um als Zertifizierungsstelle qualifiziert zu werden.

- Diese Voraussetzungen werden durch die ZeStAkk-V[126] näher umrissen, die auf der Grundlage einer Verordnungsermächtigung gem § 21 Abs 3 DSG von der DSB erlassen wurde. Als legitimierte Antragsteller zur Erlangung einer Akkreditierung als Zertifizierungsstelle gem § 4 ZeStAkk-V kommen ausschließlich juristische Personen iSd Norm ISO/IEC 17065:2012[127] in Frage.

- Die DSB überprüft sodann den Antrag und fordert die akkreditierungswerbende Stelle gegebenenfalls zur schriftlichen Abgabe ergänzender Stellungnahmen oder zur Nachreichung fehlender Unterlagen auf. Die inhaltliche Entscheidung über das Ergebnis des Antrages ergeht schließlich in Bescheidform.

Eine Akkreditierung zur Zertifizierungsstelle ist gem Art 43 Abs 4 DSGVO für eine Höchstdauer von fünf Jahren gültig, danach ist der Akkreditierungsprozess unter denselben Voraussetzungen wie bei der erstmaligen Akkreditierung erneut zu durchlaufen. Im Zuge der Akkreditierung unterliegen Zertifizierungsstellen der Aufsicht durch die DSB. Werden die Akkreditierungsvoraussetzungen im Zeitverlauf nicht mehr erfüllt oder kommt es zu Maßnahmen, die mit der DSGVO unvereinbar sind, ist die Akkreditierung gem Art 43 Abs 7 DSGVO zu widerrufen. Falls die erforderlichen Voraussetzungen für die Erteilung von Zertifizierungen durch eine Zertifizierungsstelle nicht mehr vorliegen, kann die

[126] Verordnung der Datenschutzbehörde über die Anforderungen an die Akkreditierung einer Zertifizierungsstelle (Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V), BGBl. II Nr. 79/2021 (zuletzt geändert durch: BGBl. II Nr. 149/2021).

[127] Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (ISO/IEC 17065:2012), DIN EN ISO/IEC 17065 - 2013-01 - Beuth.de (abgerufen am 12.11.2023).

DSB in Ausübung ihrer Abhilfebefugnis gem Art 58 Abs 2 lit h DSGVO bereits erteilte Zertifizierungen widerrufen, sowie die Weisung erteilen, keine weiteren Zertifizierungen mehr auszugeben.[128]

Die erfolgreiche Akkreditierung von Zertifizierungsstellen setzt das Vorliegen eines ausreichend bestimmten Zertifizierungsgegenstandes auf der Grundlage genehmigter Zertifizierungskriterien voraus. Der EDSA hat in diesem Zusammenhang Leitlinien[129] für die Festlegung von Zertifizierungskriterien erarbeitet, wonach diese:

- *„einheitlich und nachprüfbar sein sollten,*
- *insbesondere Ziele festlegen und praktische Leitlinien für die Erreichung dieser Ziele geben sollten, um im Hinblick auf eine systematische Evaluierung der Verarbeitungsvorgänge nach der DSGVO überprüfbar zu sein,*
- *für die Zielgruppe (z. B. B2B und Business-to-Customer (B2C)) relevant sein sollten,*
- *andere Standards (etwa ISO-Normen oder nationale Standards) berücksichtigen oder gegebenenfalls mit diesen interoperabel sein sollten und*
- *im Hinblick auf die Anwendung auf Organisationen unterschiedlicher Art und Größe einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen gemäß Artikel 42 Absatz 1 sowie des risikobasierten Ansatzes gemäß Erwägungsgrund 77 flexibel und skalierbar sein sollten.“*

Zertifizierungskriterien können entweder durch die Aufsichtsbehörde oder durch den EDSA genehmigt werden, wobei derzeit grundsätzlich alle eingereichten Zertifizierungskriterien genehmigungsfähiger Anträge zu Zwecken der Rechtsharmonisierung dem EDSA gem Art 64 Abs 1 lit c DSGVO zur Stellungnahme vorgelegt werden. Die DSGVO legt keine Gültigkeitsdauer für genehmigte Zertifizierungskriterien fest, weshalb diese grundsätzlich bis zu einem etwaigen Widerruf durch die Aufsichtsbehörde in Geltung bleiben. Einen Anhaltspunkt für einen derartigen Widerruf stellt etwa die Unvereinbarkeit von Zertifizierungskriterien mit dem fortschreitenden Stand der Technik oder die Änderung gesetzlicher Rahmenbedingungen dar. Genehmigte Zertifizierungsverfahren und akkreditierte

[128] Erläuterungen zur ZeStAkk-V, abrufbar unter: https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html

[129] EDSA Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.

Einrichtungen werden gem Art. 70 Abs 1 lit o DSGVO in einem öffentlichen Register des EDSA veröffentlicht.[130]

2.2.5.5 Das Zertifizierungsverfahren

Zur Erlangung einer datenschutzrechtlichen Zertifizierung müssen zertifizierungswerbende Stellen einen schriftlichen Antrag an eine akkreditierte Zertifizierungsstelle stellen und in weiterer Folge das Verfahren gem § 8 ZeStAkk-V einhalten:

- Nach Einlangen des Antrages erfolgt dessen Bewertung, der Abschluss einer Zertifizierungsvereinbarung zwischen der zertifizierungswerbenden Stelle und der Zertifizierungsstelle sowie eine Evaluierung der Zertifizierungsvoraussetzungen. Die zertifizierungswerbende Stelle verpflichtet sich dabei zur vollständigen Transparenz gegenüber der DSB sowie zur fortlaufenden Einhaltung der bestehenden Anforderungen im Zuge der Zertifizierung.

- Sobald eine Bewertung der Evaluationsergebnisse in Form eines Gutachtens erfolgt ist, wird die Zertifizierungsentscheidung innerhalb einer angemessenen Entscheidungsfrist getroffen. Diese Frist ist unter Berücksichtigung des Umfanges sowie der spezifischen Gegebenheiten des Zertifizierungsgegenstandes individuell festzulegen.

- Bevor die Zertifizierungsentscheidung ergeht, hat die Zertifizierungsstelle gem Art 43 Abs 5 DSGVO eine Notifikation über diese beabsichtigte Entscheidung an die DSB als Aufsichtsbehörde zu veranlassen.[131]

- Im Zuge einer erfolgreichen Zertifizierung erhält die zertifizierungswerbende Stelle eine schriftliche Bescheinigung von der Zertifizierungsstelle, wobei der zugrundeliegende Zertifizierungsgegenstand hinreichend konkret und transparent ersichtlich sein muss.[132] Die Zertifizierung wird gem Art 42 Abs 7 DSGVO für eine Höchstdauer von drei Jahren erteilt und kann im Zuge einer Rezertifizierung unter Einhaltung der erforderlichen Zertifizierungskriterien verlängert werden.

[130] https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and marks_en?field_edpb_lsa_target_id=All&field_edpb_certification_transf_value=All (abgerufen am 18.11.2023).

[131] *Strohmaier* in Knyrim, DatKomm Art 42 DSGVO Rn 22/1 – 22/13.

[132] §13 Abs 4 ZeStAkk-V.

- Zertifizierungsstellen haben darüber hinaus gem Art 43 Abs 2 lit c DSGVO Verfahren für die regelmäßige Überprüfung und für den Widerruf erteilter Zertifizierungen festzulegen. Nachdem die DSGVO keine näheren Vorgaben für die Regelmäßigkeit von Überprüfungen vorgibt, kann die Empfehlung der deutschen Datenschutzkonferenz als Referenzwert herangezogen werden, wonach zumindest zwei Überprüfungen innerhalb der 3-jährigen Gültigkeitssauer nach erteilter Zertifizierung erfolgen sollen.[133]

[133] *Kröpfl*, Datenschutzrechtliche Zertifizierungen, Jahrbuch Datenschutzrecht 2019, 202.

3. Praxisteil

3.1 Datenschutz im Bildungsbereich

Im österreichischen Bildungsbereich wird dem Schutz personenbezogener Daten ein hoher Stellenwert eingeräumt, nachdem der laufende Schulbetrieb tagtäglich eine Vielzahl an Verarbeitungsvorgängen im Zusammenhang mit Schülerinnen und Schülern, Erziehungsberechtigten und Lehrpersonen erfordert. Das Bildungswesen in Österreich umfasst rund 1.140.000 Schülerinnen und Schüler[134] sowie 5.930 Schulen mit einer gesetzlichen Schularztbezeichnung[135].

Verarbeitungstätigkeiten im Bereich des Schulrechtsvollzuges erfolgen primär aufgrund einschlägiger gesetzlicher Grundlagen[136] wie dem BilDokG 2020[137] und dem SchUG[138]. Darüber hinaus kommt auch die Erfüllung vertraglicher oder sonstiger rechtlicher Verpflichtungen und in Einzelfällen die Einwilligung zur Datenverarbeitung als Rechtsgrundlage zur Anwendung.

Am plastischen Beispiel der Planung eines Schulskikurses lässt sich verdeutlichen, mit welchen datenschutzrechtlichen Herausforderungen die einzelnen Schulstandorte konfrontiert sein können. In diesem Szenario wird eine klasseninterne Liste unter Offenlegung von Geburtsdaten und Namen aufgelegt, damit die Schülerinnen und Schüler weitere Angaben wie ihr Körpergewicht, ihre Körpergröße oder Schuhgröße ergänzen, um die zentrale Bestellung von Wintersportausrüstung zu erleichtern.[139] Eine vereinfachte Abwicklung für die Organisation dieses Schulskikurses scheint hierbei keine geeignete Rechtfertigung für die offenkundige Verletzung des Grundsatzes der erforderlichen Datenverarbeitung und Datenminimierung darzustellen. In weiterer Folge soll dieses Beispiel aufzeigen, dass es sich

[134] https://www.statistik.at/statistiken/bevoelkerung-und-soziales/bildung/schulbesuch/schuelerinnen (abgerufen am 18.11.2023).

[135] https://www.statistik.at/statistiken/bevoelkerung-und-soziales/bildung/schulbesuch/schulen-und-klassen (abgerufen am 18.11.2023).

[136] Index des österreichischen Bundesrechts im Sachgebiet Schule: https://www.ris.bka.gv.at/UI/Bund/Bundesnormen/IndexBundesrecht.aspx?TabbedMenu-Selection=BundesrechtTab#C7 (abgerufen am 18.11.2023).

[137] Bildungsdokumentationsgesetz 2020 (BilDokG 2020), BGBl. I Nr. 20/2021.

[138] Schulunterrichtsgesetz (SchUG), BGBl. Nr. 472/1986 (WV).

[139] *Haidinger*, Meine Tochter fährt auf Schulskikurs […], Dako 2023/13.

bei derartigen Angaben auch um besondere Datenkategorien iSd Art 9 DSGVO handeln kann, sobald ein gewisser Verwendungszusammenhang mit einem klaren Bezug zur Gesundheit einer natürlichen Person vorliegt, da der Begriff der Gesundheitsdaten gem Art 4 Z 15 DSGVO grundsätzlich sehr weit gefasst ist.[140]

Der verantwortungsbewusste Umgang mit diesen, teilweise auch besondere Datenkategorien umfassenden Informationen wird im Bundesministerium für Bildung, Wissenschaft und Forschung sowie auch im nachgeordneten Bereich an den pädagogischen Hochschulen, Bildungsdirektionen und an den einzelnen Schulstandorten aktiv gelebt und fortlaufend evaluiert. Die Datenschutzbeauftragten und Ansprechpersonen für technischen Datenschutz im Bildungsbereich[141] stehen in einem stetigen Austausch und nehmen regelmäßig an Fortbildungsveranstaltungen teil. Datenschutzrechtliche Agenden werden im BMBWF jeweils durch einen Datenschutzbeauftragten aus dem Bereich Bildung sowie Wissenschaft und Forschung, eine sektionsübergreifende Arbeitsgruppe, die aus drei Datenschutzteams besteht, sowie durch die Fachabteilung Präs/13 wahrgenommen.[142]

Ein weiteres Szenario, das für wiederkehrenden datenschutzrechtlichen Diskurs im schulischen Alltag sorgt, betrifft die Anfertigung und Veröffentlichung von Lichtbildern, auf denen Schülerinnen und Schüler in identifizierbarer Weise abgebildet werden.[143] Die DSB stellte in diesem Fall einen datenschutzrechtlichen Verstoß einer Lehrperson im Zusammenhang mit ihrer dienstlichen Tätigkeit fest. Der Schulstandort wurde als unselbstständige Einrichtung qualifiziert, weshalb der datenschutzrechtliche Verstoß der jeweiligen Schulleitung zugerechnet wurde.[144] Diese ist gem Art 56 SchUG grundsätzlich zur Besorgung aller Angelegenheiten nach diesem Bundesgesetz zuständig, fungiert als unmittelbare Vorgesetzte des Lehrpersonals und ist daher als datenschutzrechtliche Verantwortliche anzusehen.[145]

---

[140] *Haase*, Der Begriff der "Gesundheitsdaten" nach der Datenschutz-Grundverordnung (DSGVO), InTeR 2022, 94.

[141] https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds/kontakt_dsb_schule.html (abgerufen am 18.11.2023).

[142] Geschäfts- und Personaleinteilung des Bundesministeriums für Bildung, Wissenschaft und Forschung (Stand 01.03.2023) 8, 27, 117, abrufbar unter: https://www.bmbwf.gv.at/Ministerium/GuP.html (abgerufen am 18.11.2023).

[143] DSB 22.6.2022, 2022-0.442.409 (DSB-D124.4479); *Haidinger/Löffler*, Lehrerin verletzte durch Fotoaufnahme Geheimhaltungsrecht von Schüler, Dako 2023/10, 17.

[144] vgl. BVwG 27.4.2022, W214 2237072-1.

[145] vgl. BVwG 30.9.2020, W274 2225135-1.

Auf Gesetzesebene sieht § 4 Abs 1 BilDokG 2020 die Verantwortlichkeit der jeweiligen Schulleitung für die Einhaltung des Datenschutzes an ihrem Schulstandort vor, wobei das BMBWF im Bereich der Bundesschulen etwa für die Gewährleistung der erforderlichen Datensicherheit von IT-Systemen und Diensten wie der Schulverwaltungssoftware verantwortlich ist:

> *„Verantwortliche im Sinne des Art. 4 Z 7 DSGVO sind*
>
> *1. für die Evidenzen der Schülerinnen und Schüler gemäß § 5 Abs. 1 und 2 und jene der Studierenden an den Bildungseinrichtungen deren Leiterinnen oder Leiter im Sinne des § 2 Z 8 und 10, bezüglich der Einrichtungen gemäß § 2 Z 4 lit. e deren Erhalterin, sowie*
>
> *2. bezüglich der Evidenzen der Schülerinnen und Schüler gemäß § 5 Abs. 3 und 4 die zuständige Bildungsdirektorin oder der zustän*dige Bildungsdirektor."

Auf Verordnungsebene erfolgt die Abgrenzung der datenschutzrechtlichen Verantwortlichkeit bei Datenverarbeitungen am Schulstandort durch § 15 IKT-Schulverordnung:

> „*Verantwortlicher im Sinne des Art.4 Z 7 DSGVO ist*
>
> *1. hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und Einhaltung der Grundsätze des Art.5 DSGVO durch die Bildungseinrichtung sowie hinsichtlich der Wahrung des Datenschutzes am Schulstandort gemäß §4 Abs.1BilDokG 2020 die jeweilige Schulleitung und*
>
> *2. hinsichtlich der Gewährleistung der Datensicherheit der nötigen IT-Systeme und Dienste für Datenverarbeitungen (zB einer Schulverwaltungssoftware und deren Hosting) jene Stelle, die als Maßnahme bezüglich der IT-Ausstattung an Schulen die Entscheidung darüber trifft."*

Die zu verarbeitenden Datenkategorien im Bereich des Schulrechtsvollzuges ergeben sich aufgrund von § 5 sowie den Anlagen 1 und 2 zum BilDokG 2020. Diese umfassen unter anderem die Schulkennzahl, das bildungseinrichtungsspezifische Personenkennzeichen, das Datum der Aufnahme einer Ausbildung sowie die Bezeichnung der jeweiligen Ausbildung. Die IKT-Schulverordnung enthält weitere einschlägige Anforderungen an IT-Systeme und

Dienste sowie technische und organisatorische Datensicherheitsmaßnahmen für Anwendungen im Bildungsbereich.[146]

Der Pflichtgegenstand „Digitale Grundbildung“ wurde mit dem Schuljahr 2022/23 für den Unterricht in der 5. bis 7. Schulstufe und ab dem Schuljahr 2023/24 zusätzlich auch in der 8. Schulstufe eingeführt. Dadurch wird der zunehmenden Notwendigkeit zur schulseitigen Bewusstseinsbildung im Bereich des Datenschutzes, der Datensicherheit sowie im Umgang mit Technologie aus pädagogischer Sicht begegnet.[147] Entsprechende Begleitmaßnahmen für das Lehrpersonal wurden unter anderem durch die Abhaltung von sog. „Massive Open Online Courses“ - Fortbildungsveranstaltungen, die Einführung eines neuen Lehramtsstudiums zur Erlangung des Lehrbefähigung für den neuen Pflichtgegenstand sowie durch die Schaffung eines entsprechenden Hochschullehrganges an den Pädagogischen Hochschulen gesetzt.

Mit der Initiative „Privacy4kids“[148] werden Datenschutzinformationen für Kinder altersgerecht aufbereitet und vermittelt. Die DSB entwickelte hierfür in Zusammenarbeit mit der Universität Wien animierte Videos und ein Kartenspiel mit datenschutzrechtlichen sowie informationstechnischen Inhalten. Die entsprechenden Materialien stehen in der Eduthek des BMBWF mit der empfohlenen Verwendung als Lernvideo mit Lehrplanbezug zum Pflichtgegenstand Digitale Grundbildung zur Verfügung und enthalten darüber hinaus didaktische Hinweise für den Einsatz im Schulunterricht.[149]

Im Zuge eines zeitgemäßen IT-gestützten Unterrichts gem § 14a Abs 1, 2 SchUG ist der Einsatz digitaler Endgeräte als Arbeitsmittel sowie digitaler Lern- und Arbeitsplattformen vorgesehen. Die IKT-Schulverordnung konkretisiert diese Vorgaben auf Grundlage der getroffenen Verordnungsermächtigung gem § 14a Abs 3 SchUG hinreichend auf Verordnungsebene. Zur Umsetzung dieser Vorgaben werden bildungsspezifische Anwendungen auf Open Source – Basis sowie Services privater Clouddiensteanbieter eingesetzt. Das BMBWF stellt für den Bildungsbereich zentrale IT-Services bereit, nachdem

[146] Siehe ergänzend dazu die Erläuterungen zur IKT-Schulverordnung: https://www.bmbwf.gv.at/dam/jcr:9c046ff2-a48f-436b-b636-566c96594bf4/ikt_schulvo_erl.pdf.

[147] Siehe zur digitalen Grundbildung in der Sekundarstufe I: https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb.html#:~:text=Mit%20dem%20Schuljahr%202022%F23,Pflichtgegenstand%20%E2%80%9EDigitale%20Grundbildung%E2%80%9C%20eingef%C3%BChrt (abgerufen am 18.11.2023).

[148] https://privacy4kids.at/ (abgerufen am 18.11.2023).

[149] Siehe zum Eduthek Leitfaden und Überblick über die Lernvideos von privacy4kids: https://eduthek.at/resource_details?full_data=0&resource_id=32534350&return_url=/xhr/filter_resources (abgerufen am 18.11.2023).

die einzelnen Schulstandorte zumeist nicht über die erforderlichen Ressourcen für den schulautonomen Betrieb einer performanten und sicheren IT-Infrastruktur verfügen.[150] Neben den Bildungseinrichtungen stellten auch einschlägige Softwareentwickler fest, dass sich die Anforderungen im Bereich des Datenschutzes und der Informationssicherheit in rasanter Geschwindigkeit verändern und einer stetigen Evaluierung im schulischen Bereich bedürfen.[151] In diesem Zusammenhang gilt es zu beachten, dass bisher bekannte Cyberangriffe auf österreichische Bildungseinrichtungen[152] jeweils auf lokal gehostete Serverinfrastrukturen zurückzuführen waren.

Der zunehmende öffentliche Diskurs um die digitale Souveränität in der öffentlichen Verwaltung im Allgemeinen[153] sowie im Bildungssektor im Speziellen[154] spiegelt sich auch in vermehrten parlamentarischen Anfragen[155] und Stellungnahmen datenschutzrechtlicher NGOs[156] wieder. Grundsätzlich lässt sich kein explizites Verbot der Verwendung privater Clouddiensteanbieter im Bereich der Bundesverwaltung aus der DSGVO oder dem DSG ableiten. Darüber hinaus besteht mit dem kürzlich in Kraft getretenen EU-U.S. Data Privacy Framework[157] derzeit ein gültiger Angemessenheitsbeschluss gem Art 45 DSGVO für Datenübermittlungen an gelistete Datenimporteure[158] in den Vereinigten Staaten.[159]

[150] *Novotny/Menzel*, Datenschutz in der Schule, Dako 2023/4, 7-9.

[151] *Heidegger*, In Schulen darf Datensicherheit kein Zufall sein!, Dako 2023/3, 4-6.

[152] zuletzt siehe: https://science.apa.at/power-search/572466147838475840 (abgerufen am 19.11.2023).

[153] https://www.digitalaustria.gv.at/; google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj60dHSktCCAxUb_7sIHebJAssQFnoECDIQAQ&url=https%3A%2F%2Fwww.digitalaustria.gv.at%2Fdam%2Fjcr%3Aff7c2ef5-32c6-40bb-b21d462d5857a636%2FHandlungsbereiche%2520Digitale%2520Souver%25C3%25A4nit%25C3%25A4t.pdf&usg=AOvVaw0NuanYTVrSv8uIsSpI0aO8&opi=89978449 (abgerufen am 19.11.2023).

[154] vgl. *Kircher*, Mit Digitaler Souveränität den Wandel selbstbestimmt gestalten, abrufbar unter: https://unipub.uni-graz.at/obvugrhs/content/titleinfo/4868559/full.pdf (abgerufen am 19.11.2023).

[155] vgl https://www.parlament.gv.at/dokument/XXVII/AB/3380/imfname_847258.pdf; https://www.parlament.gv.at/dokument/XXVII/AB/5703/imfname_955214.pdf (abgerufen am 19.11.2023).

[156] vgl. https://epicenter.works/content/datenschutz-im-bildungsbereich-schuelerinnendaten-in-den-haenden-von-big-tech-teil-2 (abgerufen am 19.11.2023).

[157] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf (abgerufen am 19.11.2023).

[158] https://www.dataprivacyframework.gov/s/participant-search (abgerufen am 19.11.2023).

[159] https://www.dsb.gv.at/aufgaben-taetigkeiten/internationaler-datenverkehr.html (abgerufen am 19.11.2023).

Die faktische Gültigkeitsdauer dieses Angemessenheitsbeschlusses erscheint jedoch ungewiss, nachdem in diesem Zusammenhang bereits eine Nichtigkeitsklage[160] anhängig ist und auch die NGO „NOYB – Europäisches Zentrum für digitale Rechte“ die Anfechtung dieses Angemessenheitsbeschlusses vor dem EuGH angekündigt hat.[161]

Das BMBWF ist sich dieses Spannungsfelds bewusst und differenzierte daher aus datenschutzrechtlicher Sicht zwischen Verarbeitungstätigkeiten aus dem Bereich der Schulverwaltung sowie der Unterrichtsdokumentation und pädagogischen Kollaboration. Demnach dürfen private Clouddiensteanbieter unter der Einhaltung spezifischer, für den Bildungsbereich ausverhandelter Rahmenbedingungen derzeit lediglich für Daten der Unterrichtsdokumentation, jedoch nicht für die Verarbeitung von Stammdaten eingesetzt werden.[162]

Der EDSA initiierte im Februar 2022 erste koordinierte Maßnahmen zur Nutzung von cloudbasierten Diensten durch öffentliche Stellen[163], wodurch 22 nationale Aufsichtsbehörden amtswegige Prüfverfahren eingeleitet haben.[164] Die DSB als österreichische Aufsichtsbehörde leitete eine derartige Datenschutzüberprüfung gem Art 57 Abs 1 lit h iVm Art 58 Abs 1 lit b DSGVO iVm § 22 Abs 1 DSG auch gegen das BMBWF ein. Im Zuge dieser Überprüfung übermittelte das BMBWF eine ausführliche Beantwortung des vorgelegten Fragenkatalogs unter Beiziehung von Expertinnen und Experten der Research Institute AG & Co KG[165], die schließlich in anonymisierter Form in den veröffentlichten, EWR-weiten Bericht des EDSA einfließen durfte.[166]

Der datenschutzkonforme Einsatz von Services privater Clouddiensteanbieter hängt wesentlich von der Ausgestaltung ihrer technischen und organisatorischen Maßnahmen ab. Die Verarbeitung pseudonymisierter Datensätze gem Art 32 DSGVO kann ein geeignetes Mittel darstellen, um ein verstärktes Schutzniveau im IT-gestützten Unterricht gewährleisten zu können.

---

[160] EuG 12.10.2023, T-553/23 R.

[161] https://noyb.eu/de/statement-zur-angemessenheitsentscheidung-der-eu-kommission-zur-usa (abgerufen am 19.11.2023).

[162] https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html (abgerufen am 19.11.2023).

[163] https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_de (abgerufen am 19.11.2023).

[164] https://www.dsb.gv.at/download-links/bekanntmachungen.html#Cloud_Dienste (abgerufen am 19.11.2023).

[165] https://researchinstitute.at/en/home-2/ (abgerufen am 19.11.2023).

[166] Abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en (abgerufen am 19.11.2023).

Die nachfolgende Vorgehensweise soll einen denkmöglichen Ansatz für die technische Umsetzung derartiger Maßnahmen darstellen:

- Schülerinnen und Schüler können sich ab dem Schuljahr 2023/24 im neu gestalteten Bildungsportal des BMBWF als zentrale Plattform für organisatorische und kommunikative Zusammenarbeit im Bildungsbereich[167] per SSO[168] mittels ID – Austria[169] oder ihrer Login Daten verifizieren.

- Diese Plattform soll zur Erleichterung und Entbürokratisierung des schulischen Alltags für Schülerinnen und Schüler, Erziehungsberechtigte und die Schulverwaltung beitragen. Nach dem erfolgten Login erhalten Nutzerinnen und Nutzer iSd once only – Prinzips[170] nunmehr Zugang zu ausgewählten Anwendungen aus dem Bereich des EdTechHub und des E-Governments wie der edu.digicard[171] als digitaler Schülerinnen - und Schülerausweis. Ein gesonderter Login in den einzelnen Anwendungen ist dann aufgrund der angebundenen Schnittstellen nicht mehr erforderlich.

- An dieser Stelle werden die Klardaten der Nutzerinnen und Nutzer des Bildungsportals nach Maßgabe der im Schulrechtsvollzug vorgesehenen Rechtsgrundlagen verarbeitet.

- Würde eine Pseudonymisierung der für die Verarbeitung erforderlichen Daten vor der weiteren Übermittlung beispielsweise auf der Serverinfrastruktur der Bundesrechenzentrum GmbH[172] erfolgen, könnte dadurch eine anonymisierende Wirkung gegenüber privaten Clouddiensteanbietern herbeigeführt werden.[173] Aus datenschutzrechtlicher Sicht wäre keine erneute Identifizierung der betroffenen Personen mehr durch diese möglich.

[167] https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/pods.html (abgerufen am 22.11.2023).
[168] https://bildung.gv.at/idp/profile/SAML2/Redirect/SSO?execution=e2s1 (abgerufen am 22.11.2023).
[169] https://www.oesterreich.gv.at/id-austria.html (abgerufen am 22.11.2023).
[170] https://www.usp.gv.at/ivdb-hilfe/Aufgaben-und-Zielsetzung.html (abgerufen am 22.11.2023).
[171] https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/itinf/itdienstleistungen/educard.html (abgerufen am 22.11.2023).
[172] https://www.brz.gv.at/ (abgerufen am 20.11.2023).
[173] *Hofer*, Überlegungen zur anonymisierenden Wirkung der Pseudonymisierung im Außenverhältnis am Beispiel von Cloud-Computing, jusIT 2022, 173.

- Bestehenden datenschutzrechtlichen Bedenken im Zusammenhang mit etwaigen Herausgabepflichten personenbezogener Daten durch US-amerikanische Konzernmuttern aufgrund einschlägiger Gesetze wie etwa den Cloud Act[174] oder FISA[175] kann auf diese Weise begegnet werden.

Bisher ist im Zusammenhang mit den im Bildungsbereich genutzten, privaten Clouddiensten noch keine derartige technische Lösung bekannt. Aus technischer Sicht bedarf es einer Evaluierung, ob die genutzten Dienste mit pseudonymen oder anonymen Daten in der jeweiligen Laufzeitumgebung[176] noch die erforderlichen Funktionalitäten aufweisen können.

Ungeachtet dieses potentiellen Ansatzes zur Umsetzung von Maßnahmen aus dem Bereich des technischen Datenschutzes, strebt das BMBWF eine datenschutzrechtliche Zertifizierung der jeweiligen Verarbeitungstätigkeiten IT-gestützten Unterrichts unter Heranziehung von Lernplattformen sowie privaten Clouddiensteanbietern in einem Verfahren gem Art 42 DSGVO an.

Das BMBWF betreibt die beiden Lernplattformen LMS[177] und edu.vidual[178], die als Pilotprojekt innerhalb der österreichischen Bildungslandschaft einer datenschutzrechtlichen Zertifizierung gem Art 42 DSGVO unterzogen werden sollen.

3.2 Lernplattformen im Bildungsbereich

In Anbetracht der zunehmenden digitalen Transformation in einer Vielzahl an Lebensbereichen, hat das BMBWF Empfehlungen zur Nutzung digitaler Technologien an den einzelnen Schulstandorten erarbeitet. Durch die Initiative „eEducation Austria“[179] werden zahlreiche Projekte und Anwendungen aus dem Bereich des eLearnings gebündelt. Als Teil

[174] Clarifying Lawful Overseas Use of Data Act; https://www.federalregister.gov/; vgl https://www.bsa.org/files/policy-filings/09012021whatiscloudact.pdf (abgerufen am 20.11.2023).

[175] Foreign Intelligence Surveillance Act; vgl https://noyb.eu/de/projekt/eu-us-transfers. (abgerufen am 20.11.2023).

[176] Anm: Die Laufzeitumgebung besteht im Regelfall aus dem Betriebssystem, der Hardware sowie dem Speicher des jeweiligen Systems und definiert in seiner Summe jene Umgebung, in der ein Programm ausgeführt wird. Siehe dazu: https://www.computerweekly.com/de/definition/Laufzeit-Runtime#:~:text=erforderlichen%20Funktionen%20bereitstellen.-,Laufzeitumgebung,h%C3%A4ufiger%20im%20IT%2DBetrieb%20eingesetzt. (abgerufen am 22.11.2023).

[177] https://lms.at/ (abgerufen am 22.11.2023).

[178] https://www.eduvidual.at/ (abgerufen am 22.11.2023).

[179] https://eeducation.at/ueber-eeducation (abgerufen am 26.11.2023).

dieser Digitalisierungsstrategie betreibt das BMBWF die beiden e-Learning Pattformen LMS und edu.vidual zur Förderung eines individualisierbaren und zeitgemäßen Unterrichts.[180]

3.2.1 Die Lernplattform LMS – Lernen mit System

Die Lernplattform LMS - „Lernen Mit System“ wurde im Jahr 2004 von der Knowledge Markets GmbH im Zusammenhang mit dem Bildungsserver bzw. Bildungsnetzwerk Burgenland[181] gegründet. Die Lernplattform kann von österreichischen Bundesschulen kostenlos genutzt werden, wobei ein hohes Maß an Informationssicherheit durch den Betrieb über die Serverinfrastruktur der BRZ GmbH gewährleistet wird.[182]

Die strukturellen Stärken dieser Lernplattform liegen in ihrer intuitiven Anwendung und zeitsparenden Organisation von Lerninhalten an den einzelnen Schulstandorten. Eine intensive Nutzung der angebotenen Services erfolgt verstärkt in östlichen Bundesländern Österreichs. Die unterschiedlichen Funktionalitäten dieser eLearning Plattform wurden insbesondere in Anbetracht des eingeschränkten Schulbetriebs während der Covid – 19 Pandemie seit April 2020[183] als Maßnahmen aus dem Bereich des Distance – Learnings eingesetzt:

- Bereitstellung individualisierter Lernunterlagen für Schülerinnen und Schüler in Form einer digitalen Bibliothek.
- Modul zur Abgabe von Arbeitsaufträgen und Aufgaben sowie zur Überprüfung von fachspezifischen Kompetenzen.
- Dokumentation für Lehrende zur Evaluierung der erbrachten Leistungen von Schülerinnen und Schülern nach den Vorgaben der LBVO[184].
- Schul- und klassenübergreifende Koordinierung von Projekten.
- Austausch von Lernunterlagen.

[180] https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/itinf/ndts.html (abgerufen am 26.11.2023).
[181] https://www.bildungsserver.com/ (abgerufen am 26.11.2023).
[182] https://www.brz.gv.at/was-wir-tun/sicherheit-und-qualitaet.html (abgerufen am 26.11.2023).
[183] https://transparenzportal.gv.at/tdb/tp/leistung/1048198.html (abgerufen am 26.11.2023).
[184] Verordnung des Bundesministers für Unterricht und Kunst vom 24. Juni 1974 über die Leistungsbeurteilung in Pflichtschulen sowie mittleren und höheren Schulen, BGBl. Nr. 371/1974.

- Eigenständige Identifizierung von schulspezifischen Stärken und Schwächen durch Schülerinnen und Schüler unter Anwendung von Selbstlernkonzepten, Erarbeitung von Inhalten sowie Dokumentation des persönlichen Lernerfolgs.

3.2.2 Die Lernplattform edu.vidual

Das Vorgängerprojekt zur Lernplattform edu.vidual mit der Bezeichnung „edu.moodle.at“ [185] entstand ursprünglich als eine Plattform für die gemeinsame Zusammenarbeit einzelner Schulstandorte als erste Vereinigung separat betriebener Instanzen. Das Ziel dieses Projekts war die erstmalige Schaffung einer schulübergreifenden Moodle-Instanz mit zahlreichen optionalen Konfigurationsmöglichkeiten, die teilweise technische Grundkenntnisse und eine Affinität für den Bereich der Informationstechnologie durch die jeweiligen Anwenderinnen und Anwender erfordern.

Das BMBWF erteilte der Pädagogischen Hochschule Oberösterreich als nachgeordnete Dienststelle den Auftrag zur Einrichtung des Zentrums für Lernmanagement, das die Implementierung einer einheitlichen Moodle – basierten Lernplattform durchführen sollte. Das ZLM weist als Stabstelle der Pädagogischen Hochschule Oberösterreich keine eigene Rechtspersönlichkeit auf und ist für das technische Service sowie die inhaltliche Konzeption und didaktische Weiterentwicklung der Lernplattform zuständig. Der Betrieb der erforderlichen Serverinfrastruktur wird durch die BRZ GmbH sichergestellt.[186]

Eduvidual gilt als konsequente Weiterentwicklung der Moodle-basierten Plattform „edumoodle.at“ und weist als schulübergreifende Lernplattform separate Bereiche für Schulen, gemeinsame Ressourcenpools sowie eine integrierte Videokonferenzlösung für Distance Learning und hybrides Lernen auf. Durch die Bereitstellung einer Basis – Version wird die Verwendung der Software auch ohne technische Grundkenntnisse ermöglicht.[187] Der offene Quellcode ermöglicht den frei zugänglichen Betrieb und die Weiterentwicklung von Anwendungen ohne jegliches „Vendor Lock - in“.[188]

---

[185] https://www.edugroup.at/fileadmin/DAM/Edugroup/News/Dateien/Produktblatt_edumoodle-at.pdf (abgerufen am 26.11.2023).

[186] https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/itinf/itdienstleistungen.html (abgerufen am 26.11.2023).

[187] https://eeducation.at/ressourcen/eduvidual (abgerufen am 26.11.2023).

[188] Der Begriff des „Vendor – Lock - in“ beschreibt die übermäßige Abhängigkeit von einzelnen Anbietern bei der Bereitstellung von IT-Dienstleistungen, wenn diverse Einschränkungen die Möglichkeit eines Anbieterwechsels möglichst unpraktikabel gestalten. Dieser Effekt kann unter anderem bei Produkten oder

Einige der wichtigsten Kernfunktionalitäten der Lernplattform edu.vidual umfassen:

- Digitale Kompetenzraster für das Lehrpersonal.
- Zurverfügungstellung gemeinsamer Ressourcen in Form von Beispielen für die Erstellung von Leistungsüberprüfungen sowie Unterrichtssequenzen.
- Reduzierung des Verwaltungsaufwandes für die jeweiligen Schulstandorte durch die Übernahme zahlreicher administrativer Tätigkeit durch das ZLM.
- Kommunikationsplattform zwischen Schülerinnen und Schülern sowie Lehrenden, digitales Mitteilungsheft.
- Zugang zu Ressourcen aus dem Bildungsbereich wie der Eduthek[189] oder Edutube[190].

3.2.3 Gegensätze und Gemeinsamkeiten

Die Lernplattformen LMS und edu.vidual weisen ähnliche Kernfunktionalitäten im Bereich der Bereitstellung und Verteilung von Inhalten innerhalb eines Klassenverbundes sowie der Leistungsdokumentation auf.

Die beiden Lernplattformen unterscheiden sich jedoch insbesondere dadurch voneinander, dass LMS eine zentrale Steuerung der entsprechenden Lerninhalte für die jeweiligen Schulstandorte zur Verfügung stellt und keine codebasierte Individualisierung oder einschlägige Programmierkenntnisse erforderlich sind. Hingegen erscheint edu.vidual als Moodle – basierte Plattform zur kreativen und codebasierten Individualisierung der Unterrichtsgestaltung besser geeignet zu sein und spricht daher entsprechend technisch versiertes Lehrpersonal als Zielgruppe an.

Unter Berücksichtigung der weitestgehenden Autonomie bei der Auswahl von Lehrmitteln[191] können Lehrpersonen grundsätzlich auch über den Einsatz von Lernplattformen entscheiden. Im Bereich der Allgemeinbildenden Höheren Schulen kommt es erfahrungsgemäß zum

Dienstleistungen eines firmeneigenen Ökosystems auftreten, die in Verbindung mit weiteren Produkten des gleichen Herstellers Vorteile bieten, bei einem Wechsel auf Produkte anderer Hersteller jedoch Probleme bereiten. Siehe dazu: https://cybersecurity-magazine.com/what-is-vendor-lock-in-and-how-to-avoid-it/ (abgerufen am 26.11.2023).

[189] https://eduthek.at/ (abgerufen am 26.11.2023).

[190] https://www.edutube.at/ (abgerufen am 26.11.2023).

[191] vgl. § 14 SchUG.

vermehrten Einsatz von edu.vidual als Moodle – basierte Anwendung, wohingegen LMS im Bereich der Berufsschulen sowie der Land- und Forstwirtschaftlichen Schulen häufig angewandt wird.

3.3. Vorbereitung der datenschutzrechtlichen Zertifizierung nach Artikel 42 DSGVO im Bildungsbereich

Lernplattformen bestehen in ihrer Gesamtheit aus einer Vielzahl von Verarbeitungsvorgängen und Vorgangsreihen wie beispielsweise dem Login-Prozess, der Verwendung von Nutzerschnittstellen zur Bereitstellung von Lerninhalten sowie der Beurteilung eingereichter Leistungen. In einer Zusammenschau dieser einzelnen Verarbeitungsvorgänge kann eine Lernplattform als Produkt abgebildet werden, das einer Zertifizierung zuträglich ist.

Derzeit führt das BMBWF ein Pilotprojekt mit datenschutzrechtlichen Beratungsaudits der beiden Lernplattformen LMS und edu.vidual zur Vorbereitung auf die datenschutzrechtliche Zertifizierung nach Art 42 DSGVO durch. Diese Audits erfolgen unter der Herbeiziehung von Expertinnen und Experten der Research Institute AG & Co KG, wobei der aktuelle Evaluierungsgegenstand allgemeine Konformitätsaspekte umfasst. Die im weiteren Projektverlauf erwarteten Erkenntnisse werden zur kritischen Evaluierung des jeweiligen DSMS sowie geeigneter Verarbeitungsvorgänge im Hinblick auf das avisierte Zertifizierungsaudit herangezogen.

Die Ergebnisse dieses Projekts sollen als Leitfaden für die Zertifizierung weiterer Verarbeitungsvorgänge im Bildungsbereich sowie einer ersten Aufwandsschätzung dienen, wobei Synergien zur kontinuierlichen Verbesserung von datenschutzrechtlichen Prozessen des BMBWF genutzt werden.

Der bisherige Ablauf dieses zum Zeitpunkt der Verfassung der Masterthesis noch laufenden Projekts stellt sich dar wie folgt:

- Eingangs erfolgte eine Bestandaufnahme mit allen beteiligten Stakeholdern, um den Umfang der geplanten Zertifizierung festzulegen. In dieser Phase des Projekts wurde auch das Ausmaß der erforderlichen datenschutzrechtlichen Dokumentation erörtert, die seitens des BMBWF sowie der beiden Lernplattformen zur Verfügung gestellt wird. Die Vorlage bestehender Löschkonzepte, eines Verzeichnisses der Verarbeitungstätigkeiten, ausgearbeiteter Konzepte für die Wahrung von

Betroffenenrechten sowie etwaiger Auftragsverarbeitervereinbarungen erwies sich hierbei als geeignet.

- Im Zuge mehrstündiger Workshops beantworteten die externen Auditorinnen und Auditoren Fragen zum bevorstehenden Beratungsaudit und es wurde die Bedeutung der angestrebten datenschutzrechtlichen Zertifizierung für die jeweilige Anwendung erörtert. Bereits zu diesem Zeitpunkt konnte ein hohes Maß an intrinsischer Motivation zur Durchführung des Projekts verzeichnet werden, da es als Gelegenheit zur professionellen Evaluierung der jeweils implementierten Prozesse und der Organisation des DSMS angesehen wurde.

- Im weiteren Projektverlauf wurde für jede Lernplattform ein eigener Auditplan auf der Grundlage der ÖNORM A 2017 sowie unter Zugrundelegung spezifischer Kriterienkataloge erstellt. Im Zuge dieser Planung legte das Projektteam die genauen Ziele, den Umfang, die zeitliche Gestaltung der Überprüfung sowie die erforderlichen Mitwirkungspflichten im Zusammenhang mit dem geplanten Beratungsaudit fest.

- Unter Zugrundelegung eines Prüfschemas nach Maßgabe der ÖNORM A 2017 wurden die zur Verfügung gestellten Dokumente gesichtet. Anhand dieses Dokumentenaudits erfolgte die Überprüfung der bisherigen organisatorischen Prozesse aus dem Bereich der Informationssicherheit und des Datenschutzes.

- Nach der Sichtung der vorliegenden Dokumente erfolgen jeweils zwei halbtägige Audit – Workshops zur Erstellung eines „Soll – Ist“ Vergleichs anhand des zu Projektbeginn festgelegten Prüfungsumfangs. Die daraus gewonnenen Erkenntnisse werden in einem Bericht zusammengefasst und allen Beteiligten in Form einer „Gap – Analyse“ mitgeteilt. Dieser Bericht wird schließlich auch in einer Abschlussbesprechung erörtert. Im Zuge des finalen Prüfberichts werden die ermittelten Ergebnisse unter Zugrundelegung von Empfehlungen zur etwaigen Implementierung von Verbesserungen des jeweiligen DSMS in Schriftform übermittelt.

Der Beratungscharakter dieses friendly Audits wird dadurch verdeutlicht, dass die externen Expertinnen und Experten über die bloße Konformitätsbeurteilung des Zertifizierungsgegenstands mit dem zugrundeliegenden Prüfplan hinaus für bestehende Fragen zur Verfügung stehen und Möglichkeiten zur Verbesserung des jeweiligen DSMS

aufzeigen. Das BMBWF ist sich der Verantwortung zur stetigen Weiterentwicklung und Verbesserung datenschutzrechtlicher Prozesse und Abläufe bewusst und verortet in der Durchführung dieses Pilotprojektes eine geeignete Möglichkeit, die beiden betriebenen Lernplattformen und hinkünftig auch weitere Anwendungen im Bildungsbereich bestmöglich auf die bevorstehende Zertifizierung nach Art 42 DSGVO vorzubereiten.[192]

[192] Anm: Die Abbildung der beschriebenen Prozesse erfolgt anhand der Wahrnehmung des Verfassers der Masterthesis als zuständiger Projektleiter der datenschutzrechtlichen Beratungsaudits im BMBWF.

4. Zusammenfassung der aufgestellten Thesen

1. Die Erkenntnisse aus den aktuellen Vorbereitungen auf die Vornahme datenschutzrechtlicher Zertifizierungen nach Artikel 42 DSGVO verdeutlichen, dass die zu zertifizierenden Anwendungen im österreichischen Bildungsbereich hiervon profitieren und ihre bestehenden datenschutzrechtlichen Prozesse zielführend optimieren können. Im Hinblick auf den im Bildungsbereich von Datenverarbeitungsvorgängen betroffenen Personenkreis stellt die Zertifizierung eine vielversprechende Möglichkeit zur Attestierung des von der DSGVO geforderten Datenschutzniveaus dar. Die Zertifizierung erster Anwendungen aus dem Bildungsbereich ist vorgesehen, sobald entsprechende Zertifizierungsstellen in Österreich akkreditiert werden.

2. Die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO unterscheidet sich durch ihre rechtliche Verankerung auf der Ebene des europäischen Sekundärrechts von bisherigen Konformitätsbeurteilungen im Bereich des Datenschutzes. Im Vergleich zu den meisten privatwirtschaftlich etablierten Zertifizierungen müssen die zugrundeliegenden Zertifizierungskriterien hierbei durch die nationale Aufsichtsbehörde oder den Europäischen Datenschutzausschuss genehmigt werden.

3. Durch die Harmonisierung des Datenschutzniveaus im Geltungsbereich der DSGVO sowie koordinierte Zertifizierungskriterien weist die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO ein großes Potential zur Etablierung eines bisher unerreichten, transnationalen Qualitätsstandards im Bereich des Datenschutzes auf.

Abstract

Die Masterthesis setzt sich mit den folgenden Forschungsfragen auseinander:

- Können datenschutzrechtliche Zertifizierungen nach Artikel 42 DSGVO im österreichischen Bildungsbereich zielführend vorgenommen werden?
- Wie unterscheidet sich die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO von bisher bereits etablierten Zertifizierungen?
- Weist die datenschutzrechtliche Zertifizierung nach Artikel 42 DSGVO das Potential zur Etablierung eines transnationalen Qualitätsstandards im Bereich des Datenschutzes auf?

Die Zielsetzung der Masterthesis liegt in der strukturierten Untersuchung von Voraussetzungen und Vorteilen einer Implementierung der datenschutzrechtlichen Zertifizierung nach Artikel 42 DSGVO im österreichischen Bildungsbereich.

Es erfolgt eine allgemeine Gegenüberstellung risikobasierter Gesichtspunkte unter der Berücksichtigung ihrer Systematik innerhalb der DSGVO sowie eine Auseinandersetzung mit praxisbezogenen Anwendungsmöglichkeiten innerhalb des Wirkungsbereiches des Bundesministeriums für Bildung, Wissenschaft und Forschung.

Abstract – english version

The Master's thesis deals with the following research questions:

- Is the Austrian education sector capable of effectively implementing data protection certifications in accordance with Article 42 of GDPR?
- How does the data protection certification in accordance with Article 42 GDPR differ from already established certifications?
- Does data protection certification in accordance with Article 42 GDPR have the potential to establish a transnational quality standard in the field of data protection?

The objective of the master's thesis is to provide a structured analysis of the requirements and advantages of implementing data protection certification in accordance with Article 42 GDPR in the Austrian education sector.

At the beginning, the master thesis makes a general comparison of risk-based aspects under their systematic consideration within the GDPR, as well as a practice-oriented examination of potential application possibilities within the scope of the Austrian Federal Ministry of Education, Science and Research.

Literaturverzeichnis

Aichinger, Wie Hermann Nitsch Chat-GPT-Nutzern hilft, Die Presse 2023/21/01.

Bergauer/Jahnel, Das neue Datenschutzrecht, 3. Auflage (2018).

Bergt/Pesch in Kühling/Buchner, DS-GVO, 3. Auflage, Art 42 Rz 15.

Bogendorfer in Knyrim (Hrsg), DatKomm Art 28 DSGVO Rn 56 - 57 (Stand: 1.12.2022).

DSK, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen (2018).

EDSA Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0. (2021).

EDSA Leitlinien 04/2019 zu Artikel 25 DSGVO, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0 (2020).

EDSA Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, Version 3.0 (2019).

EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals (2023).

Geuer/Reinisch, Haftung des Auftragsverarbeiters nach der DSGVO, Dako 2019/47, 82-85.

Gühr/Karper/Maseberg, Der lange Weg zur Akkreditierung nach Art. 42 DSGVO, DuD 2020/10, 649 – 653.

Haase, Der Begriff der "Gesundheitsdaten" nach der Datenschutz-Grundverordnung (DSGVO), InTeR 2022, 94.

Haidinger, Meine Tochter fährt auf Schulskikurs, Dako 2023/13.

Haidinger/Löffler, Lehrerin verletzte durch Fotoaufnahme Geheimhaltungsrecht von Schüler, Dako 2023/10, 17.

Heiler/Ciarnau, Datenanonymisierung der Schlüssel zum Erfolg, ecolex 2022/114, 166.

Herold/Tober, DSGVO-Zertifizierung - Das Europäische Datenschutzsiegel, CB 2023, 361.

Heidegger, In Schulen darf Datensicherheit kein Zufall sein!, Dako 2023/3, 4-6.

Hofer, Überlegungen zur anonymisierenden Wirkung der Pseudonymisierung im Außenverhältnis am Beispiel von Cloud-Computing, jusIT 5/2022, 173-176.

Hofmann, Dynamische Zertifizierungen, Datenschutzrechtliche Zertifizierung nach der Datenschutzgrundverordnung am Beispiel des Cloud Computing 1. Auflage (2019) 62 – 164.

Hötzendorfer/Kastelitz/Tschohl in Knyrim (Hrsg), DatKomm Art 24 DSGVO (Stand: 1.5.2022).

Jahnel (Hrsg), Kommentar zur Datenschutz-Grundverordnung (2021).

Jahnel/Pallwein-Prettner, Datenschutzrecht, 3. Auflage (2021).

Kamara, Leenes, Lachaud, Stuurman, Van Lieshout, Bodea, Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final report of the European Commission (2019).

Kircher, Mit Digitaler Souveränität den Wandel selbstbestimmt gestalten (2020).

Knyrim (Hrsg), Praxishandbuch Datenschutzrecht, 4. Auflage (2020).

Knyrim (Hrsg), Praxiskommentar zum Datenschutzrecht – DSGVO und DSG – DatKomm (Stand: 01.12.2023).

Kröpfl, Datenschutzrechtliche Zertifizierungen, Jahrbuch Datenschutzrecht 2019, 163.

Kröpfl, Von der Akkreditierung der DS-GVO-Zertifizierungsstellen, jusIT 2021/74, 198 – 201.

Kröpfl, Konformitätsbewertung im Datenschutzrecht, Jahrbuch Datenschutzrecht 2020, 221-225.

Lamprecht, Cyber-Security: Das unterschätzte Risiko?, DJA 2018/9.

Löffler, Cyber Security in der Risikoberichterstattung, Dako 2021, 118.

Mertens, Accountability im europäischen Datenschutzrecht Kapitel B (Stand: 30.6.2023).

Niederbacher, Datenschutz und Informationssicherheitsmanagementsysteme, GRC aktuell 2018, 122.

Novotny/Menzel, Datenschutz in der Schule, Dako 2023/4, 7-9.

Pachinger, Zeit wird knapp: Sechs Monate bis zum neuen Datenschutz, Die Presse 2017/47/05.

Piltz in Gola/Heckmann (Hrsg), DS-GVO Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen, 3. Auflage (2022) 597 f.

Pollirer, DSGVO und Informationssicherheit, in Knyrim (Hrsg), Praxishandbuch Datenschutzrecht, 4.Auflage (Stand: 1.4.2020).

Pollirer in Knyrim (Hrsg), DatKomm Art 32 DSGVO (Stand: 1.5.2022).

Pollirer/Weiss/Knyrim/Haidinger, Datenschutzgrundverordnung, 2. Auflage (Stand: 1.7.2022).

Roth, Die systemische Umsetzung von Organisationspflichten des Verantwortlichen am Beispiel des Art. 30 DSGVO, DSB 2023, 230.

Schefzig in Moos/Schefzig/Arning (Hrsg), Praxishandbuch DSGVO einschließlich BDSG und spezifischer Anwendungsfälle, 2. Auflage (Stand: 1.4.2021) Kapitel 10 Rn 4.

Schmidl, Die Datenschutzbehörde am 25. 5. 2018 - Funktion und Stellung der DSB nach der DS-GVO und dem DSG (2018), jusIT 2017/79.

Schmidt/Brink in Wolff/Brink/Ungern-Sternberg (Hrsg), Beck‘scher Online-Kommentar Datenschutzrecht DS-GVO, 44. Edition (2022) Art 24.

Schröder, Der risikobasierte Ansatz in der DS-GVO, ZD 2019/11, 503.

Stadler/Drolz, Pflicht und Kür bei der Abwehr von Cybercrime, Die Presse 2023/09/03.

Strohmaier in Knyrim (Hrsg), DatKomm Art 42 DSGVO Rn 1, 7 – 8, 12, 22/1 – 22/13 (Stand: 1.5.2022).

Struck/Aßhoff, Privacy Tech als Anwendungsfall für Legal Tech Applikationen Technologiegestütztes Datenschutzmanagement - neue Anwendungsfälle treiben die Digitalisierung und Integration voran, LTZ 2022, 224 – 225.

Trieb/Kröpfl, Datenschutzzertifizierungen in greifbarer Nähe, Dako, 2020/32, 52 - 54.

Tschohl, Kastelitz, Hospes, Rothmund-Burgwall, Datenschutzrechtliche Fragestellungen beim Einsatz von Clouddienste-Anbietern (2022) 82.

Veil, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD 2015, 347 f.

Wolff/Brink/Ungern-Sternberg (Hrsg), Beck‘scher Online-Kommentar Datenschutzrecht DS-GVO 44. Edition (2022).

Judikaturverzeichnis

BVwG 27.4.2022, W214 2237072-1.

BVwG 30.9.2020, W274 2225135-1.

DSB 19.9.2023, 2023-0.632.875 (Verfahrenszahl: DSB-D130.1174).

DSB 22.6.2022, 2022-0.442.409 (Verfahrenszahl: DSB-D124.4479).

DSB 22.2.2021, 2020-0.833.281 = ZVers 2021, 69.

DSB 23. 7. 2019, DSB-D123.822/0005-DSB/2019.

DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018.

DSB 13.9.2018, DSB-D123.070/0005-DSB/2018.

EuG 12.10.2023, T-553/23 R.

EuGH 14.12.2023, C-340/21
(Natsionalna agentsia za prihodite).

EuGH 05.12.2023, C-807/21
(Deutsche Wohnen SE gg Staatsanwaltschaft Berlin).

EuGH 05.12.2023, C-683/21 d
(Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos gg Valstybinė duomenų apsaugos inspekcija).

EuGH 19.10.2016, C-582/14
(Breyer gg Bundesrepublik Deutschland).