Strategiebericht

Kapazitätsaufbau für Informationssicherheit bei europäischen Bürger*innen und Arbeitnehmer*innen

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Dieses Dokument wurde im Rahmen des ERASMUS+-Projekts "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi" erstellt, Projekt-ID: 2018-1-EN02-KA202-005218

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

Mit ihrem Inkrafttreten im Jahr 2018 hat die Datenschutz-Grundverordnung einen Wandel in der Wahrnehmung und im Wert personenbezogener Daten bei Verbraucher*innen, Unternehmen und in der Gesellschaft insgesamt ausgelöst. Die Einführung verbindlicher und sanktionierbarer Standards und Gesetze für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten sollte die Rechte der Verbraucher*innen stärken, der Nutzung und Erhebung von Daten Grenzen setzen und letztlich das Recht auf Privatsphäre und persönliche Freiheit im digitalen Zeitalter stärken und gewährleisten.

Seitdem sind nach vielen öffentlichen Diskussionen über Sinn und Unsinn sowie „Dos und Don'ts“ erste Reibungen überwunden, und die anfängliche Welle der Aufmerksamkeit ist abgeflacht. Datenschutz ist zu einem festen Bestandteil der Arbeit eines jeden Unternehmens geworden. Die Unternehmen sind nicht nur verpflichtet, Verantwortlichkeiten für die ordnungsgemäße Durchführung des Datenschutzes in ihrem Unternehmen zuzuweisen, sondern jede Mitarbeiterin und jeder Mitarbeiter muss sich über mögliche Datenschutzverletzungen in ihrem/seinem Arbeitsalltag und die Einhaltung festgelegter Verfahren im Klaren sein. Schließlich haben auch die Beschäftigten selbst ein Interesse am Schutz ihrer Daten, wenn sie ein Arbeitsverhältnis eingehen, was unter dem Arbeitnehmerdatenschutz subsumiert wird. Die Mitarbeiter*innen als schwächstes Glied in der Informationssicherheitsstrategie eines Unternehmens müssen dabei besondere Beachtung finden. Während Großkonzerne erfolgreich eine Reihe von Schulungsprogrammen zur Sensibilisierung ihrer Mitarbeiter*innen aufgelegt haben, sind die Prioritäten in KMUs zum Aufbau von Informationssicherheits- und Datenschutzkapazitäten im Vergleich dazu gering geblieben.

Die Informationssicherheit, die im Gegensatz zum Datenschutz keine zwingende Position oder rechtlich bindende Vorgaben für die Arbeit von Organisationen darstellt. Sie berührt jedoch viele Aspekte der Datenverarbeitung, -erhebung und -speicherung und erfordert daher eine breite Aus- und Weiterbildung des verantwortlichen Personals. Aus- und Weiterbildung, insbesondere im Zusammenhang mit dem Know-how-Schutz eines Unternehmens, bleibt ein zentraler Aspekt zur Erhöhung der Sicherheit von KMU in der EU. In diesem Bericht wollen wir die Voraussetzungen und Perspektiven der Aus- und Weiterbildung von Informationssicherheits- und Datenschutzkompetenzen in der EU darlegen und Empfehlungen für die weitere Entwicklung insbesondere im KMU-Umfeld geben.

2 Datenschutz in den Partnerländern

2.1 Polen

Name der Einrichtung	Kurzbeschreibung	Website
Urząd Ochrony Danych Osobowych (UODO) (Amt für den Schutz personen-bezogener Daten)	UODO ist die wichtigste staatliche Einrichtung, die sich mit dem Schutz personenbezogener Daten befasst. Im Rahmen der Aufgaben, die durch Art. 57 DSGVO zugewiesenen Aufgaben gehören unter anderem: die Überwachung und Durchsetzung der Anwendung der DSGVO; die Verbreitung von Wissen über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung in der Gesellschaft sowie das Verständnis für diese Phänomene; die Beratung des nationalen Parlaments, der Regierung und anderer Institutionen und Einrichtungen in Datenschutzangelegenheiten, die Prüfung von Beschwerden, die von der betroffenen Person oder der Einrichtung, Organisation oder Vereinigung eingereicht werden; die Durchführung von Verfahren in Bezug auf die Anwendung der DSGVO, der Erlass von Entscheidungen und - wenn es verhältnismäßig ist - die Festlegung der Höhe von Bußgeldern für Verstöße gegen die DSGVO und deren Verhängung.	
Das GovTech-Zentrum	Das GovTech-Zentrum hat einen Teil der Aufgaben des Ministeriums für Digitalisierung übernommen, das im Herbst 2020 aufgelöst wurde. Die direkten Empfänger*innen von GovTech-Diensten sind die weit gefasste lokale und zentrale Verwaltung sowie andere Einrichtungen, die öffentliche Aufgaben erfüllen, wie Krankenhäuser, Schulen oder Verkehrsunternehmen. Die Empfänger*innen von GovTech-Diensten sind der öffentliche Sektor, aber auch Unternehmen.	
Fundacja Panoptykon (Die Stiftung Panoptykon)	Die Stiftung Panoptykon überwacht die Überwachungspraktiken. Sie prüft das geltende Recht, die Tendenzen der Gesetzgebung, die Maßnahmen der Behörden und der privaten Unternehmen. Sie verfolgt die Berichte der Medien und der Zivilgesellschaft. Sie analysieren die gesammelten Informationen, stellen Probleme fest und reagieren. Sie nehmen Stellung zu Vorschlägen für neue Gesetze, erheben Einwände gegen bestehende Gesetze und machen eigene Vorschläge für Änderungen. Sie weisen auf Missstände und Nachlässigkeiten hin.	

Państwowy Instytut Badawczy NASK	NASK - ein staatliches Forschungsinstitut, das der Kanzlei des Premierministers untersteht. Die Aufgabe ist die Suche nach und die Umsetzung von Lösungen, die der Entwicklung von IKT-Netzen in Polen und der Verbesserung ihrer Effizienz und Sicherheit dienen. Das Institut führt wissenschaftliche Forschungs- und Entwicklungsarbeiten sowie operative Tätigkeiten zum Nutzen der Sicherheit des polnischen zivilen Cyberspace durch. Ein weiteres wichtiges Element der NASK-Tätigkeit ist die Aufklärung der Nutzer*innen und die Förderung des Konzepts der Informationsgesellschaft, vor allem zum Schutz von Kindern und Jugendlichen vor den Gefahren, die mit der Nutzung der neuen Technologien verbunden sind.	
ZFODO Związek Firma Ochrony Danych Osobwych (Verband der Unternehmen für den Schutz personen-bezogener Daten)	Die in der Association of Personal Data Protection Companies zusammengeschlossenen Unternehmen verfügen über langjährige Erfahrung in der Unternehmensberatung im Bereich des Schutzes personenbezogener Daten. Sie erbringen professionelle Dienstleistungen auf höchstem Niveau für die größten Unternehmen des privaten Sektors sowie für lokale und zentrale Regierungsstellen. Sie verfügen über Erfahrungen in einer Vielzahl von Sektoren und Branchen, die es ihnen ermöglichen, ihren Klient*innen individuelle, auf deren Bedürfnisse zugeschnittene Lösungen anzubieten. Sie haben viele Geschäftspartner - Anwaltskanzleien, IT- und Marketing-Beratungsunternehmen. Dadurch können sie ihre Klient*innen umfassend beraten - nicht nur im Bereich des Datenschutzes, sondern im Bereich des gesamten Geschäfts ihrer Klienten.	www.zfodo.org.pl
Fundacja Wiedza To Bezpieczeństwo (Stiftung Wissen ist Sicherheit)	Die Stiftung popularisiert das Wissen im Bereich der Informationssicherheit. Sie organisiert wissenschaftliche Konferenzen und hilft bei der Lösung von Problemen, mit denen die Menschen im täglichen Leben konfrontiert sind, sowohl im privaten als auch im geschäftlichen Bereich. Sie führen soziale Kampagnen durch, um das Bewusstsein zu schärfen. Auf diese Weise zeigen wir, welche Gefahren im Zusammenhang mit der unrechtmäßigen Nutzung unserer personenbezogenen Daten drohen.	

Tabelle 1: Interessenvertretung aus Polen.

Zu den häufigsten Fehlern im Zusammenhang mit der Umsetzung von RODO (polnisches Äquivalent zu GDPR) in polnischen Unternehmen gehört laut dem Bericht "10 größte Fehler bei der Einhaltung von RODO", dass ZFODO am häufigsten genannt wird:

- Missverständnis der Idee von RODO, d.h. Umsetzung nur "auf dem Papier". Dies hat zur Folge, dass niemand die Verfahren kennt und befolgt. Die mangelnde Umsetzung kann zu Sanktionen seitens der Aufsichtsbehörde führen.
- Unzureichendes Bewusstsein für die Informationssicherheit. Durchführung von Risikoanalysen durch unqualifiziertes Personal oder solche mit zu wenig Erfahrung, was zu fehlenden oder falsch durchgeführten Analysen führt. Das Ergebnis sind nicht erkannte Bedrohungen, mögliche Datenverluste und mangelnde Sicherheit.
- Unzureichender IT-Bereich, Fehlen einer festgelegten Datenaufbewahrungspolitik oder mangelnde Umsetzung von Aufbewahrungsregeln in IKT-Systemen. Das Ergebnis kann der Verlust von Daten oder der unbefugte Zugriff auf Daten sein, und die Unfähigkeit, die Rechte, auf die sich die Daten beziehen, zu realisieren.

Darüber hinaus wurden folgende Punkte genannt: fehlerhafte Datenschutz-Folgenabschätzung, fehlende Regelung des Verhältnisses zwischen den Einrichtungen, Verwirrung zwischen den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsverarbeiter", fehlende Umsetzung des Verfahrens zur Informationspflicht, fehlender Koordinator für die Umsetzung der Verfahren, fehlende Sensibilisierung der Mitarbeiter*innen, fehlende ganzheitliche Betrachtung der Umsetzung.

Die oben genannten Bereiche sind die "Hauptsünden", aber es gibt auch andere Aspekte der Umsetzung der neuen Verordnungen, die sich als problematisch erwiesen haben.

So wird beispielsweise die Rolle des Datenschutzbeauftragten meist unterschätzt und seine Stellung in der Organisation ist gering. Oft ist der DSB eine "handverlesene" Person. Die Rolle des behördlichen Datenschutzbeauftragten wird häufig unterschätzt, und seine Stellung in der Organisationsstruktur ist gering. Der DSB wird häufig eingestellt, verfügt nicht über die entsprechenden Qualifikationen und hat wenig Einfluss auf die Entscheidungen der obersten Führungsebene; seine Stimme wird nur als beratende Stimme behandelt. Der Bericht wird auf Polnisch veröffentlicht von(ZFODO 2020) ZFODO (2020) .

Informationen darüber, wie RODO in der Praxis umgesetzt wurde, und über das Ausmaß von Verstößen und Vorfällen im Zusammenhang mit dem Schutz personenbezogener Daten bei polnischen Unternehmen und Institutionen finden sich unter anderem in einem Bericht, der vom Verband der Datenschutzunternehmen (ZFODO) erstellt wurde.

Der Bericht umfasst 454 Organisationen, die von ZFODO-Mitgliedsunternehmen im Zeitraum Mai 2019 bis Mai 2020 betreut werden. Zu den Befragten gehörten Organisationen und Unternehmen sowohl aus dem privaten als auch aus dem öffentlichen Sektor. Die Statistik zeigt, dass ein Vorfall (Datenschutzvorfall) bei einem durchschnittlichen Verantwortlichen statistisch gesehen 0,65 Mal pro Jahr auftritt. Das

ist zu wenig, um die nötige Übung in der Vermeidung oder Bewältigung solcher Vorfälle zu erlangen, während ein Fehler im Umgang mit auch nur einem einzigen Vorfall katastrophale Folgen für das Unternehmen haben kann.

Der Bericht zeigt, dass fast 70 % der Vorfälle nicht an die Aufsichtsbehörde gemeldet wurden. Gemäß Artikel 33 Absatz 1 der RODO muss ein Vorfall nicht an die Aufsichtsbehörde gemeldet werden, wenn "der Verstoß wahrscheinlich nicht zu einem Risiko der Verletzung der Rechte oder Freiheiten natürlicher Personen führt". In 70 % der Fälle wurden die von diesen Vorfällen betroffenen Personen nicht informiert. Unabhängig von der Meldung des Vorfalls an die Aufsichtsbehörde sollten wir gemäß Artikel 34 der RODO auch die betroffenen Personen selbst informieren, wenn eine Verletzung der Rechte oder Freiheiten natürlicher Personen wahrscheinlich zu einem hohen Risiko führt.

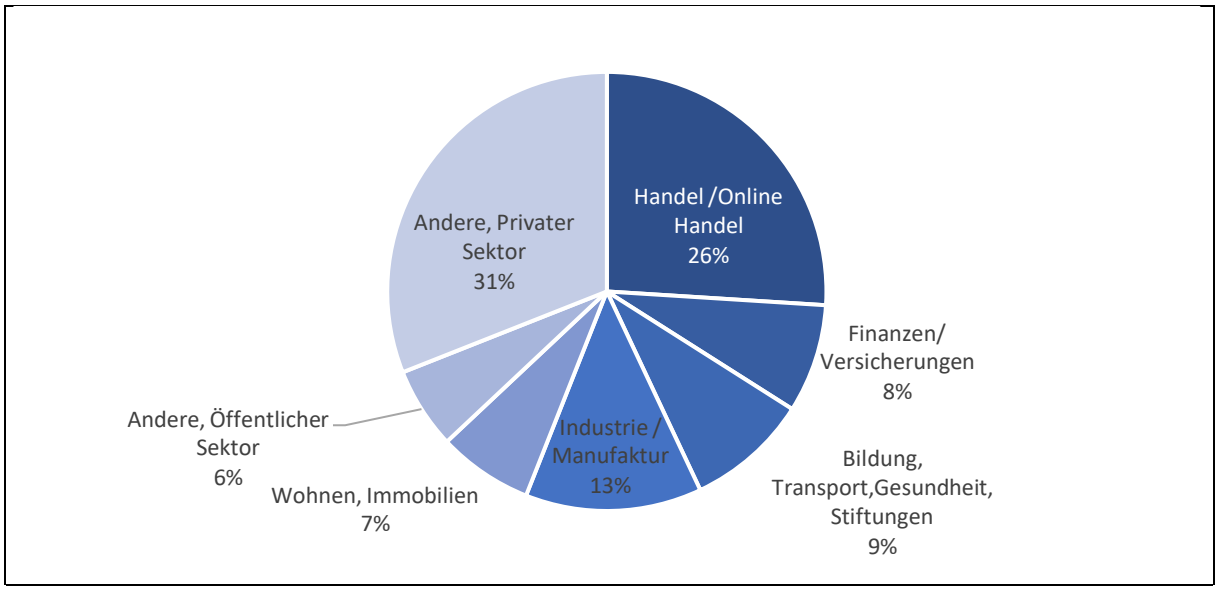

Abbildung 1: Industrien/Branchen, die am meisten von Verletzungen des Schutzes personenbezogener Daten bedroht sind
Quelle: ZFODO (2021) Eigene Darstellung.

Die Quellen für Verstöße gegen den Schutz personenbezogener Daten lagen sowohl innerhalb des Unternehmens/der Einrichtung (68 %) als auch außerhalb (20 %) und gingen vom so genannten Auftragsverarbeiter aus, d. h. einer Stelle, die Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet (12 %). Zu den Externen gehören z. B. ehemalige Mitarbeiter*innen oder Hacker, zu den Internen - Mitarbeiter und Beschäftigte der Organisation.

In 92 % der Fälle handelte es sich um unbeabsichtigte Vorfälle (falsch adressierte E-Mails, Fehlen einer versteckten Kopie, Versand herkömmlicher Korrespondenz mit falschem Inhalt). Zu den vorsätzlichen Vorfällen gehörten: Diebstahl von Laptops oder anderen Datenträgern, Phishing, Weitergabe von Daten an Unbefugte. Fast 96 % der Vorfälle wurden durch persönliche Gründe verursacht. Dazu gehörte das Handeln eines menschlichen Faktors. Nicht personenbezogene Ursachen sind Situationen, in

denen die Verletzung durch eine Fehlfunktion der Technologie verursacht wurde, Situationen, die sich der Kontrolle des menschlichen Willens entziehen.

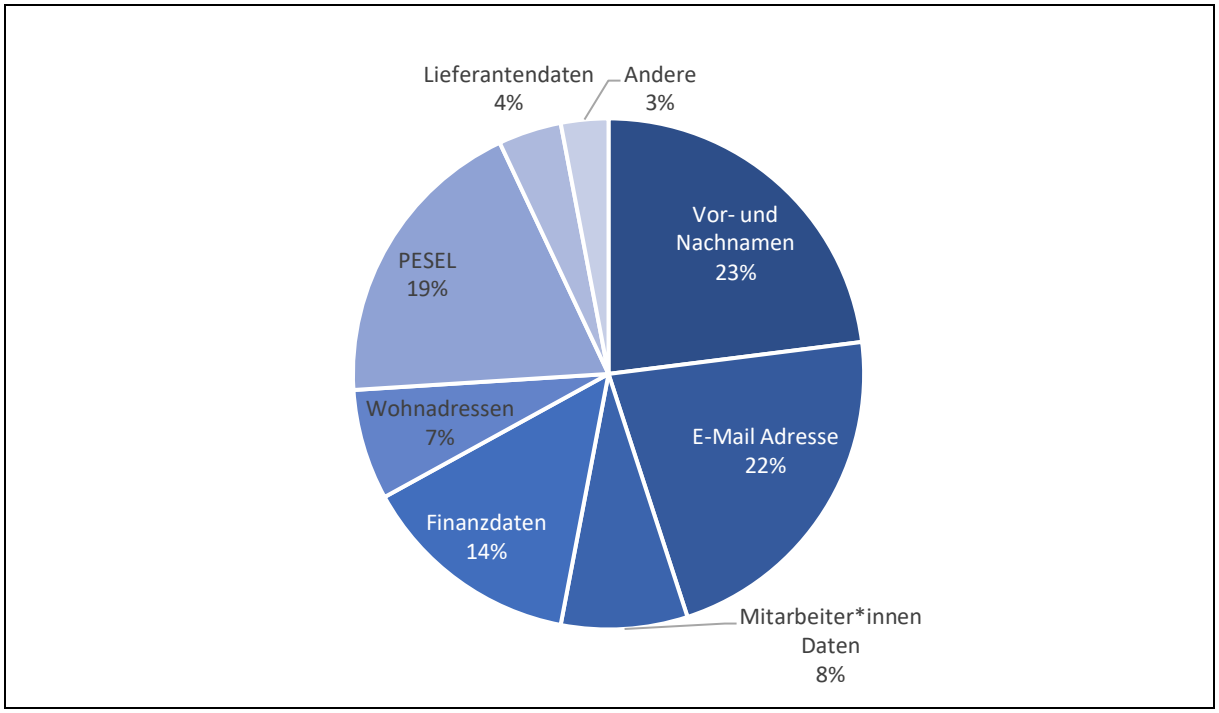

Abbildung 2: Am häufigsten verletzte Datenkategorien.
Quelle: ZFODO (2021) Quelle: ZFODO (2021) , eigene Darstellung.(ZFODO 2021)

Was den Schutz personenbezogener Daten von Arbeitnehmern betrifft, so wurde leider kein Bericht gefunden, der das Ausmaß und die häufigsten Situationen im Zusammenhang mit diesem Thema in Polen analysiert. Um den Einstellungsprozess zu erleichtern und die Orientierung in den Vorschriften zu erleichtern, hat das UODO (Amt für den Schutz personenbezogener Daten) eine Veröffentlichung mit dem Titel "Schutz personenbezogener Daten am Arbeitsplatz. Leitfaden für Arbeitgeber" herausgegeben. (Amt für den Schutz personenbezogener Daten 2018) .

2.2 Österreich

Name der Einrichtung	Kurzbeschreibung	Hauptzweck	Website
WKO – Wirtschafts-kammer Österreich / WKO Wirtschafts-kammer	Die WKO fordert die Unternehmen auf, eine geeignete Sicherheitsstrategie zu entwickeln, die vor möglichen Bedrohungen schützt.	Die Sensibilisierung der Mitarbeiter*innen ist ein wichtiger Sicherheitsfaktor. Es wurde eine eigene Abteilung für IT-Sicherheit und Datensicherheit eingerichtet. Die KMU werden durch verschiedene Initiativen unterstützt.	https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
Österreichische Datenschutz-behörde / Austrian Data Protection Authority (DSB)	Die Österreichische Datenschutzbehörde ist die nationale Aufsichtsbehörde für den Datenschutz in der Republik Österreich.	Das Rechtsinformationssystem der Republik Österreich (www.ris.bka.gv.at) bietet die österreichische Gesetzgebung in ihrer aktuellen Fassung (Bund und Länder), Gesetzblätter (Bund und Länder) und Rechtsprechung.	www.dsb.gv.at
BFI Wien Schulung Datenschutz und IS	Schulungsanbieter für Datenschutz und IS	Als staatlich anerkanntes Weiterbildungsinstitut ist das BFI berechtigt, Zertifizierungen auszustellen und Anerkennungsverfahren für non-formale Bildungsangebote bei der NQR-Koordinierungsstelle (NKS) - oder über seine Servicestellen - einzureichen.	https://www.bfi.wien/edv-und-informationstechnologien/datenschutz-und-informationssicherheit/
KMU-Plattform	Dieses Netzwerk von Experte*innen aus Wirtschaft und Technologie wurde zur Unterstützung von KMU in Österreich gegründet, um Unternehmen im digitalen Wandel zu begleiten.	Neben vielen anderen Dienstleistungen werden auch Workshops zu den unterschiedlichsten Themen angeboten. Der Slogan "Gemeinsamkeit statt Größe" macht deutlich, dass der Schwerpunkt auf der Zusammenarbeit zwischen kleinen Unternehmen liegt, die sich damit einen Wettbewerbsvorteil verschaffen.	https://www.kmu-plattform.eu/
Agentur für Digitalisierung / Digitalisierungs-agentur	Innerhalb der FFG, der Forschungsförderungs gesellschaft, wurde die "Digitalisierungsagentur" eingerichtet, die Förderungen an KMU -	Damit vor allem Österreichs Klein- und Mittelbetriebe (KMU) ihre Chancen bei der Digitalisierung bestmöglich nutzen können, bietet die "Initiative KMU DIGITAL" konkrete Hilfestellung: Die	

	kleine und mittlere Unternehmen - in Österreich vergibt, um die Digitalisierung gezielt zu fördern.	Unternehmen profitieren von Förderungen für Beratung, Qualifizierung, Wissenstransfer und Weiterbildung.	
Wiener Wirtschafts-agentur / Wirtschafts-agentur Wien	Das Förderprogramm "Wien Digital" unterstützt MEs und KMUs bei der Umsetzung von Digitalisierungsmaßnahmen.	Die Wirtschaftsagentur Wien bietet persönliche Beratung und verfügt über ein breites Netzwerk an KMU und (öffentlichen) Kooperationspartnern. Startups, EinzelunternehmerInnen, nationale und internationale Klein- und Mittelbetriebe oder Konzerne werden in wichtigen Fragen unterstützt.	https://wirtschaftsagentur.at/
Business Circle	Anbieter eines Lehrgangs zum zertifizierten Datenschutzbeauftragten	Die im Lehrgang erworbenen Qualifikationen werden nach einer positiv beurteilten Abschlussprüfung mit dem Zertifikat von Austrian Standards nach den Kriterien der ISO/IEC 17024 bestätigt.	https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/
1a Beratung e.U. - Ing. Roland Fürbas	Privater Anbieter für GDPR- und IS-Schulungen	Daten- und IT-Sicherheit / DSGVO-DSB / Geschäftsentwicklung / Online-Dienste	http://www.1a-beratung.eu
72Lösungen	Privater Anbieter für GDPR- und IS-Schulungen	GDPR – Experte*innen, die beraten und maßgeschneiderte Lösungen für Datenschutzmaßnahmen entwickeln.	https://www.72solutions.eu
TÜV Austria Akademie	Anbieter von Schulungen zum Datenschutz - GDPR-Experte	Das Angebot umfasst rund 20 Kurse, die nach Branchen gegliedert sind.	https://www.tuv-akademie.at/kursprogramm?s=Datenschutz

Tabelle 2: Stakeholder aus Österreich

Österreich war eines der ersten europäischen Länder mit einer Behörde für Datenschutz, der Datenschutzkommission. Sie wurde mit dem ersten Datenschutzgesetz, Bundesgesetzblatt Nr. 565/1978, geschaffen. Mit der EU-Datenschutzrichtlinie 95/46/EG wurde das Datenschutzrecht europaweit auf eine neue Grundlage gestellt (EUR-LEX 1995) . In Österreich wurde diese Richtlinie durch das Datenschutzgesetz 2000 (DSG 2000) umgesetzt (Rechtsinformationssystem des Bundes (RIS) 1999) . Seit dem 25. Mai 2018 stellt die Datenschutz-Grundverordnung (DSGVO) das Datenschutzrecht europaweit auf eine neue Grundlage. EUR-LEX . (1995) . In Österreich wurde diese Richtlinie durch das Datenschutzgesetz 2000 (DSG 2000) umgesetzt. Rechtsinformationssystem des Bundes (RIS) (1999) . Nach dem 25. Mai 2018 werden die Datenschutzgrundverordnung (DSGVO) (Bundesministerium

der Finanzen (BMF)) und das überarbeitete Datenschutzgesetz (DSG) (Bundesministerium der Finanzen (BMF)) die Grundlage für das Datenschutzrecht (siehe DSB 2019).

Laut UGB und GmbHG liegt die Verantwortung für Datenschutz und IT-Sicherheit immer bei der Geschäftsführung. Auch wenn sicherheitsrelevante IT-Aufgaben an Mitarbeiter*innen übertragen werden, trägt die Unternehmensleitung die Letztverantwortung für die Einhaltung der gesetzlichen Bestimmungen. Mit der NIS-Richtlinie (EU) 2016/1148 (EUR-LEX) die in Österreich Ende 2018 durch das Netzwerk- und Informationssystemsicherheitsgesetz (NISG) umgesetzt wurde, gibt es erstmals umfassende Regelungen im Bereich der Cybersicherheit für strategisch wichtige Unternehmen, digitale Dienstleister und Behörden auf europäischer und nationaler Ebene. Unternehmen müssen geeignete technische und organisatorische Maßnahmen (z.B. Datensicherung, Verschlüsselung, Zugangskontrollen) ergreifen, um Daten vor zufälliger Zerstörung, Datenverlust oder unrechtmäßiger Nutzung durch Dritte zu schützen. Andernfalls können hohe Geldstrafen verhängt werden.

Die EU-Datenschutzgrundverordnung (DSGVO) und das österreichische Datenschutzgesetz regeln den Umgang mit personenbezogenen Daten (z.B. Name, Geburtsdatum, E-Mail-Adresse, IP-Adresse). Das bedeutet, dass alle Unternehmerinnen und Unternehmer in Österreich an die gesetzlichen Bestimmungen gebunden sind. Unternehmen, die einen gewissen Digitalisierungsgrad erreicht haben, kennen diese in der Regel gut und werden regelmäßig informiert, insbesondere durch die Wirtschaftskammer. Problematischer sind Kleinstunternehmen, die sich aus Zeit- und Kostengründen oft weniger intensiv mit den Themen IS und EDV auseinandersetzen.

Besonders problematisch scheint die Frage der Informationspflicht nach GDPR zu sein, die laut Conrad Lienhardt in Österreich vor allem in kleinen Unternehmen oft nicht umgesetzt wird: "Die Rechte der betroffenen Personen, also derjenigen, deren personenbezogene Daten verarbeitet werden, beinhalten nach der Datenschutzgrundverordnung (DSGVO) ein umfassendes Recht auf Information. Für die Unternehmen und Organisationen bedeutet dies umfangreiche Informationspflichten. Diese sind in den Artikeln 13 und 14 der DSGVO geregelt." Lienhardt warnt davor, die Informationspflicht zu unterschätzen: "Es gibt Unternehmen und Organisationen, die personenbezogene Daten aus öffentlichen Datenbanken wie Grundbüchern, Adressverzeichnissen etc. beziehen und diese dann verarbeiten. Viele denken, dass sie nicht der Informationspflicht unterliegen, zumal es sich beim "Abschöpfen" von Daten aus öffentlichen Verzeichnissen zudem oft um große Mengen personenbezogener Daten handelt. Mit Beschwerden und privaten Schadensersatzklagen ist zu rechnen. Deshalb gilt hier: Nehmen Sie die Informationspflicht ernst." (Lienhardt 2020) .

Arbeitnehmerdaten nach der EU-Datenschutzgrundverordnung: In Österreich gelten nicht nur datenschutzrechtliche, sondern auch arbeits- und sozialrechtliche

Bestimmungen, wie die WKO betont: "Hier ist zu prüfen, auf welcher Grundlage die Daten verarbeitet werden (gesetzliche Verpflichtung, notwendig für die Erfüllung des Dienstvertrages, Einwilligung...). [...] Da der Lohnverrechner in der Regel aufgrund eines Auftragsverarbeitungsverhältnisses mit dem Auftraggeber (=Verantwortlicher) tätig wird und der Auftraggeber aufgrund des Dienstverhältnisses die Verpflichtung hat, auch korrekt abzurechnen, ist dafür keine Zustimmung des jeweiligen Mitarbeiters des Auftraggebers erforderlich. Sie müssen jedoch einen schriftlichen Auftragsverarbeitungsvertrag abschließen." (Wirtschaftskammer Österreich 2021b) .

Auch die WKO (Wirtschaftskammer Österreich) bietet mit branchenspezifischen Informationen, Leitfäden, Musterdokumenten und Checklisten Unterstützung bei der Umsetzung der DSGVO. Der Leitfaden zu technischen und organisatorischen Maßnahmen im Rahmen der DSGVO gibt einen praktischen Überblick, welche technischen Sicherheitsmaßnahmen notwendig und sinnvoll sind und wie sie im Unternehmen umgesetzt werden können.
(vgl. Wirtschaftskammer Österreich (2020))
Schließlich ist der "IT-Safe" der WKO (Wirtschaftskammer Österreich 2021a) eine gut etablierte und bekannte Initiative zur Unterstützung von KMU bei der Umsetzung von IT-Sicherheitsmaßnahmen.

Den Unternehmen in Österreich stehen zahlreiche Informationsquellen zur DSGVO zur Verfügung. Es liegt jedoch in der Natur der Sache, dass diese sehr umfangreichen Rechtstexte nicht auf einen Blick zu erfassen sind. Hervorzuheben ist in diesem Zusammenhang das Angebot der Wirtschaftskammer Österreich, die eine wichtige Anlaufstelle für alle - vor allem auch für kleine - Unternehmen ist. Mit "IT-Safe" wurde ein umfassender Leitfaden entwickelt, und es werden zahlreiche kostenlose Informationsveranstaltungen angeboten. Ein besonders wichtiges Angebot ist eine professionelle Website, die die wichtigsten Grundlagen der GDPR verständlich darstellt (vgl. Wirtschaftskammer Österreich (2021b)

Ein weiteres attraktives Angebot macht der KSV (Kreditschutzverband), der Unternehmen bei der Einführung der DSGVO auf mehreren Ebenen kostengünstig unterstützt: Beratung, Schulung und die App "DSVGO Assistant" (KSV1870).

Trotz aller Bemühungen spricht man in Österreich immer noch gerne über die "ungeliebte DSGVO"! Wir haben die folgende - aus unserer Sicht - passende Presseaussendung gefunden:

Die ernüchternde Realität in österreichischen Unternehmen

In dieser Pressemitteilung der APA (Austrian Press Agency) vom Mai 2020, Österreichische Presseagentur (2020) berichtet die APA über die Umsetzung der EU-DSGVO in Österreich unter dem Titel: "Verständnis ja, Umsetzung schleppend". (Österreichische Presseagentur) Pressemitteilung vom Mai 2020, Österreichische

Presseagentur (2020) berichtet über die Umsetzung der EU-DSGVO in Österreich unter dem Titel: "Verständnis ja, Umsetzung schleppend".

> "Trotz deutlich gestiegener Sensibilität in Sachen Datenschutz wird die EU-Verordnung seit 2018 nur von 30 Prozent der heimischen Unternehmen vollständig umgesetzt."

Der Artikel hebt hervor, dass zwei Jahre nach Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DSGVO) österreichische Unternehmen ein deutlich gestiegenes Verständnis für das Thema Datenschutz zeigen. In einer vor der Corona-Krise durchgeführten KSV1870-Umfrage im Rahmen des Austrian Business Check im Februar 2020 mit rund 600 Unternehmen gaben 40 % der befragten Unternehmen an, dass dieses in den letzten drei Jahren "auf breiter Front" gestiegen sei. Die Umfrage zeigt deutlich, dass es noch einiges zu tun gibt, bis die EU-DSGVO von allen Unternehmen in Österreich vollständig umgesetzt ist, denn nur 30 % der Befragten haben sie bisher vollständig in ihrem Betrieb verankert. Als am häufigsten umgesetzte Maßnahme zur Erhöhung des Datenschutzes nannten 46% der Umfrageteilnehmer*innen die Einführung oder Anpassung von Datenschutz- und IT-Sicherheitsmaßnahmen. Positiv erwähnt der Autor, dass das Verständnis für einen vertrauensvollen und bewussten Umgang mit Informationen in österreichischen Unternehmen in den letzten drei Jahren deutlich gestiegen ist. (Österreichische Presseagentur 2020) hebt hervor, dass zwei Jahre nach Inkrafttreten der EU-Datenschutzgrundverordnung (EU-DSGVO) das Verständnis für das Thema Datenschutz in österreichischen Unternehmen deutlich gestiegen ist. In einer vor der Corona-Krise durchgeführten KSV1870-Umfrage im Rahmen des Österreichischen Wirtschaftschecks im Februar 2020 bei rund 600 Unternehmen gaben 40 % der befragten Unternehmen an, dass dieses in den letzten drei Jahren "auf breiter Front" gestiegen sei. Die Umfrage zeigt deutlich, dass es noch einiges zu tun gibt, bis die EU-DSGVO von allen Unternehmen in Österreich vollständig umgesetzt ist, denn nur 30 % der Befragten haben sie bisher vollständig in ihrem Betrieb verankert. (Österreichische Presseagentur 2020)

"So bestätigen 40 % der inländischen Unternehmen, dass diese Entwicklung "auf breiter Front" stattgefunden hat - weitere 32 % sehen zumindest in Teilbereichen eine Steigerung. Während für 19 % eine Verbesserung nicht erkennbar ist, hat sie sich für 2 % sogar verringert." 7 % der Befragten machten keine Angaben. (Österreichische Presseagentur , 2020) . Zwischen dem Verständnis und der tatsächlichen Umsetzung notwendiger Datenschutzmaßnahmen klafft oft eine erhebliche Lücke. Gerade in Zeiten zunehmender Digitalisierung durch die Corona-Krise ist es besonders besorgniserregend, dass nicht einmal ein Drittel der heimischen Unternehmen die EU-DSGVO vollständig umgesetzt haben", erklärt Ricardo-José Vybiral, MBA, CEO der KSV1870 Holding AG. Dazu gehört unter anderem das geforderte "Verzeichnis der Verarbeitungsvorgänge", das bisher nur 34% der befragten Unternehmen erfolgreich umgesetzt haben. (Österreichische Presseagentur 2020) Zwischen dem Verständnis und der tatsächlichen Umsetzung notwendiger Datenschutzmaßnahmen klafft oft eine

erhebliche Lücke. Gerade in Zeiten der zunehmenden Digitalisierung durch die Corona-Krise ist es besonders besorgniserregend, dass nicht einmal ein Drittel der heimischen Unternehmen die EU-DSGVO vollständig umgesetzt hat", erklärt Ricardo-José Vybiral, MBA, CEO der KSV1870 Holding AG. Dazu gehört unter anderem das geforderte "Verzeichnis der Verarbeitungsvorgänge", das bisher nur 34% der befragten Unternehmen erfolgreich umgesetzt haben (Österreichische Presseagentur 2020) .

Die Deloitte Services Wirtschaftsprüfungs GmbH (2020) hat auch eine Studie zum Umsetzungsgrad der GDPR in österreichischen Unternehmen Anfang 2020 veröffentlicht. 191 Unternehmensvertreter in Führungspositionen wurden in einer Online-Befragung befragt: "Das Ergebnis: Die Mehrheit der Unternehmen ist noch mit der Umsetzung der Anforderungen beschäftigt und sieht die langfristige Einhaltung als Herausforderung. Doch die Wichtigkeit des Themas ist inzwischen erkannt worden: Fast alle Befragten berücksichtigen die Datenschutzanforderungen inzwischen bei ihren Geschäftsentscheidungen." (Deloitte Services Wirtschaftsprüfungs GmbH(2020))

Ähnlich wie der KSV kommt auch Deloitte zu dem Schluss, dass der vollständige Umsetzungsstand der DSGVO in österreichischen Unternehmen bei knapp einem Drittel liegt: "Die Mehrheit der Unternehmen (54 %) befindet sich bei der Umsetzung der EU-DSGVO noch auf der Zielgeraden, wie schon vor einem Jahr. Während fast ein Drittel (32 %) der Befragten die Umsetzung der Richtlinie mittlerweile vollständig abgeschlossen hat, befinden sich rund 12 % noch mitten im Prozess und haben akuten Nachholbedarf." Deloitte stellt in dem Bericht fest, dass es keine Ausreden mehr für die Nichtumsetzung der Richtlinie geben darf. Den betroffenen Unternehmen wird dringend empfohlen, sich aktiv mit diesem Thema auseinanderzusetzen und gegebenenfalls externe Hilfe in Anspruch zu nehmen, um die Umsetzung zu beschleunigen.

Auf die Frage nach dem Stand der Umsetzung der Datenschutzgrundverordnung antworteten die Unternehmen wie folgt:

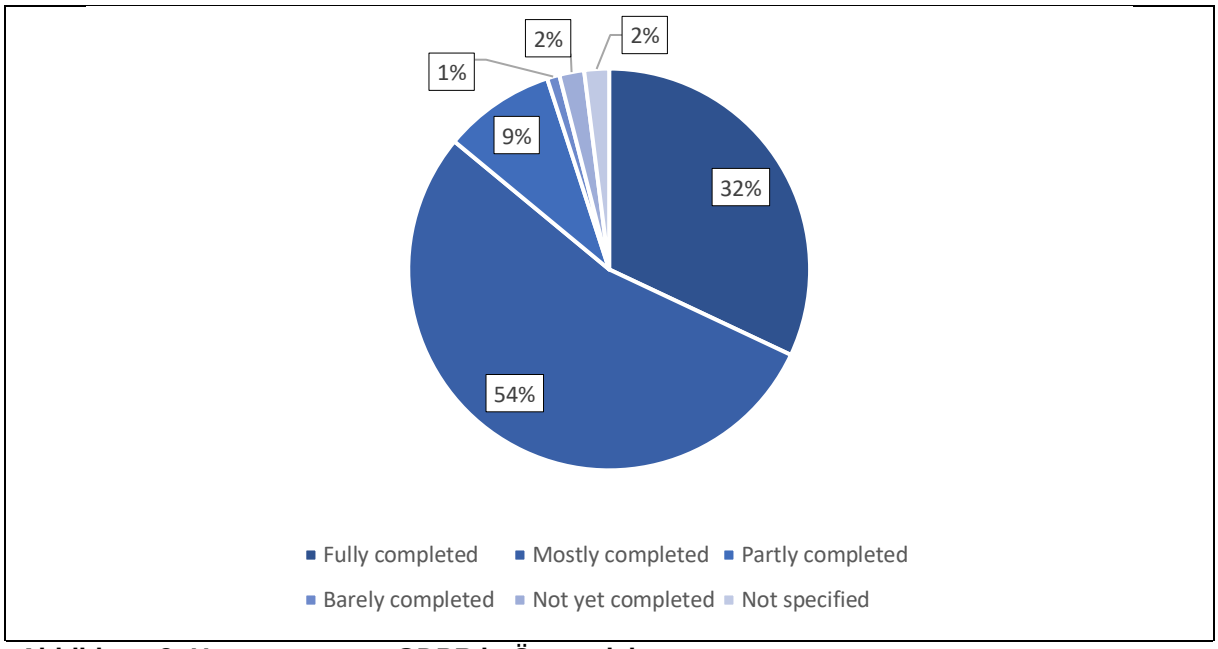

Abbildung 3: Umsetzung von GDPR in Österreich

Quelle: Eigene Darstellung. Verwendete Daten aus Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Wie in den Medien berichtet wurde, kam es im Jahr 2020 zu einem Anstieg der Bußgelder für die Nichteinhaltung von Datenschutzbestimmungen. Deloitte befragte daher die Unternehmen, wie diese Bescheide das Verhalten im Unternehmen beeinflussen: "Nur bei einem Viertel der Unternehmen haben die Entscheidungen der Datenschutzbehörde bisher einen Einfluss auf den Umgang mit der EU-DSGVO gehabt. Von diesen hat die Mehrheit die Erkenntnisse genutzt, um den Stand im eigenen Unternehmen zu bewerten oder zu verbessern." Die Frage wurde wie folgt formuliert: Haben die jüngsten Entscheidungen der österreichischen Datenschutzbehörde Ihren Umgang mit der EU-DSGVO beeinflusst?

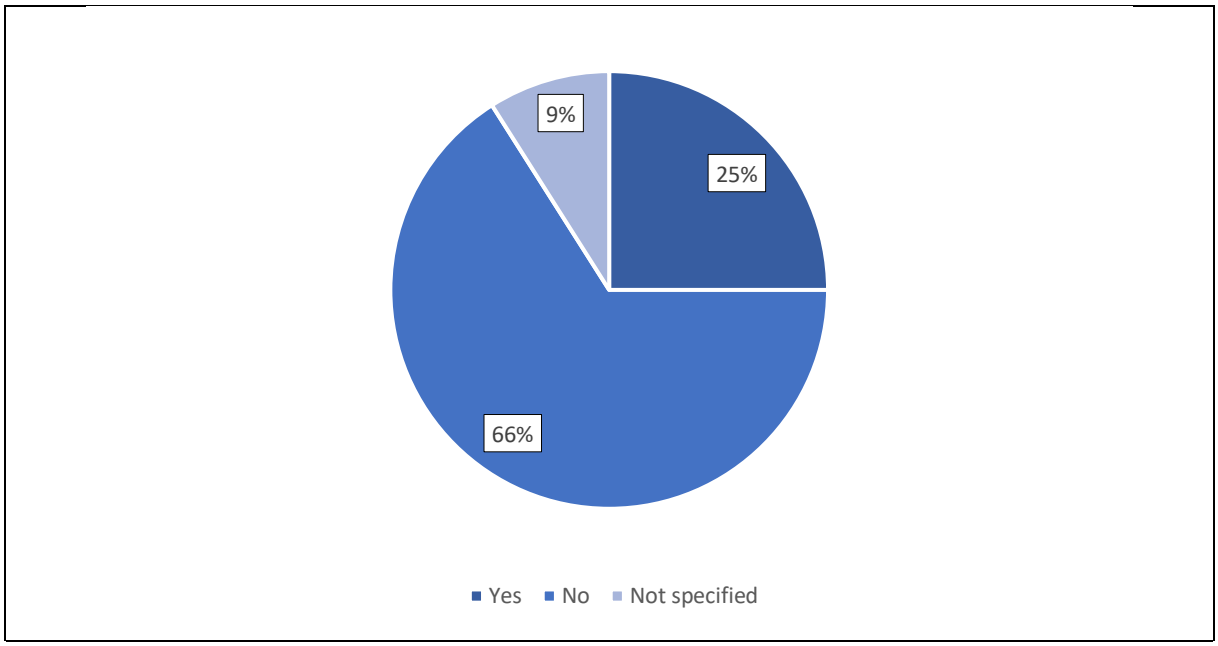

Abbildung 4: Einfluss der österreichischen Datenschutzbehörde auf den Umgang mit der EU-DSGVO

Quelle: Eigene Darstellung. Verwendete Daten aus Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Die Deloitte-Studie unterstreicht, dass viele Unternehmen in Österreich in den letzten Jahren leider ihre Hausaufgaben nicht gemacht haben. Oft fehlt es an einer strukturierten Datenklassifizierung, die den Aufwand deutlich reduzieren würde. Interessant ist die folgende Auswertung der nächsten Frage: Wie hoch schätzen Sie den Aufwand ein, um die Anforderungen der EU-DSGVO in Zukunft zu erfüllen?

Abbildung 5: Potenzieller Aufwand zur Erfüllung der Anforderungen der EU-DSGVO

Quelle: Eigene Darstellung. Verwendete Daten aus Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Der Bericht zeigt, dass die Mehrheit der Unternehmen die langfristige Einhaltung der Datenschutzgrundverordnung als Herausforderung empfindet. Den größten Aufwand sehen die Befragten in der Berücksichtigung von Löschfristen.

Eine weitere interessante Frage von Deloitte ist, ob es genügend geschulte Mitarbeiter*innen für Datenschutzaufgaben gibt: "Mehr als einem Viertel der befragten Unternehmen fehlen die personellen Ressourcen, um die EU-DSGVO einzuhalten und die damit verbundenen Arbeiten umzusetzen. Umso wichtiger ist andere Unterstützung: So greifen immer mehr österreichische Unternehmen auf technologische Unterstützung zurück, um die Anforderungen der EU-DSGVO erfüllen zu können. Während letztes Jahr noch 39% kein Tool hatten, sind es aktuell rund 30%."

Der Deloitte-Bericht kommt zu dem Schluss: "Nach anfänglichen Unsicherheiten haben die österreichischen Unternehmen ein deutlich klareres Bild über den bestehenden Handlungsbedarf. Einige der identifizierten Schlüsselthemen erfordern jedoch umfassende Veränderungen. Auch die Unternehmenskultur ist betroffen." (Deloitte Services Wirtschaftsprüfungs GmbH)

Aus Sicht von Hafelekar können wir die Situation in Österreich wie folgt zusammenfassen: Man kann sagen, dass es in Österreich klare Gesetze zum Thema Umsetzung der DSGVO gibt, auch wenn diese nicht immer leicht verständlich formuliert sind. Es gibt mehrere öffentliche Stellen, allen voran die WKO, an die sich Unternehmen zur Unterstützung bei der Umsetzung der DSGVO wenden können. In Österreich liegt die Haftung für jegliches Fehlverhalten in Bezug auf Datenschutz und IT-Sicherheit bei der Geschäftsführung, auch wenn diese Aufgaben an Mitarbeiter*innen delegiert. Die Umsetzung läuft noch immer nicht zufriedenstellend und wie wir bereits mit unserer Expertengruppe in Österreich festgestellt haben, ist wohl der Zeitmangel in KMUs ausschlaggebend für diese langsame Umsetzung. Laut unserer TeBeISi-Lenkungsgruppe gibt es in Österreich jedenfalls ein großes Interesse an leistbaren Weiterbildungen zu den Themen Datenschutz und IT-Sicherheit. Hier gibt es noch viel zu tun.

2.3 Deutschland

Name der Einrichtung	Kurzbeschreibung	Hauptzweck	Website
Deutsche Vereinigung für Datenschutz e.V. (DVD)	Die DVD ist für die Veröffentlichung von Meldungen zum Datenschutz (DANA) zuständig. Öffentlichkeits- und Medienarbeit zu aktuellen Themen, Pressekonferenzen und Pressemitteilungen gehören ebenfalls zu den Aufgaben. Außerdem werden Treffen in Zusammenarbeit mit Partnerorganisationen und Seminare durchgeführt. Die DVD beteiligt sich auch an der jährlichen Verleihung der Big Brother Awards.	Ziel der DVD ist es, die Öffentlichkeit über die Risiken der elektronischen Datenverarbeitung und die mögliche Einschränkung des Rechts auf informationelle Selbstbestimmung zu beraten und zu informieren.	https://www.datenschutzverein.de
Gesellschaft für Datenschutz und Datensicherheit (GDD)	Die GDD wurde 1977 gegründet und hat heute mehr als 3.800 Mitglieder. Bundesweit gibt es 34 Erfahrungsaustauschkreise mit mehr als 3.500 Teilnehmer*innen und mehr als 10.000 Datenschutzbeauftragte wurden bereits in der GDD-Akademie ausgebildet.	Datenschutz, Datensicherheit und ordnungsgemäße Datenverarbeitung sollen alle Beteiligten vor Gefahren schützen und gleichzeitig Informationsfreiheit und Informationsgleichgewicht gewährleisten. Die gesetzlichen Verpflichtungen betreffen alle Unternehmen und Verwaltungseinheiten, unabhängig von Größe und Branche. Die GDD will dazu einen wichtigen Beitrag leisten.	https://www.gdd.de/
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfG)	Am FIfG arbeiten rund 700 Personen aus Wissenschaft und Praxis, insbesondere Fachleute aus der Informatik und Informationstechnik. Ziel ist es, einen Austausch zwischen allen an der Informatik und Informationstechnik Beteiligten zu	Die FiFG warnt die Öffentlichkeit vor schädlichen Entwicklungen auf dem Gebiet der Informationssicherheit. Außerdem kämpft der Verein gegen den Einsatz von Informationstechnologie zur Kontrolle und Überwachung. Das FiFG setzt sich auch für die Gleichberechtigung von Menschen mit Behinderungen bei der Gestaltung und Nutzung der Informationstechnologie ein und	https://www.fiff.de

	ermöglichen. Das FiFG ist offen für alle, die mitmachen oder sich informieren wollen.	bekämpft die Diskriminierung von Frauen in der Informatik.	
Digitalcourage e.V.	Der Verein wurde 1987 gegründet. *Digitalcourage e.V.* setzt sich u.a. für Grundrechte und Datenschutz ein, leistet Aufklärungsarbeit durch Öffentlichkeitsarbeit, z.B. durch Kampagnen und Projekte, und ist verantwortlich für die jährliche Verleihung des BigBrotherAwards.	Ein großer Teil der Arbeit besteht in der Organisation von Projekten und Kampagnen, aber auch in der Organisation von politischen Kongressen. Außerdem steht der Verein der Presse und den Medien als Referent und Experte für Datenschutzfragen zur Verfügung. Das Hauptziel ist es, sich für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter einzusetzen.	https://digitalcourage.de/
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDi)	Die Hauptaufgaben der 1978 gegründeten Institution sind die Überwachung und Durchsetzung der DSGVO, des BDSG und anderer datenschutzrechtlicher Vorschriften. Außerdem geht es um Sensibilisierung und Öffentlichkeitsarbeit.	Hauptziel ist die Wahrung und Weiterentwicklung des Datenschutzes. Seit 2006 kann sich jeder, der sein Recht auf Informationszugang nach dem Informationsfreiheitsgesetz (IFG) verletzt sieht, an den Bundesbeauftragten wenden. Das Amt wird derzeit von Prof. Ulrich Kelber wahrgenommen.	https://www.bfdi.bund.de/

Tabelle 3: Interessenvertreter aus Deutschland.

Die Europäische Datenschutzgrundverordnung (DSGVO) ist am 24. Mai 2016 in Kraft getreten. Ab dem 25. Mai 2018 sind die darin enthaltenen Datenschutzanforderungen in den jeweiligen Mitgliedsstaaten auch ohne gesonderte Umsetzung in nationales Recht verbindlich. Die europäische Datenschutzverordnung soll vor allem die Rechte der Verbraucher stärken. Daten verarbeitende Unternehmen müssen mit strengeren Vorschriften rechnen. Die Nichteinhaltung der GDPR kann das betreffende Unternehmen bis zu 20 Millionen Euro an Bußgeldern oder bis zu 4 % seines weltweiten Umsatzes kosten (je nachdem, welcher Wert höher ist) (datenschutz 2021) . Der Stand der Umsetzung der Datenschutz-Grundverordnung durch die Unternehmen in Deutschland ist in Abbildung ***6***dargestellt. Die Statistik wurde im Herbst letzten Jahres veröffentlicht. Es handelt sich um die aktuellste verfügbare Studie über die Umsetzung der Datenschutz-Grundverordnung. Zum Zeitpunkt der Umfrage gaben 37% der Befragten an, dass sie die GDPR-Richtlinien bereits umgesetzt haben. Mehr als die Hälfte der Teilnehmer*innen gab an, dass die Richtlinie entweder teilweise oder vollständig umgesetzt und für die weitere Entwicklung festgelegt ist (Statista 2020) . Die europäische Datenschutzgrundverordnung (GDPR) trat am 24. Mai 2016 in Kraft. Ab dem 25. Mai 2018 sind die darin enthaltenen Datenschutzanforderungen in den jeweiligen Mitgliedsstaaten auch ohne gesonderte

Umsetzung in nationales Recht verbindlich. Die europäische Datenschutzverordnung soll vor allem die Rechte der Verbraucher stärken. Daten verarbeitende Unternehmen müssen mit strengeren Vorschriften rechnen. Die Nichteinhaltung der DSGVO kann das betreffende Unternehmen bis zu 20 Millionen Euro an Bußgeldern oder bis zu 4 % seines weltweiten Umsatzes kosten (je nachdem, welcher Wert höher ist) Datenschutz (2021) . Der Stand der Umsetzung der Datenschutz-Grundverordnung durch die Unternehmen in Deutschland ist in Abbildung ***6*** dargestellt. Die Statistik wurde im Herbst letzten Jahres veröffentlicht. Es handelt sich um die aktuellste verfügbare Studie über die Umsetzung der Datenschutz-Grundverordnung. Zum Zeitpunkt der Umfrage gaben 37% der Befragten an, dass sie die GDPR-Richtlinien bereits umgesetzt haben. Mehr als die Hälfte der Teilnehmer*innen gab an, dass die Richtlinie entweder teilweise oder vollständig umgesetzt und für die weitere Entwicklung festgelegt ist. Statista (2020) [1]

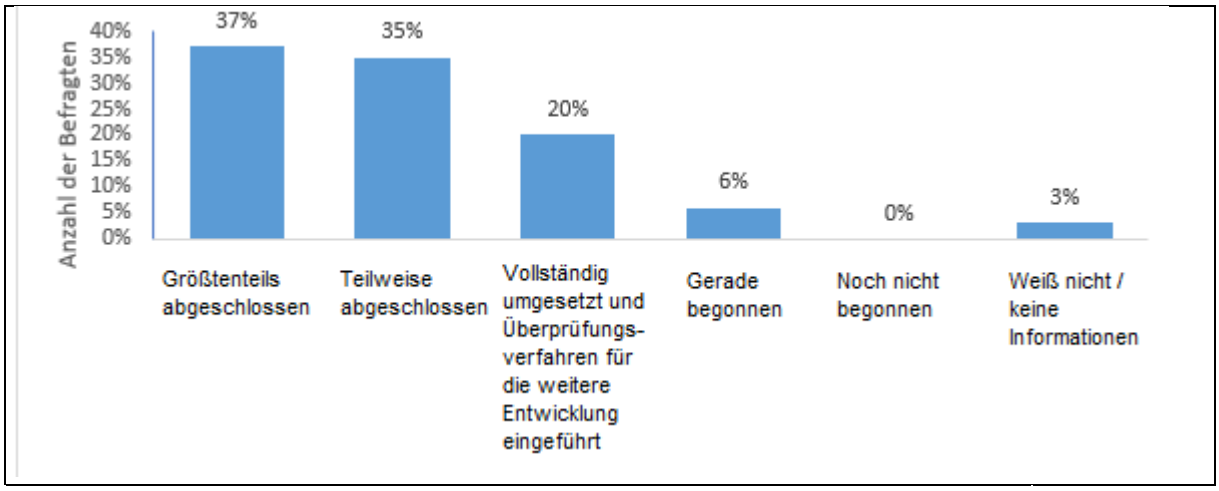

Abbildung 6: Stand der Umsetzung der DSGVO durch die Unternehmen in Deutschland (09/2020)

In Anbetracht der Tatsache, dass seit der Veröffentlichung rund 5 Jahre vergangen sind und seit dem Inkrafttreten 3 Jahre verstrichen sind, lässt sich ableiten, dass die Unternehmen an der vollständigen Umsetzung der Datenschutz-Grundverordnung gehindert werden. Die spezifischen Auswirkungen wurden in der von der Kommission durchgeführten Studie detailliert beschrieben Bitkom e.V. (2020) . Einer der Gründe, warum sich Unternehmen mit der Umsetzung schwertun, ist der hohe Aufwand, angefangen bei einem anfänglichen (und einmaligen) Mehraufwand (63 %), der Erwartung eines dauerhaften Mehraufwands (im Vergleich zum vorherigen Rechtsstand, 29 %) und dem Bedarf an zusätzlichem Personal (26 %). Der Personalbedarf spiegelt sich auch in der Entscheidung der Unternehmen wider, die Dienstleistung Datenschutz bei Dienstleistern einzukaufen, entweder in Form von externer Rechtsberatung (40 %), externer Datenschutzberatung (31 %) oder externer

[1] Weitere Informationen zur Studie: Erscheinungsdatum 09/2020, Deutschland, Erhebungszeitraum 09/2020, Anzahl der Befragten: 504 Unternehmen mit 20 und mehr Beschäftigten, telefonische Befragung.

Überprüfung (28 %). Nichtsdestotrotz wird die Datenschutz-Grundverordnung von der Mehrheit der Unternehmen als positiver Beitrag zum Betrieb und zur Leistung des Unternehmens wahrgenommen. In Anbetracht der Auswirkungen auf ein einheitliches Wettbewerbsumfeld in der EU (57 %).

Angesichts der komplexen regulatorischen Veränderungen lassen jedoch mehrere Aspekte Zweifel an den positiven Auswirkungen auf die Wirtschaftstätigkeit aufkommen. Unter anderem überwiegen die Bedenken hinsichtlich der langfristigen Verbesserung des rechtlichen Umfelds (43 %), der Behinderung von Innovationen (35 %) und der Komplizierung von Geschäftsprozessen (25 %). Die Risiken der Umsetzung der Datenschutz-Grundverordnung spiegeln sich auch in den Maßnahmen wider, denen die größte Dringlichkeit beigemessen wird, wie in Abbildung 7sehen ist.

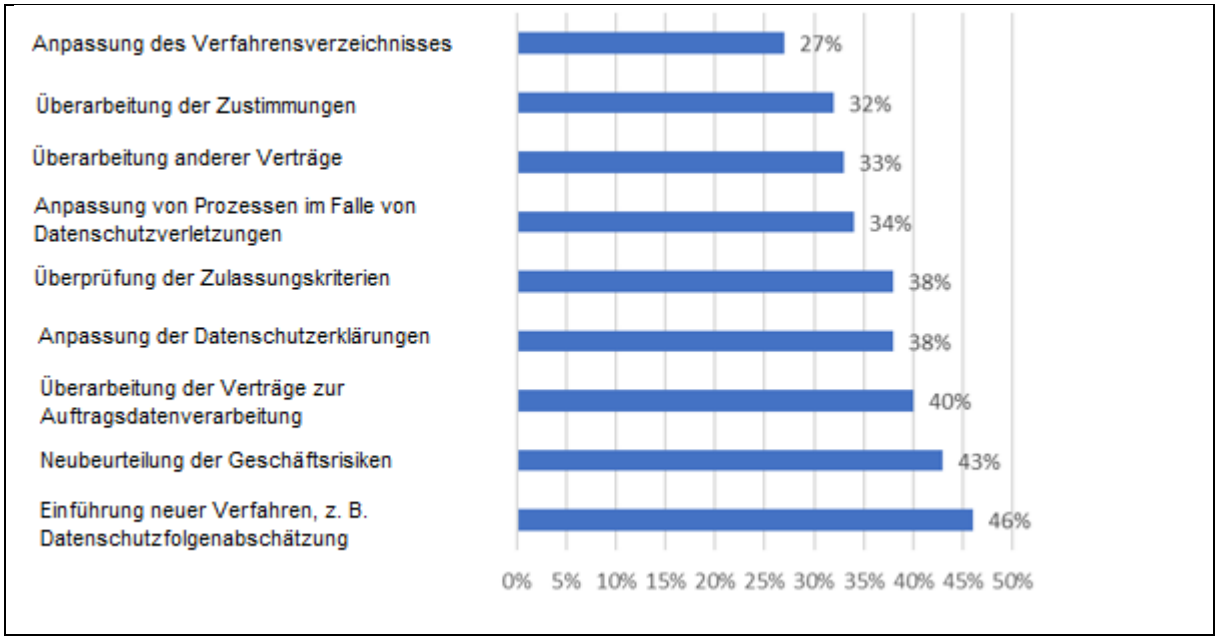

Abbildung 7: Welche Maßnahmen zur Umsetzung der DSGVO werden Sie mit hoher Dringlichkeit durchführen?
Quelle: Bitkom e.V. (2020)

Eine Studie aus dem Jahr 2021 unterstreicht die allgemein hohe Priorität des Datenschutzes in Deutschland, das damit unter allen europäischen Ländern an zweiter Stelle steht, was die allgemeine und angemessene Behandlung des Datenschutzes angeht (heyData 2021) . Von allen betrachteten Kategorien ist bemerkenswert, dass "Unternehmen" im Vergleich zu "Strafverfolgung", "Datenschutzkompetenz" und "öffentliche Meinung" am niedrigsten und "Privatpersonen" vergleichsweise am höchsten rangieren. Jede Kategorie lässt sich in mehrere Kriterien aufschlüsseln, die Aufschluss über spezifische Stärken und Schwächen geben. Betrachtet man die Situation der Unternehmen, wie in Abbildung 8sehen ist, wird deutlich, dass nur 17% der Unternehmen über eine obligatorische Weiterbildung verfügen, im Vergleich zu den 24,29% des EU-Durchschnitts. Ein zweites großes Manko im Vergleich zur

restlichen EU zeigt sich beim Versicherungsschutz, wo Deutschland um 4 Prozentpunkte schlechter abschneidet als der EU-Durchschnitt.

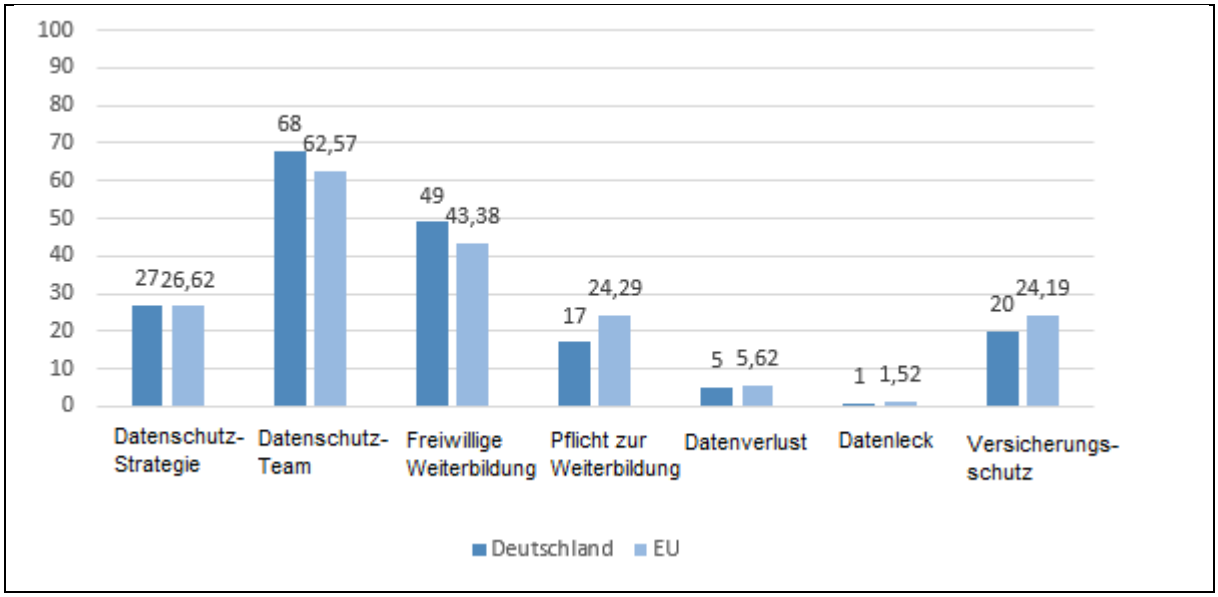

Abbildung 8: Zusammensetzung des Datenschutz-Scores für Deutschland und den EU-Durchschnitt in %-Wert

Quelle: heyData (2021) . Eigene Darstellung.

Verstöße gegen den Datenschutz werden in Deutschland streng geahndet. Mit rund 69 Mio. EUR an Bußgeldern im Jahr 2020 werden Datenschutzverstöße streng geahndet. Dieser Befund geht einher mit der Tatsache, dass in Deutschland die höchste Gesamtzahl an Datenschutzverstößen gemeldet wurde. Vor allem in Zeiten von Homeoffice im Rahmen der Pandemie ist die Zahl der Datenschutzverletzungen im Vergleich zum Vorjahr um rund 76 % gestiegen. Die Verzweigung dieses Ergebnisses wird wie folgt erklärt: "Im europäischen Vergleich verhalten sich die Unternehmen in Deutschland größtenteils sehr vorbildlich. Das ist aber auch notwendig. Die Strafverfolgung wird in Deutschland streng gehandhabt" (Milos Djurdjevic, CEO heyData, (Mai 2021)).

In Anbetracht dieser Daten ist es nicht verwunderlich, dass sich mehrere Verbände gegründet haben, die sich speziell mit der ordnungsgemäßen Umsetzung des Datenschutzes im öffentlichen und unternehmerischen Bereich befassen. Das "Recht auf informationelle Selbstbestimmung" (BVerfG 15.12.1983) und der Schutz der Persönlichkeitsrechte vor der zunehmenden Betonung von Sicherheitsinteressen ist elementarer Bestandteil der Arbeit dieser Verbände. Die Bedrohung des Datenschutzes und der Informationssicherheit wird daher nicht nur von kriminellen und feindlichen Akteuren, sondern auch von der Bundesregierung und ihren Sicherheitsinteressen wahrgenommen.

2.4 Italien

Name der Einrichtung	Kurzbeschreibung	Hauptzweck	Website
Apindustria Vicenza - Verband der KMU in Vicenza.	Rund 1.000 Mitglieder (die meisten von ihnen sind Kleinst-/Kleinunternehmen mit weniger als 20 Beschäftigten). Sie bieten folgende Dienstleistungen an: Kontakte zu lokalen und regionalen Behörden (Regionalabteilung, Kammern, Regionalpolitik); steuerliche und rechtliche Dienstleistungen für Mitglieder; Schulungen; spezifische Dienstleistungen (z. B. für Export, Netzwerk, Nachfolge, rechtliche Fragen, EU-Projekte, Zertifizierungen usw.). Kontaktperson: Herr Manuel Maraschin (Direktor; E-Mail: m.maraschin@apindustria.vi.it)	Einige Unternehmen (die mit Apindustria Vicenza verbunden sind) haben intern bereits einen IT- und DV-Manager. In diesem Fall könnten wir einen (Teil-)Zertifizierungsprozess mit diesen Manager*innen überprüfen und pilotieren, indem wir die Ausbildungswege anhand der IO3-Inhalte (Online-Fragebogen) überprüfen. Umgekehrt könnten wir mit externen Expert*innen (Beratern, IT-Anbietern, Anwälten usw.), die KMU unterstützen, prüfen, ob die Zertifizierung zu ihrer täglichen Arbeit passt. Apindustria Vicenza steht zur Verfügung, um einige Treffen mit lokalen KMUs zu organisieren und gleichzeitig den IT- und DV-Managern einige Interviews vorzuschlagen, die für das Projekt IOs nützlich sein könnten. Apindustria ist keine öffentliche Einrichtung, sondern eine Art "Zwischenorganisation", die auch lokale/regionale kollektive Interessen vertritt. Apindustria Vicenza nimmt als Berufsverband an einigen regionalen Arbeits- und Fachtischen teil. Bei diesen Treffen geht es auch um das Berufsprofil, die Definition spezifischer Kompetenzen, (Teil-)Zertifizierungsprozesse usw. Apindustria könnte also die Umsetzung dieses neuen Profils unterstützen, auch weil sie mehrere lokale KMU vertritt. Dank einiger ESF-Kurse (Europäischer Sozialfonds) konnte Apindustria am Ende des Projekts auch spezifische Ausbildungswege implementieren, die von unserem regionalen Ausbildungsbüro (teilweise) zertifiziert werden könnten. Zeitplan: Die neue EU-Planung für den Zeitraum 2021 - 2027 ist noch in der Diskussion. Derzeit finden mehrere technische Treffen auf regionaler Ebene statt (Hauptziel der Ausbildungsstrategie, neue Inhalte, Angleichung der Berufsprofile auf nationaler und europäischer Ebene, ESCO-Prioritäten usw.). Apindustria konnte aber auch die regionalen Behörden über Projektinhalte informieren. Dadurch konnten einige Projektergebnisse in neuen Programmen umgesetzt werden.	WWW. apindustria.vi.it
CPV -Centro Produttività Veneto	Es ist einer der größten Bildungsanbieter in der Region Venetien und verfügt über fast 70 Jahre Erfahrung. Das CPV bietet eine breite Palette von Schulungskursen für KMU, Arbeitnehmer, Manager, Berater*innen und Arbeitslose an. In den letzten 2/3 Jahren hat das CPV auch mehrere Schulungskurse zu Projektthemen organisiert. Kontaktperson: Herr Enrico Bressan, (Leiter der Ausbildungsabteilung und der EU-Projekte; E-Mail: bressan@cpv.org). Er ist auch ein externer Experte für die Agentur für	Herr Bressan verfügt über umfangreiche Erfahrungen (dank einiger regionaler, nationaler und transnationaler Projekte) mit der ESCO-Plattform, dem Ecvet-Rahmen, den EQR-Systemen usw. Er könnte das Projekt unterstützen und seine Erfahrungen austauschen. Darüber hinaus ist das CPV in der Lage, mehrere lokale Kleinunternehmen einzubeziehen. Als Bildungsanbieter hat das CPV ein starkes regionales Netzwerk im Bereich der beruflichen Bildung und der Erwachsenenbildung aufgebaut. Und es verfügt über eine große Anzahl von Expert*innen (z. B. Berater*innen und Ausbilder*innen), die eine Liste von Kompetenzen überprüfen und validieren können. Das CPV ist in der Lage, lokale Kleinunternehmen einzubeziehen, indem es zum Beispiel Interviews mit potenziellen Kandidaten und Treffen (Workshops) mit Unternehmen organisiert. Das CPV betreibt auch eine "Studiengruppe" (seit 1985), die sich auf IT, Informatik, Datenschutz, Digitalisierung usw. konzentriert. Die Zwischen- und Endergebnisse des Projekts könnten dort vorgestellt werden. Als "öffentliche/private" Institution sitzt das CPV in mehreren Fachgremien auf regionaler Ebene (z. B. im Expertenausschuss für die Anerkennung und Bewertung von Kompetenzen und Berufsprofilen). Es könnte unseren	www.cpv.org

	lebenslanges Lernen in Rom.	regionalen Anpassungsplan überprüfen und danach einige Lobbyarbeit bei unseren regionalen Behörden leisten.	
Cesar srl	Es ist das Schulungszentrum in Vicenza für den örtlichen Handwerksverband (dem mehr als 20.000 Kleinst- und Kleinunternehmen angehören). Es bietet eine breite Palette von Schulungsdienstleistungen an, darunter Kurse in IT-Sicherheit, Datenschutz, GDPR usw. Ansprechpartnerin: Frau Daniela Bucci, (stellvertretende Leiterin der Schulungsabteilung; E-Mail: d.bucci@confartigianatovicenza.it).	Cesar arbeitet nur mit Kleinst- und Kleinunternehmen (unter 10 Mitarbeiter*innen). Normalerweise verfügen diese Unternehmen nicht über einen internen Experten wie einen IT-Sicherheits- und Datenschutzbeauftragten. Dank der (finanzierten oder nicht finanzierten) Schulungen ist Cesar in der Lage, den (Teil-)Zertifizierungsprozess zu unterstützen. Cesar könnte in mehreren Phasen involviert sein, wie z.B.: Einbeziehung von Kleinunternehmen; Bedarfsanalyse; Definition von Schlüsselkompetenzen; Pilotierung und Schulung. In Zukunft könnten sie den lokalen Unternehmen auch TEBEISI-zertifizierte Kurse mit allen Projektergebnissen anbieten. Cesar ist Teil des regionalen Netzwerks von Ausbildungszentren für Kleinst- und Kleinunternehmen, das sich aus 7 Provinzen zusammensetzt (insgesamt 75.000 Mitglieder). Cesar ist sehr häufig an verschiedenen regionalen Fachtischen und Arbeitsgruppen für Berufsprofile und Zertifizierungsverfahren beteiligt. Er könnte unsere regionale Behörde über Projektziele und -ergebnisse, vor allem für Kleinstunternehmen, informieren.	www.confartigianatovicenza.it
Handels-kammer von Vicenza	Es handelt sich um eine öffentliche Einrichtung in Italien, die einen obligatorischen Dienst für alle Unternehmen anbietet. Zum Beispiel muss jedes lokale Unternehmen in der lokalen Datenbank registriert sein (für alle Geschäftsphasen, von der Gründung bis zur Schließung). Die Kammer von Vicenza vertritt über 90.000 Unternehmen, von denen die meisten Kleinst- oder Kleinunternehmen sind. Kontaktperson: Herr Diego Rebesco (Leiter der Abteilung für Statistik und Werbung; E-Mail: diego.rebesco@vi.camcom.it).	Die Kammer bietet eine breite Palette von Dienstleistungen an, die mehr oder weniger alle Bedürfnisse der Unternehmen abdecken (Verwaltungsaufgaben, Ausbildung, Export, Zertifizierungen, Patente, usw.). Die Kammer ist auch auf dem Gebiet der Anerkennung von Berufsprofilen aktiv, zum Beispiel durch das Bildungs- und Arbeitsministerium in Rom. Sie führt auch Praktika für junge Menschen (von den Gymnasien) durch, die kurze Erfahrungen in einem Unternehmen machen, durch einige zertifizierte Praktika, die am Ende bewertet werden. Sie könnte nicht nur in die Projektförderung und -verbreitung (z. B. Newsletter oder lokaler Workshop), sondern auch in den Zertifizierungsprozess einbezogen werden, dank der Verbindung zu unserem nationalen Ministerium. Zumindest könnte sie über den Projektfortschritt informiert werden. Es könnte aber auch eine lokale Arbeitsgruppe (Provinz Vicenza) einrichten. Dieses Gremium könnte am Ende des Projekts die endgültige (Teil-)Zertifizierung von TEBEISI unserer regionalen Behörde zur vollständigen Anerkennung vorlegen. Es könnte unsere öffentliche Einrichtung sein, die den gesamten regionalen Anpassungsplan als Teil seiner Funktionalität und seines Ziels verifiziert und zertifiziert. Im Einzelnen könnte sie den Zeitplan, die Rollen der einzelnen Teilnehmer*innen und vor allem die Hauptinhalte des Plans überprüfen, auch im Hinblick auf künftige spezifische Gesetze zum Projektthema oder spezifische Anforderungen, die in regionale Schulungsprogramme aufgenommen werden könnten.	www.vi.camcom.it
Proservizi srl	Es ist das regionale Schulungszentrum der ConfProfessioni Veneto (die mehr als 45.000 Mitglieder wie Rechtsanwält*innen, Steuerexpert*innen, Notar*innen, Berater*innen usw. hat). Es bietet eine breite Palette von Schulungsdienstleistungen an, darunter Kurse in IT-Sicherheit, Datenschutz, GDPR usw. Ansprechpartnerin: Frau Greta Cosentino, (Leiterin	Proservii hat als Klienten*innen nur Berater*innen (nicht Unternehmen). So sind sie in der Lage, eine große Anzahl von Anwälten einzubeziehen, die auf IT-Sicherheit und Datenschutzrecht spezialisiert sind. Darüber hinaus bieten sie häufig Schulungen (Grund- und Aufbaukurse) zu GPPR und Datenschutzgesetz an. Auf diese Weise sind sie in der Lage, die Projektpfade (z. B. in Bezug auf die Liste der spezifischen Kompetenzen) und die Anforderungen des Marktes (der Unternehmen) zu überprüfen und zu vergleichen. Proservizi hat sich bereits an Projektaktivitäten beteiligt. Zum Beispiel haben einige Mitglieder (z.B. Juristen) Projektinterviews durchgeführt. Sie bieten auch finanzierte Ausbildungskurse an (dank des ESF - Europäischer Sozialfonds - und/oder spezieller Zuschüsse aus ihrem Ausbildungssystem, dem "Fondo ConfProfessioni"). So sind sie in der Lage, den TEBEISI-Profilkurs in der nächsten Zukunft zu finanzieren.	www.proservizi.it

	der Schulungsabteilung; E-Mail: greta.cosentino@proservizi.it).	Proservizi könnte vor allem die Pilotphasen unterstützen, in denen z.B. einige lokale Anwälte mit einigen kleinen Unternehmen (ihren Klient*innen) zusammenarbeiten, um die Projektinhalte zu überprüfen. Aber auch, um neue Kompetenzen im Bereich der IT-Sicherheit und des Datenschutzmanagers zu erwerben. Sie könnten auch einen speziellen Ausbildungsweg für die Mitglieder organisieren, der alle TEBEISI-Ergebnisse und -Resultate beinhaltet. Proservi ist sehr häufig an verschiedenen regionalen Arbeitsgruppen beteiligt, die sich mit dem Ausbildungsbedarf und der Anerkennung von Qualifikationen befassen. So könnte Proservi unserer regionalen Ausbildungsbehörde zum Beispiel neue Inputs für das nächste ESF-Programm vorschlagen (das den Zeitraum 2021 - 2027 abdeckt).	
SATEF srl	Es ist das regionale Schulungszentrum. Es bietet eine breite Palette von Schulungsdienstleistungen an, darunter Kurse in IT-Sicherheit, Datenschutz, GDPR usw. Es ist auch auf den Gesundheits- und Sicherheitssektor spezialisiert, einschließlich Altenpflegezentren. Kontaktperson: Herr Paolo Pedron, (Gründer und Leiter der Schulungsabteilung; E-Mail: pedron@satef.com).	Herr Pedron, der Direktor, ist ein ESCCO / Ecvet Experte auf regionaler und nationaler Ebene. Er hat eine spezielle Schulungsplattform für die Anerkennung von Kompetenzen und die (Teil-)Zertifizierung eingerichtet. Zurzeit betreibt er sie in zwei Sektoren: Gesundheit und Sicherheit sowie Tourismus. Wir könnten also unsere Projektinhalte in seiner Plattform testen und erproben. An diesem Test könnten auch kleine Unternehmen und einige Berater*innen/Expert*innen beteiligt sein. Satef könnte die Projektinhalte z. B. im Bereich Tourismus testen. Dank früherer Erfahrungen existiert die Plattform bereits, auch in Bezug auf den Ausbildungsweg. So könnten die TEBEISI-Ausbildungsinhalte getestet werden, aber auch ein (Teil-)Zertifizierungsprozess könnte durchgeführt werden, auch auf regionaler Ebene. Herr Pedron nimmt an einigen regionalen Arbeitsgruppen zum Thema "Zertifizierung und Bewertung von Berufsprofilen" teil. So kann er unsere Umsetzungsphase stark unterstützen. Aufgrund seiner Rolle auf regionaler Ebene ist Pedron in der Lage, die Projektinhalte und -ergebnisse (einschließlich der Testphasen) bei unserer Behörde bekannt zu machen. Er konnte auch informell unseren "regionalen Anpassungsplan" bewerten, kurz bevor er ihn (zur abschließenden Diskussion) an unsere regionale Abteilung für Ausbildung und Arbeit in Venedig schickte.	www.satef.com
ENGIM Venetien	Es ist der größte Bildungsanbieter in der Region Venetien und verfügt über fast 90 Jahre Erfahrung. ENGIM bietet eine breite Palette von Schulungskursen für KMU, Arbeitnehmer*innen, Manager*innen, Berater*innen und Arbeitslose an. In den letzten 2/3 Jahren wurden auch mehrere Schulungen zu den Projektthemen organisiert. Kontaktperson: Herr Manuel Fochesato, (Leiter der Ausbildungsabteilung und der EU-Projekte; E-Mail: manuel.fochesato@engimvi.it).	Herr Fochesato verfügt über umfangreiche Erfahrungen (dank einiger regionaler, nationaler und transnationaler Projekte) mit der ESCO-Plattform, dem Ecvet-Rahmen, den EQR-Systemen usw. Er könnte das Projekt unterstützen und seine Erfahrungen austauschen. Darüber hinaus ist ENGIM in der Lage, mehrere lokale Kleinunternehmen, aber auch Berater, Ausbilder und Experten einzubeziehen. Engim fungiert auch als Berufsbildungseinrichtung; ein Teil der Ausbildungskurse richtet sich daher an Jugendliche, Erwachsene, die eine zusätzliche Ausbildung benötigen, und vor allem an Arbeitslose. Engim betreibt (und plante) bereits mehrere Schulungsplattformen, die nicht nur Schulungsmaterialien (d.h. Online-Kurse für eine breite Palette von Bildungsbedürfnissen), sondern auch IT-Systeme umfassen, die zum Teil bestimmte Kompetenzen erkennen. Engim kann die Implementierung von Berufsprofilen auf verschiedene Weise unterstützen: Endnutzer (kleine Unternehmen und/oder Berater*innen/Expert*innen) finden; Auszubildende (Jugendliche und/oder Erwachsene) einbeziehen, die nach einer neuen beruflichen Spezialisierung suchen, und nicht zuletzt mit lokalen (regionalen) Ausbildungsbehörden diskutieren und austauschen. Aufgrund der Rolle und Erfahrung von Fochesato auf regionaler Ebene ist er in der Lage, die Projektinhalte und -ergebnisse (einschließlich der Testphasen) bei unserer Behörde bekannt zu machen. Engim könnte auch den regionalen Anpassungsplan an verschiedene öffentliche Akteure weitergeben. Es könnte	www.engimvi.it

		aber auch neue Inhalte in seine Online-Schulungsplattformen einbringen, einschließlich der TEBEISI-Inhalte.	
Veneto lavoro	Sie ist die öffentliche regionale Agentur, die alle den Arbeitsmarkt betreffenden Inhalte verwaltet (Kurse, Zertifizierungen, lokale Arbeitszentren für Arbeitslose usw.). Kontaktperson: Herr Mirco Casteller, (verantwortlich für die Sozialabteilung und EU-Projekte; E-Mail: mirco.casteller@venetolavoro.it).	Die Region Venetien betreibt über Veneto Lavoro die "Abteilung für Arbeit und Ausbildung", d. h. die öffentliche Behörde, die alle Mittel (z. B. ESF - Europäischer Sozialfonds) für Arbeitnehmer, Unternehmen, Manager und Berater/Ausbilder verwaltet. Veneto Lavoro betreibt auch das "RRSP - Repertorio Regionale Standard Professionali" (die regionale Datenbank/Repertorium für berufliche Standards und Qualifikationen). Als öffentliche Einrichtung ist Veneto Lavoro der wichtigste Stakeholder auf regionaler Ebene, vor allem weil sie das RRSP betreibt. Und Herr Casteller ist unser Hauptansprechpartner für diesen strategischen Austausch und die Diskussion. Veneto Lavoro spielt eine entscheidende Rolle bei der Umsetzung des TEBEISI-Profils/der TEBEISI-Profile, vor allem in den letzten Projektphasen (wo der italienische Partner einige Leitlinien und Empfehlungen verbreiten sollte). Als unabhängiges und öffentliches Büro kann Veneto Lavoro nicht direkt in den Prozess involviert sein, aber es könnte als "öffentlicher Berater" agieren. Veneto Lavoro kann unseren "regionalen Anpassungsplan" Schritt für Schritt validieren. Das bedeutet, dass wir Veneto Lavoro von Anfang an über die Projektfortschritte informieren könnten und am Ende dieses neue Berufsprofil vorschlagen könnten, das als (Teil-)Zertifikat in die regionale Datenbank für Berufsstandards (RRSP) aufgenommen werden könnte.	www.venetolavoro.it
INAPP – Arbeits-ministerium	Es ist die neue Agentur auf nationaler Ebene, die alle nationalen (und europäischen) Projekte im Zusammenhang mit der Kompetenzbewertung und -zertifizierung leitet und kontrolliert. Kontakte: urp@inapp.org (oder einige spezifische Abteilungen, wie atlante_lq@inapp.org)	Wie der zuvor erwähnte Stakeholder (Veneto Lavoro) könnte INAPP unser Projekt durch Austausch und Vorschläge für den gesamten Zertifizierungsprozess stark unterstützen. Insbesondere betreibt INAPP den neuen "Atlante del lavoro e delle qualificazioni" (Atlas der Berufe und Qualifikationen). Der Atlas ist die allgemeine (nationale) Datenbank / Repertorium für die beruflichen Standards und Qualifikationen. Er enthält auch Profile für Studenten (Gymnasien und Universitäten) und Leitlinien für Berufsbildungseinrichtungen und Ausbildungszentren. Kürzlich hat INAPP auch den "Atlas für Fachleute" (wie Berater*in, Ausbilder, Anwälte usw.) eingeführt und sie konnten den Projektfortschritt in Bezug auf die neuen Profile von "TEBEISI IT-Security und DP-Managern" überprüfen. Und mittelfristig auch dieses neue Profil einführen und fördern. INAPP könnte auch die Projektinhalte im Hinblick auf zukünftige ESF - Europäische Sozialfonds - neue Trainingskurse (Programm: 2021 _ 2027) basierend auf TEBEISI Ergebnissen überprüfen. INAPP könnte über den Fortschritt auf regionaler Ebene informiert werden. Und prüfen, ob die Kohärenz und die Nachhaltigkeit des Projekts mittelfristig gewährleistet sind, indem es einige Rückmeldungen/Vorschläge gibt. Außerdem könnte es die Schulungsmaterialien bewerten, vor allem den Prozess der (Teil-)Kompetenzzertifizierung, zumindest auf nationaler Ebene. Das NAPP unterhält Dutzende von Arbeitsgruppen auf nationaler Ebene. Oftmals sind diese Gruppen auch auf regionaler Ebene tätig. Wir könnten uns also mit einigen Gruppenmitgliedern treffen und mit ihnen diskutieren und ihnen einen regionalen Anpassungsplan vorschlagen, bevor das Projekt abgeschlossen wird.	www.inapp.org
AIPSI	Associazione italiana dei professionisti sicurezza informatica (der italienische Verband für IT-Sicherheitsfachleute und -experten). Sie ist die italienische Sektion der IVSS, einer internationalen	AIPSI ist einer der wichtigsten italienischen Verbände für IT-Sicherheitsexpert*innen. Er arbeitet aber auch mit Datenschutzbeauftragten zusammen. Sie bietet eine breite Palette von Dienstleistungen an, die für das TEBEISI-Projekt nützlich sind, wie z.B.: Umfragen und Untersuchungen, Berichte, Schulungen und Beratung und natürlich (Teil-) Bewertungs- und Zertifizierungsaktivitäten für die Berufsprofile. Die meisten ihrer Kurse (kostenlos oder gegen	www.aipsi.org

	Non-Profit-Organisation von Fachleuten und erfahrenen Praktikern. Durch die aktive Beteiligung einzelner Mitglieder und ihrer Sektionen auf der ganzen Welt ist die AIPSI als Sektion der IVSS Teil der größten gemeinnützigen Vereinigung von Sicherheitsexpert*innen mit über 13.000 Mitgliedern weltweit. Kontaktperson: Frau Yvette Agostini (Direktorin, info@aipsi.org)	Bezahlung) wurden bereits von einer nationalen oder regionalen Einrichtung zertifiziert. Es ist auch Teil eines größeren internationalen Netzwerks und könnte uns daher eine größere Vision und weitere Informationen liefern. AIPSI könnte die Projektinhalte und Bewertungsphasen überprüfen. Insbesondere könnten sie einige neue Schulungsmaterialien akzeptieren und überprüfen, zum Beispiel einige spezifische Kompetenzen (wie Soft Skills oder persönliche Fähigkeiten). AIPSI hat mehrere Mitglieder, die auch aus der Region Venetien kommen (es gibt auch ein lokales Büro in Venedig; die meisten der lokalen Mitglieder sind Informatikingenieure). Mit ihnen könnten wir einige Inhalte austauschen und vor allem die Endfassungen überprüfen. Außerdem könnte unser Projekt Clusit-Mitglieder (die Fachleute sind) mit KMUs verbinden. AIPSI nimmt bereits an mehreren technischen Arbeitsgruppen auf nationaler Ebene (insbesondere im Ministerium für Innovation und Bildung) und an mehreren regionalen Task Forces teil. Insbesondere ihre Berichte und Veröffentlichungen bilden die wissenschaftliche Grundlage für weitere gesetzliche Verbesserungen im Bereich der Anerkennung von (neuen) Berufsbildern. Für unsere Region könnte der lokale AIPSI Präsident oder Direktor die wissenschaftlichen und technischen Experten vertreten.	
CLUSIT	Associazione Italiana per la sicurezza informatica (der italienische Verband für IT-Sicherheit). CLUSIT Italien wurde auf der Grundlage der Erfahrungen anderer europäischer Verbände für Computersicherheit wie CLUSIB (Belgien), CLUSIF (Frankreich), CLUSIS (Schweiz) und CLUSIL (Luxemburg) gegründet, die in ihren jeweiligen Ländern seit mehr als 20 Jahren ein Bezugspunkt für die Computersicherheit sind. Hauptziel: Verbreitung der Kultur der Informationssicherheit in Unternehmen, öffentlichen Verwaltungen und bei den Bürgern. Kontaktperson: Herr Gabriele Faggioli (der Präsident; president@clusit.it)	Clusit ist einer der wichtigsten italienischen Verbände für IT-Sicherheitsexpert*innen. Er arbeitet aber auch mit Datenschutzbeauftragten zusammen. Clusit bietet eine breite Palette von Dienstleistungen an, die für das TEBEISI-Projekt nützlich sind, wie z.B.: Umfragen und Untersuchungen, Berichte, Schulungen und Beratung und natürlich (teilweise) Bewertungs- und Zertifizierungsaktivitäten für die Berufsprofile. Die meisten ihrer Kurse (kostenlos oder gegen Bezahlung) wurden bereits von einer nationalen oder regionalen Einrichtung zertifiziert. Clusit konnte die Projektinhalte und Bewertungsphasen überprüfen. Insbesondere könnte Clusit einige neue Schulungsmaterialien akzeptieren und überprüfen, zum Beispiel einige spezifische Kompetenzen (wie Soft Skills oder persönliche Fähigkeiten). Clusit hat mehrere Mitglieder, die ebenfalls aus der Region Venetien kommen (die meisten von ihnen sind Informatikingenieure). Mit ihnen könnten wir einige Inhalte austauschen und vor allem die Endversionen überprüfen. Außerdem könnte unser Projekt Clusit-Mitglieder (die Fachleute sind) mit KMU verbinden. Clusit beteiligt sich bereits an mehreren technischen Arbeitsgruppen auf nationaler Ebene (insbesondere im Ministerium für Innovation und Bildung) und an mehreren regionalen Task Forces. Insbesondere ihre Berichte und Veröffentlichungen bilden die wissenschaftliche Grundlage für weitere gesetzliche Verbesserungen im Bereich der Anerkennung von (neuen) Berufsprofilen.	www.clusit.it
Universität Padua - Fachbereich Informatik und Computer-technik".	In den letzten Jahren haben sie mehrere Umfragen zu Projektthemen durchgeführt: Prof. Antonio Scipioni (scipioni@unipd.it).	Die Universität Padua organisiert bereits Masterstudiengänge der zweiten Ebene zu Projektthemen (Datenschutzbeauftragter, IT-Sicherheitsexperte usw.) und auch Fortbildungskurse. Ihre Ausbildungsinhalte und -wege könnten für die Auswahl von Bewerbern und Stellenprofilen nützlich sein. Sie könnten Manager*innen, Expert*innen und KMU's einbeziehen, z. B. für die Durchführung von Inteviews, Workshops usw. Als Universität könnten sie einen wissenschaftlichen Ansatz und die richtigen Methoden "garantieren". Als Athenaeum könnten sie auch mehrere Fachbereiche (Wirtschaft, Recht, IT - Informatik, Management, usw.) einbeziehen. Die Universität ist eine öffentliche Einrichtung, die an mehreren regionalen Lenkungsausschüssen und Arbeitsgruppen beteiligt ist, darunter auch Expertengruppen zu Projektthemen. Wenn sie	www.unipd.it

		also über den Projektfortschritt informiert ist, könnte sie den Zertifizierungsprozess auf regionaler Ebene unterstützen.	
APCO - Italienischer Verband der Unterneh-mensberater	Er ist der italienische Verband für Unternehmensberater, der 1968 gegründet wurde und heute über 400 Mitglieder hat. APCO bietet verschiedene Dienstleistungen für Mitglieder an, wie z.B.: Schulungen, Netzwerkinitiativen, Lobbyarbeit bei Institutionen, etc. Kontaktperson: Frau Cesara Pasini (Präsidentin; E-Mail: presidenza@apcoitalia.it)	APCO hat mehrere "Communities of Practice", die sich auf verschiedene Themen konzentrieren. Insbesondere zwei von ihnen (digitale Transformation / Innovationsmanager und Compliance / ISO-Normen) könnten uns bei der Teilzertifizierung helfen. APCO förderte ein spezielles nationales Gesetz (Nr. 4, Jahr 2013), das auch Berater anerkennt, die nicht in einem Berufsverband (durch das Gesetz) registriert sind; aber sie müssen einen Zertifizierungsprofessor und eine kontinuierliche Ausbildung haben. APCO ist in der Lage, einige Treffen (auch online) mit einigen Mitgliedern zu organisieren, die an Projektthemen arbeiten. APCO ist keine öffentliche Einrichtung, sondern eine Art "Zwischenorganisation", die auch lokale/regionale kollektive Interessen vertritt. Zum Beispiel gibt es die "Nordost"-Delegation (Venetien, Trentino-Südtirol und Friaul-Julisch-Venetien), die in einige Projektaktivitäten einbezogen werden könnte. Die lokale Delegation (Region Venetien, Herr Paolo Ferrarese als Koordinator) könnte Lobbyarbeit bei unseren lokalen Behörden (Region, Abteilung Arbeit und Ausbildung) leisten.	www.apcoitalia.it

Tabelle 4: Stakeholder aus Italien

Die Datenschutz-Grundverordnung (DSGVO) ist in Italien schon seit einiger Zeit offiziell anwendbar, genauer gesagt seit dem 25. Mai 2018. Am 19. September 2018 trat dann der Text zur Anpassung der italienischen Gesetzgebung an die Datenschutz-Grundverordnung, nämlich das Dekret 101/2018, in Kraft.

Italienische Datenschutzverordnung: Wo stehen wir nach drei Jahren?

Im Juni 2021 hat das "Büro der Datenschutzaufsichtsbehörde" einen Bericht über seine Aktivitäten in den drei Jahren der Durchsetzung der Verordnung veröffentlicht, und es hat sich gezeigt, dass das Bewusstsein der betroffenen Personen in Bezug auf ihre Rechte mit etwa 27.192 Beschwerden und Berichten über Verstöße an die Garante gestiegen ist. (GDPD 2020) Die hohe Zahl der Meldungen, etwa 24 pro Tag, 365 Tage im Jahr über drei Jahre, zeigt, dass die Verabschiedung der Datenschutz-Grundverordnung das Bewusstsein der betroffenen Personen in Bezug auf ihre Rechte und die Forderung nach ihrem Schutz sicherlich geschärft hat.

Die Zahl der Meldungen stieg im Quartal zwischen dem 1. Januar und dem 31. März 2021 auf 2839, ein Zeichen dafür, dass das Pandemiejahr mit der Digitalisierung vieler Tätigkeiten auch zu einer größeren Aufmerksamkeit der Nutzer*innen für den Schutz personenbezogener Daten geführt hat.

Ebenso gab es 3.873 Meldungen über Datenschutzverletzungen (ca. 3,5 pro Tag), was im Vergleich zu den Statistiken über Cyberangriffe wenig ist, aber dennoch zeigt, wie wichtig es ist, Sicherheitsmaßnahmen und -instrumente zur Vorbeugung zu ergreifen. Ein grundlegender Aspekt ist in jedem Fall die Schulung und Sensibilisierung des Personals für das Thema Sicherheit und für das Verhalten bei Anfragen, die nicht den Unternehmensverfahren entsprechen.

Es wurden die Namen von 59.838 Datenschutzbeauftragten (auch DSB genannt) mitgeteilt, und nicht alle davon von öffentlichen Verwaltungen, die nach der Verordnung verpflichtet sind, einen DSB zu bestellen. Dies zeigt, dass die Notwendigkeit einer Koordinierungs-, Überwachungs- und Kontaktperson zwischen der Aufsichtsbehörde, den betroffenen Personen und dem für die Verarbeitung Verantwortlichen als wichtige Anforderung angesehen wird.

Was die Sanktionen betrifft, so wurden in Europa 654 Verfahren mit einem Gesamtbetrag von 283.757.083 Euro durchgeführt (Quelle). Betrachtet man die nach Ländern gegliederte Statistik, so steht Italien an erster Stelle, was den Gesamtbetrag der verhängten Sanktionen in Höhe von 76.298.601 Euro bei 79 Maßnahmen angeht, was die Tätigkeit der italienischen Garante und die Aufmerksamkeit bestätigt, mit der Beschwerden und Meldungen bearbeitet werden. Diese Zahl berücksichtigt natürlich nur Sanktionen, die gemäß Artikel 83 DSGVO verhängt wurden, und berücksichtigt keine Schadensersatz- oder Entschädigungszahlungen an betroffene Personen, deren Rechte verletzt wurden. Wie die Mitglieder der Aufsichtsbehörde anlässlich des Jahrestages der EU-Verordnung feststellten, ist es noch ein weiter Weg, um die Digitalisierung der Mitgliedstaaten mit einem sicheren Infrastrukturmanagement zu verbinden. Die Zunahme der Anfälligkeit von Unternehmen aufgrund der mehr oder weniger erzwungenen Einführung von Fernarbeitslösungen erfordert von den Eigentümern ein Überdenken der Datenflüsse und der Sicherheitsverfahren innerhalb ihrer Organisationen.

Aber was bedeutet das für die Unternehmen in unserem Land? Erfreulicherweise scheint der Trend positiv zu sein. Fast zwei Jahre nach der vollständigen Anwendung der Verordnung werden in Italien erhebliche Fortschritte bei der Einhaltung der Verordnung erzielt, wobei die den Organisationen zur Verfügung stehenden Haushaltsmittel aufgestockt werden und der Reifegrad in Bezug auf die Konkretheit der Projekte und die gezielten organisatorischen Veränderungen zunimmt.

Die Komplexität und die Bedeutung des Themas erfordern jedoch ständige Anstrengungen der Unternehmen, um sich an die Grundsätze der Datenschutzvorschriften anzupassen und auf die Anfragen der Behörden zu reagieren. In diesem Zusammenhang wurden in mehreren europäischen Ländern die ersten Bußgelder für Verstöße gegen die Verordnung verhängt. In Italien hingegen war die Haltung der Aufsichtsbehörde zunächst kulant, auch aufgrund von Verzögerungen bei der Wahl des neuen Kollegiums der Aufsichtsbehörde. In jüngster Zeit wurden jedoch die Kontrollen und Inspektionen intensiviert und die ersten Sanktionen, die in den lokalen und supranationalen Datenschutzgesetzen vorgesehen sind, verhängt, und dank der von der Beobachtungsstelle für Cybersicherheit und Datenschutz durchgeführten Untersuchungen können wir sehen, wie diese Rechtsvorschriften den italienischen Kontext verändern.

Der Stand der Einhaltung der italienischen Datenschutzgrundverordnung

Um die Veränderungen zu untersuchen, die in italienischen Unternehmen im Hinblick auf den Datenschutz stattfinden, hat die Beobachtungsstelle vier Aspekte untersucht:

- Stand der Compliance-Projekte
- eigenes Budget
- durchgeführte Maßnahmen
- Kritische Probleme, die aufgetreten sind

Die Studie zeigt, dass fast alle italienischen Unternehmen Projekte zur Einhaltung der DSGVO durchgeführt oder perfektioniert haben. Mehr als die Hälfte der Organisationen gab an, die Anforderungen der Gesetzgebung zu erfüllen. Gleichzeitig ist die Zahl der Unternehmen, die angaben, sich der Auswirkungen der DSGVO nicht bewusst zu sein, zurückgegangen.

Zu letzterem Punkt ist jedoch anzumerken, dass es sich dabei um Unternehmen handelt, in denen das Thema Datenschutz noch nicht an der Spitze angekommen ist, aber dennoch den Fachfunktionen wie IT-Sicherheit, Recht und Compliance bekannt ist. Ein weiteres positives Zeichen für die Reife und das Bewusstsein für die DSGVO in Italien ist der geringe Prozentsatz der Unternehmen (5 %), die sich noch in der Phase der Analyse der Anforderungen und der Festlegung von Plänen zur Einhaltung der Vorschriften befinden, während dieser Anteil vor zwei Jahren noch bei 34 % lag. Ein positives Bild ergibt sich auch in Bezug auf das Budget, das für Maßnahmen zur Einhaltung der DSGVO bereitgestellt wird: 45 % der italienischen Unternehmen haben ihr entsprechendes Budget aufgestockt. Diese Zahl ist zwar positiv, aber es stimmt auch, dass sich der Schwerpunkt noch auf spezifische Aktivitäten wie regelmäßige Audits, die Aktualisierung von Verfahren und Sicherheits- und Datenschutztechnologien verlagern muss. (Andrea Antonelli 2020)

Maßnahmen zur Einhaltung der DSGVO

Was tun italienische Unternehmen konkret, um die Datenschutz-Grundverordnung einzuhalten? Es ist zu bedenken, dass der Prozess der Einhaltung der Vorschriften notwendigerweise aus mehreren Phasen besteht, die derzeit unterschiedlich weit fortgeschritten sind:

- Erstellung des Verarbeitungsregisters (85%): obligatorische Erstellung eines Registers, in dem alle durchgeführten Verarbeitungen festgehalten werden;
- Festlegung von Aufgaben und Zuständigkeiten (81 %): Ermittlung und vertragliche Festlegung aller für die Verarbeitung Verantwortlichen;
- Änderung von Formularen (76 %): Aktualisierung von Formularen gemäß den Anforderungen der Datenschutz-Grundverordnung;
- Verfahren zur Meldung von Datenschutzverletzungen (68 %): Verfahren zur Benachrichtigung der Aufsichtsbehörde über Verletzungen der Vertraulichkeit von Daten;
- Festlegung von Sicherheitsmaßnahmen und Risikobewertung (66 %): Ergreifung von Maßnahmen, um sicherzustellen, dass die Verarbeitung mit der Verordnung im Einklang steht;
- Datenschutz-Folgenabschätzung (56 %): obligatorische Datenschutz-Folgenabschätzung (DPIA), wenn die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt;
- Umsetzung von Verfahren zur Ausübung der Rechte der betroffenen Personen (54 %): Maßnahmen zur Durchsetzung der Rechte, die den betroffenen Personen durch die Verarbeitung gewährt werden. (Andrea Antonelli 2020)

Zusätzlich zu diesen Maßnahmen ist es auch notwendig, die Einbindung des Datenschutzbeauftragten (DSB) in die Unternehmen zu berücksichtigen. Dieser Beauftragte, dessen Ernennung in der Datenschutz-Grundverordnung in einigen Fällen vorgesehen ist, ist in 65 % der **Unternehmen** vorhanden. Diese Zahl ist sicherlich positiv, denn sie zeigt, dass die Zahl der Unternehmen, die diese Funktion eingeführt haben, gestiegen ist.

Welche kritischen Fragen bringt die Datenschutz-Grundverordnung für italienische Unternehmen mit sich?

Es stimmt zwar, dass der Stand der Einhaltung der italienischen Datenschutzgrundverordnung im Allgemeinen positiv ist, aber es stimmt auch, dass die Organisationen auf einige Schwierigkeiten gestoßen sind. Tatsächlich haben viele Unternehmen immer noch Schwierigkeiten in organisatorischer Hinsicht, z. B. bei der Festlegung von Rollen und Verantwortlichkeiten innerhalb des Unternehmens, während andere von einer erheblichen Verlangsamung der täglichen Aktivitäten berichten.

Diese negativen Elemente sind jedoch von geringer Bedeutung im Vergleich zu einem ausgereiften Szenario, in dem italienische Unternehmen sich nicht nur auf die Herausforderungen des Datenschutzes einstellen, sondern sich auch des gesamten Themas bewusst sind.

2.5 Litauen

Name der Einrichtung	Kurzbeschreibung	Hauptzweck	Website
Alytus Unternehmn-beratungs-zentrum (AVKC)	Das Alytus Business Consulting Center (AVKC) ist das erste Unternehmensberatungszentrum in Litauen, das am 13. Mai 1993 als gemeinnützige Organisation registriert wurde, die später als öffentliche Einrichtung umregistriert wurde. Alytus Business Consulting Centre - Alytus Regional Development Strategy Teilnehmer*innen an der internationalen Entwicklungszusammenarbeit in der regionalen Entwicklung mit dem schwedischen Jonkompingo County, Polen, Dänemark, Ungarn, Italien regionalen Behörden, Ministerium für bestehende Wirtschaftsförderung Agenturen, Alytus County Gemeinden und assoziierten Strukturen des Initiators.	Alytus Business Consulting Center's Mission - die Förderung und Entwicklung von kleinen und mittleren Unternehmen, die Bereitstellung von Business-Training, Beratung, Information, neue Business Development-Initiativen bei der Entwicklung und Umsetzung der Vernetzung Entwicklung in Alytus Region.	https://www.avkc.lt/lt/
Verband der Leiter der kommunalen Sozialhilfe-anstalten	Verband der Leiter der kommunalen Sozialhilfeeinrichtungen - eine unabhängige, freiwillige Non-Profit-Organisation, der 30 kommunale Pflegeeinrichtungen angehören	Zweck des Vereins - Hilfe bei der Lösung von Problemen von Nutzern der Sozialfürsorge aller Personengruppen durch Verbesserung ihrer Qualität und Integration in die Gesellschaft.	http://ssgivasociacija.blogspot.com/
Anwalts-kanzlei ALIANT Tarvainyte Vilys Bitinas	Das ALIANT®-Team in Litauen bietet integrierte juristische Dienstleistungen in allen Prozessen der Unternehmensführung und -entwicklung sowie bei Geschäftsstreitigkeiten vor nationalen und internationalen Gerichten. Sie arbeiten auch auf dem Gebiet des Datenschutzes	Das ALIANT®-Team in Litauen bietet integrierte juristische Dienstleistungen in allen Prozessen der Unternehmensführung und -entwicklung sowie bei Geschäftsstreitigkeiten vor nationalen und internationalen Gerichten.	www.aliantlaw.lt
LDAPA - Litauischer Verband der	Das vorrangige Ziel der LDAPA-Mitglieder ist es, eine innovative, nicht-kommerzielle Plattform für Fachleute	Das vorrangige Ziel der LDAPA-Mitglieder ist es, eine	https://ldapa.lt/

Datenschutz-beauftragten Lösungen.	im Bereich des Schutzes personenbezogener Daten zu schaffen, um juristisches Fachwissen, bewährte Verfahren, praktische und neue	innovative, nicht-kommerzielle Plattform für Fachleute im Bereich des Schutzes personenbezogener Daten zu schaffen, um juristisches Fachwissen, bewährte Verfahren, praktische und neue	
Zentrum für Informations-sicherheit	Um die operativen Ziele des Zentrums zu erreichen, werden die für die Daten-verarbeitung Verantwortlichen und die Auftragsverarbeiter zur Umsetzung ge-eigneter technischer und organisatori-scher Maßnahmen zum Datenschutz konsultiert. Die betroffenen Personen werden zur Umsetzung der Menschen-rechte im Bereich des Datenschutzes konsultiert.	Ziel des Informati-onssicherheitszent-rums ist es, die Öf-fentlichkeit für die Themen sichere per-sonenbezogene Da-tenverarbeitung, In-formationsschutz und Cybersicherheit zu sensibilisieren.	https://in-fosec.mobi/

Tabelle 5: Interessenvertreter aus Litauen

Das Gesetz über die Entwicklung kleiner und mittlerer Unternehmen der Republik Litauen (2017) legt fest, dass kleine und mittlere Unternehmen mittlere, kleine und sehr kleine Unternehmen sind, die bestimmte Anforderungen erfüllen (Anzahl der Mitarbeiter*innen, Einkommen, Unabhängigkeit) und natürliche Personen, die zur Selbstständigkeit berechtigt sind. Im Jahr 2019 ist die Zahl der kleinen und mittleren Unternehmen um 0,4 Prozent gestiegen. (registriert 11153). Der größte Anteil - 83% - der KMU waren sehr kleine Unternehmen (0-9 Beschäftigte). Kleine Unternehmen machten 14 % aus (10-49 Beschäftigte), mittlere Unternehmen (50-249 Beschäftigte) - 3 % im Jahr 2019. Im Laufe des Jahres stieg die Zahl der Beschäftigten in KMU um 2,2 %.

Trotz der Fortschritte im Bereich der kleinen und mittleren Unternehmen, der Verbesserung des allgemeinen Unternehmensumfelds und des Abbaus von Markteintrittsschranken ist die Dynamik des Unternehmertums in Litauen nach wie vor schwach. Die Verwaltungsverfahren für die Gründung neuer Unternehmen sind komplex, und den Unternehmern fehlt es an Startkapital, Management- und Finanzkenntnissen, Marketing- und Exportkenntnissen und Informationen. Beschlüsse zur Überwindung einer Pandemiekrise, zur Ankurbelung der Wirtschaft und zur Verbesserung des Unternehmensumfelds sind schwer umzusetzen und führen nicht zu den erwarteten Ergebnissen.

Die Untersuchungen des TebeISi-Projekts in Litauen zeigen, dass diesem Thema zu wenig Aufmerksamkeit geschenkt wird. Dem öffentlichen Sektor sowie kleinen und mittleren Unternehmen wird zu wenig Aufmerksamkeit geschenkt. Die mangelnde Aufmerksamkeit hängt mit dem Mangel an Finanzmitteln zusammen. Der Teil der Gesellschaft, der auf die eine oder andere Weise von der Informationssicherheit betroffen ist, schenkt ihr mehr Aufmerksamkeit. Nach Ansicht von Expert*innen wird staatlichen Einrichtungen viel Aufmerksamkeit geschenkt. Was die Unternehmen betrifft, so ist die Aufmerksamkeit weitaus geringer, da nicht viele Menschen das Thema vollständig verstehen. Die Aufmerksamkeit der Öffentlichkeit für die Informationssicherheit nimmt auch durch öffentliche Sicherheitsvorfälle zu. Die Untersuchung zeigt, dass die KMU der innerbetrieblichen Ausbildung nicht genügend Aufmerksamkeit schenken. Dies hängt in der Regel von der Initiative der Mitarbeiter*innen selbst ab, die sich um eine Schulung bemühen und daran teilnehmen. In jüngster Zeit haben Expert*innen den Mangel an Schulungen auch mit der schwierigen Situation der COVID-19-Pandemie in Verbindung gebracht, als viele Unternehmen suspendiert wurden und sich auf das Überleben konzentrierten.

Eine quantitative Studie, durchgeführt von M. Lipinskienes (2019) Eine quantitative Studie, durchgeführt von M. Lipinskienes (Österreichische Presseagentur 2020) (2019) über die Umsetzung der Datenschutz-Grundverordnung in litauischen Unternehmen ergab, dass die an der Umfrage teilnehmenden Unternehmen in Litauen, die selbst personenbezogene Daten verarbeiten und einen Datenverarbeiter mit der Datenverarbeitung betrauen, die DSGVO in ausreichendem Maße einhalten. Bei der Fragebogenerhebung beantworteten die Befragten die Aussage: "Das Unternehmen, das ich vertrete, hat die Anforderungen der Datenschutz-Grundverordnung wirksam umgesetzt" von 1 "stimme überhaupt nicht zu" bis 100 "stimme voll zu". Die Antworten wurden im SPSS-Programm auf einer Intervallskala kodiert und die durchschnittliche Punktzahl der Befragten wurde berechnet. Insgesamt 77 Befragte beantworteten die Aussage, die niedrigste Bewertung war 0, die höchste 100, und die durchschnittliche Punktzahl war 77 auf einer 100-Punkte-Skala, was "ich stimme zu" bedeutet. Die Befragten bewerteten ihr Unternehmen am häufigsten mit 100 Punkten - 23 Befragte, 8 Befragte - mit 95 Punkten, 6 - 90 Punkte, 7 - 85 Punkte, 6 - 80 Punkte. Bis zu einer Punktzahl von 80 werden die Antworten mit "stimme voll und ganz zu" bewertet, was eine vollständige Einhaltung der DSGVO bedeutet. Von den 77 befragten Unternehmen haben 50 zugestimmt, was 65 % entspricht. Mehr als die Hälfte der Unternehmensvertreter stimmen der Aussage, dass das Unternehmen den GDPR-Standard einhält, voll und ganz zu".

Die Umfrage ergab, dass die Verordnung nach Meinung der Befragten eher abstrakt, lakonisch, schwer zu lesen und für Nicht-Juristen schwer zu verstehen ist. Den Unternehmen, die die Daten selbst verarbeiten, fehlt es an Wissen und Verständnis für die DSGVO, was zu Unwissenheit und Zögern führt. Innerbetriebliche Schulungen sind jedoch wichtig und bedeutsam für jede Mitarbeiterin und jeden Mitarbeiter des Unternehmens und für das Unternehmen selbst. Um die DSGVO einzuhalten, muss

der für die Datenverarbeitung Verantwortliche herausfinden, welche personenbezogenen Daten gespeichert werden, wo, zu welchem Zweck, wie lange und wie sie verarbeitet und gespeichert werden. Nur wenn der für die Datenverarbeitung Verantwortliche weiß, was er zu tun und zu verwalten hat, kann er sich entsprechend verhalten. Dies wurde im Rahmen des TebeISi-Projekts "Desk-Research" (IQ1), "Data Processing" (Datenverarbeitung) und "Personal Data Protection Assessment" (Schutz personenbezogener Daten) als Gelegenheit zur Ermittlung redundanter Informationen und zur Überprüfung von Geschäftsprozessen bestätigt. Auf diese Weise würden effiziente Geschäftsprozesse in Unternehmen erkannt, ineffiziente und redundante Prozessschritte reduziert oder eliminiert. Dies würde den Unternehmen helfen, die Sicherheit von Informationen und den Schutz personenbezogener Daten zu gewährleisten.

Ausbildungssituation

In Litauen gibt es ein breites Angebot an Schulungen (1,5 Stunden bis mehrere Tage) zur Daten- und Informationssicherheit. Meistens werden die Schulungen von privaten Einrichtungen angeboten, zum Beispiel: Cyber Security Academy, gegründet von UAB "Hermitage Solutions", deren Ziel es ist, IT-Spezialisten auszubilden, die in der Lage sind, komplizierte Cybersicherheitsprobleme rechtzeitig und effizient zu lösen und die Anfälligkeit der IT-Infrastruktur ihres Unternehmens zu bewerten. UAB "Atea" ist der führende baltische Anbieter von IT-Lösungen und -Dienstleistungen und unterstützt Klient*innen mit Fachkompetenzen, Produkten, Dienstleistungen und Lösungen in den Bereichen IT-Infrastruktur, Softwareentwicklung und Sicherheit. NRD Cyber Security ist ein Unternehmen für Cybersecurity-Technologieberatung, Incident Response und angewandte Forschung. Das Unternehmen konzentriert sich auf Dienstleistungen für spezialisierte öffentliche Dienstleister (Strafverfolgung, nationale CERTs, Telekommunikation, nationale Kommunikationsregulierungsbehörden, nationale kritische Infrastrukturen), die Finanzindustrie und Unternehmen mit hoher Datensensibilität. UAB "Competence Development" bietet Schulungen zur Vorbereitung auf die gängigsten Zertifizierungen an, die die Grundlage für die Arbeit mit Geräten anderer Hersteller bilden, so dass diese Zertifizierungen von Arbeitgebern nicht nur in Litauen, sondern auch im Ausland häufig bevorzugt werden.

Schulungen zur Informationssicherheit werden für verschiedene Zielgruppen organisiert: sowohl für Anfänger als auch für fortgeschrittene IT-Benutzer und IT-Fachleute. Die Hauptthemen der Informationsschulung sind: "Informationssicherheitsschulung"; "Cybersicherheitsschulung"; "Informationssicherheitsschulung für Nichtfachleute". Eine separate Gruppe von Informationssicherheitsschulungen richtet sich an IT-Fachleute. Sie werden zu Themen geschult wie: "Grundlagen der Cybersicherheit"; "Hack IT to Defend IT"; “Ethical Hacker“; “Practitioner“; "Sicheres Programmieren"; "IT-Sicherheitspraktiker"; "Cybersicherheitsvorfallmanagement" und "IT-Sicherheitsschulung".

Berufliche Schulungen auf verschiedenen Ebenen zu Datenschutzthemen richten sich meist an IT-Fachleute. Die Hauptthemen solcher Schulungen beziehen sich auf den Schutz personenbezogener Daten im Rahmen der GDPR-Anforderungen. Schulungen zur Datensicherheit werden auch für Unternehmensjuristen, Verwaltungsangestellte, Manager*innen und Personalleiter*innen organisiert. Solche Schulungen beinhalten eine Einführung in die DSGVO, den "Schutz personenbezogener Daten und die Verantwortung bei Verstößen gegen die DSGVO" sowie den "Schutz personenbezogener Daten und Verstöße gegen die Datenschutzgesetze im Jahr 2018".

2.6 Die Datenschutz-Grundverordnung und wirtschaftliche Tätigkeiten

Mit der Einführung der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 hat die Europäische Kommission kohärente Leitplanken gesetzt, die das Grundrecht auf Datenschutz gewährleisten und eine Grundlage für die Umsetzung der Charta der Grundrechte der Europäischen Union bieten. Die DSGVO hat viele andere Länder rund um den Globus dazu angespornt, in ihrer Datenschutzregulierung aktiv zu werden und dem Weg der EU zu folgen und die Haltung und das Verhalten aller Beteiligten zum Wohle der europäischen Bürger zu beeinflussen.

Dennoch stößt die Annahme der Europäischen Datenstrategie (Europäische Kommission 2020a) auf mehrere Hindernisse, wie die Europäische Kommission in einer Mitteilung über die Umsetzung der Datenschutz-Grundverordnung berichtet (Europäische Kommission 2020b) . Inzwischen ist das allgemeine Bewusstsein für den Wert personenbezogener Daten bei den Bürger*innen gestiegen, und die Verfahrensrechte haben die Möglichkeit gestärkt, Fälle von Fehlverhalten zu melden, vor allem bei der grenzüberschreitenden Nutzung von Daten gibt es noch Defizite. In dieser Hinsicht muss das Recht auf Datenübertragbarkeit zwischen den Diensten zugunsten der Nutzung öffentlicher Güter erforscht und einschränkende Faktoren aufgedeckt werden. (Europäische Kommission 02.06.2020) .

Was die Bedürfnisse der KMU betrifft, so hat die Datenschutz-Grundverordnung die Möglichkeiten des freien Datenflusses innerhalb der EU und des verbesserten Datenflusses mit Unternehmen außerhalb der EU erhöht und dadurch Innovation und wirtschaftliche Aktivitäten gefördert. Die KMU müssen sich jedoch mit der relativ anspruchsvollen Umsetzung der Datenschutz-Grundverordnung auseinandersetzen, um von diesen neuen Möglichkeiten profitieren zu können, da das Risiko von Datenschutzverletzungen nicht mit der Größe eines Unternehmens abnimmt. Daher sollen die Bemühungen um die Bereitstellung praktischer und leicht zu bedienender Instrumente für KMU verstärkt werden. Die Kommission möchte insbesondere KMU unterstützen, indem sie Vorlagen für Verträge und Klauseln bereitstellt, die mit der Datenschutz-Grundverordnung vereinbar sind.

Letztlich spiegelt sich die erfolgreiche Umsetzung auch in der erfolgreichen Durchsetzung durch die nationalen Datenschutzbehörden wider. Wie in Abbildung 9sehen ist, zeigen sich große Unterschiede zwischen den Mitgliedsstaaten.

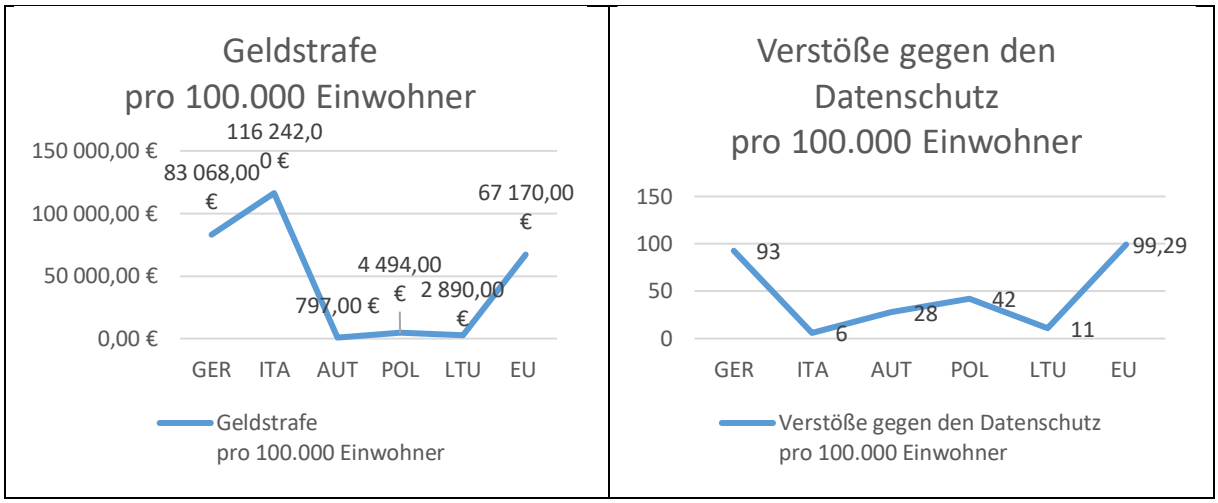

Abbildung 9: Durchsetzung des Datenschutzrechts in den Mitgliedstaaten. Nettowerte pro 100.000 Einwohner.

Daten: heyData (2021) . Eigene Darstellung.

Während alle Länder unter dem EU-Durchschnitt der Gesamtzahl der Datenschutzverletzungen pro 100 000 Einwohner*innen bleiben, der von den hohen Zahlen in Irland (245), Dänemark (325) und den Niederlanden (382) dominiert wird, sind bei den gezahlten Bußgeldern erhebliche Spitzenwerte zu verzeichnen. Um die Beziehung zwischen der Höhe der gezahlten Bußgelder und der Zahl der Verstöße besser zu verstehen, wurden die Nettowerte um die Kaufkraftparität bereinigt, um die Vergleichbarkeit zwischen den Ländern zu gewährleisten. Die Ergebnisse zeigen, dass Deutschland nahe an der durchschnittlichen Aufdeckungsrate in der EU liegt, während Italien, Österreich, Polen und Litauen deutlich darunter liegen. Ähnliches gilt für die gezahlten Bußgelder, mit der herausragenden Ausnahme Italiens, wo die gezahlten Bußgelder fast doppelt so hoch sind wie im europäischen Durchschnitt und rund 40 % über denen in Deutschland liegen. Diese Spitze führte zu einer weiteren Analyse, bei der die Kosten einer Datenschutzverletzung, bereinigt um die Kaufkraftparität, berechnet wurden (Abbildung 10, links), sowie das Risiko der Entdeckung, wobei das durchschnittliche Risikoniveau berechnet wurde, indem der EU-Durchschnittswert auf 1 gesetzt wurde.

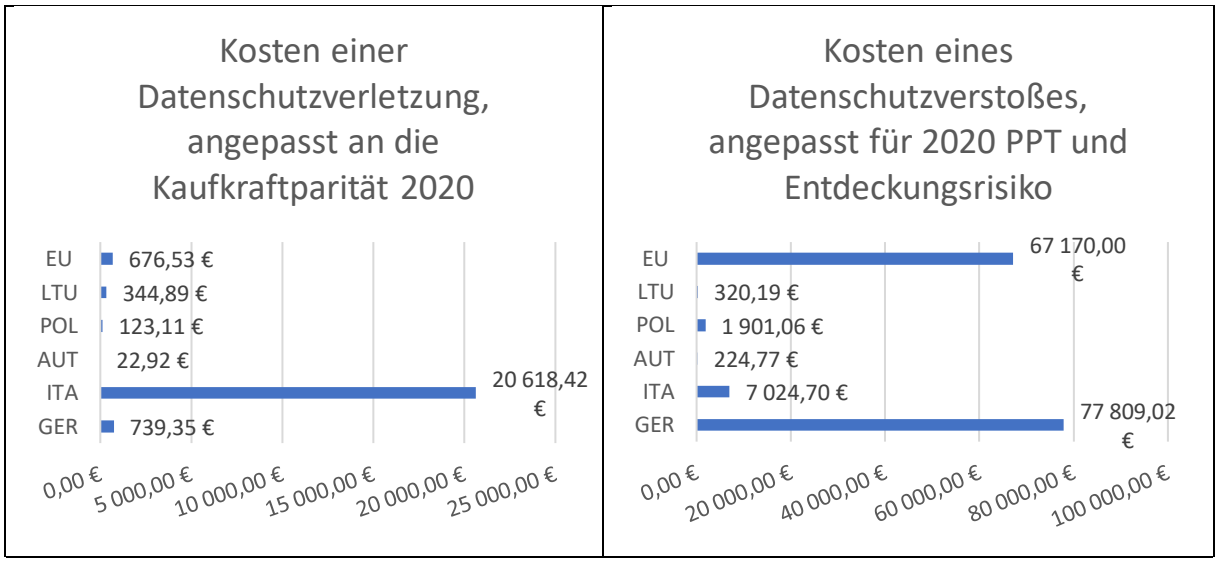

Abbildung 10: Kosten von Datenschutzverletzungen unter Berücksichtigung der Kaufkraftparität und des Entdeckungsrisikos.

Daten: heyData (2021) . Eigene Illustration.

Während die Beobachtung der PPT-Anpassungen deutlich macht, dass pro gemeldeten Fall eine extreme Spitze in Italien zu beobachten ist, macht die Risikoanpassung deutlich, dass es sich dabei um sehr wenige Fälle mit hohen Geldstrafen handelt. Dennoch ist zu erkennen, dass bei der Risikokostenberechnung für Datenschutzverstöße große Unterschiede bestehen, wobei in Österreich, Litauen und Polen nur geringfügige Strafen verhängt werden, während in Deutschland hohe Strafen verhängt werden. Daraus lässt sich schließen, dass die Strafverfolgung noch einen weiten Weg vor sich hat, um in allen Mitgliedstaaten gleichermaßen wirksam zu sein.

In Anbetracht der individuellen Situation in den Partnerländern, speziell für KMU, werden die Herausforderungen im Umsetzungsprozess deutlich. Vor allem Zeitmangel und fehlende Ressourcen wurden als Hauptgründe für die schleppende Umsetzung genannt. Vor allem die Anpassung von Prozessen und die Kontrolle von GDPR-relevanten Informationen im Unternehmen sind Bereiche, in denen KMU in allen Ländern Verbesserungspotenzial haben. Letztlich ist die Frage der ordnungsgemäßen Umsetzung eng mit der Verfügbarkeit von Personal und dem Bedarf an praxisorientierten Schulungen verbunden. Die starke Nachfrage nach Weiterbildungskursen (sowohl freiwillig als auch verpflichtend) verdeutlicht die Marktlücke für prägnante, übertragbare und transparente Kurse, wie in der TeBeISi-Forschungsagenda vorgeschlagen.

2.7 Das schwächste Glied - die Rolle der Mitarbeiter*innen und Privacy Calculus

Angesichts der Bemühungen von Unternehmen, Nichtregierungsorganisationen und Behörden, die DSGVO in die Tat umzusetzen, stößt eine erfolgreiche Implementierung auf die gleichen Hemmnisse wie bei der Umsetzung der Informationssicherheit: den Faktor Mensch. Wie in Kapitel 2.6 gezeigt wurde, besteht ein großer Bedarf an Personal und vor allem an Weiterbildungsangeboten. Die Mitarbeiter*innen als Hauptverursacher von Informationsverlusten und Datenschutzverletzungen spielen eine zentrale Rolle bei der Durchführung und Einhaltung von Datenschutz und Informationssicherheit.

Unternehmen haben viele Möglichkeiten, den Schutz ihrer Daten zu gewährleisten, sei es auf organisatorischer oder auf technischer Ebene. Aus organisatorischer Sicht können sie Prozesse einführen, die sicherstellen, dass nur eine geringe Menge an Daten gesammelt wird, dass physische und digitale Speicher gesichert sind, dass der Zugang zu den Daten auf das zuständige Personal beschränkt ist usw. Die Analyse und Umsetzung dieser Maßnahmen liegt in der Kompetenz des Informationssicherheitsbeauftragten in Zusammenarbeit mit und mit Unterstützung der Unternehmensleitung.

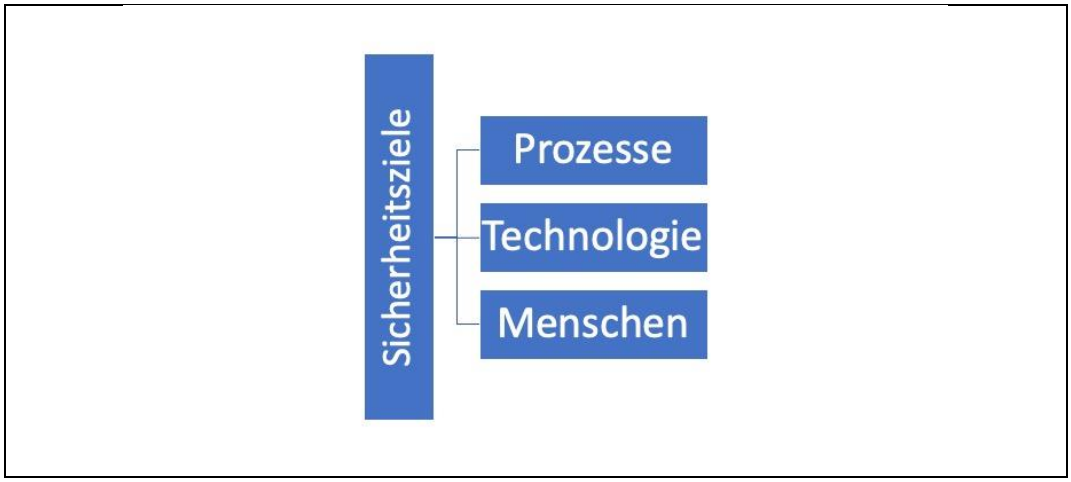

Abbildung 11: Dimensionen des Risikos für die Sicherheitsziele

Auf technischer Ebene können Programme und Anwendungen entwickelt werden, die die Einhaltung der Datenschutzgesetze und der spezifischen Vorschriften des Unternehmens gewährleisten, d. h. "privacy by design". Dienstanbieter haben begonnen, aus Software-as-a-Service-Plattformen (SaaS) ein Geschäftsmodell zu machen, indem sie Privacy as a Service (PaaS) einführen. Auf diese Weise wird die Speicherung und Verarbeitung von Informationen mit Zustimmung des Nutzers auf ein ordnungsgemäßes Verhalten entsprechend den individuellen Anforderungen ausgerichtet. Darüber hinaus hat die Bedeutung sicherer Software in den letzten Jahren stark zugenommen, da Datenlecks in der Öffentlichkeit leichter bekannt werden und den Ruf der Unternehmen schädigen können. Folglich haben die Unternehmen ein Interesse daran, sichere Software zu entwickeln und das Vertrauen ihrer

Nutzer*innen zu gewinnen, was ihnen einen Wettbewerbsvorteil auf dem Markt verschafft.

Schließlich müssen die Unternehmen beim Schutz ihres Know-hows und ihrer kritischen Daten auch die menschliche Dimension berücksichtigen. Sie ist der Nutzer und Akteur im Unternehmen, der Maschinen und Technologien bedient, Aufgaben ausführt und Prozesse überwacht. Während sowohl die Technologie als auch die Prozesse über eine sehr hohe Zuverlässigkeit verfügen, neigen die Mitarbeiter*innen dazu, Fehler zu machen, da sie einer "begrenzten Rationalität" unterworfen sind (Simon 1990) . In der Tat sind etwa 88 % der Datenverletzungen oder Informationsverluste auf menschliche Fehler zurückzuführen, was diese Dimension zur wichtigsten Dimension macht, um die Sicherheit der Daten in einem Unternehmen zu gewährleisten. (Tessian 2021)

Kurz gesagt, das Konzept der begrenzten Rationalität lehnt die Annahme ab, dass menschliches Denken, Verhalten und Handeln von vollständiger Rationalität geleitet wird, da dies ungebundene kognitive Fähigkeiten voraussetzen würde, um alle verfügbaren Informationen sofort zu verarbeiten und vollständig informierte Entscheidungen zu treffen. Stattdessen wird davon ausgegangen, dass der Mensch seinen individuellen Nutzen maximiert, d. h. er wählt eine Handlung, die seinem eigenen wahrgenommenen Bedürfnis am meisten entspricht (so genanntes "Satisficing"). Schließlich kann eine Person auch zu dem Schluss kommen, dass ihr Informationen fehlen, um eine Entscheidung zu treffen, dass aber die Suche nach diesen Informationen mit einem erheblichen Zeit- und Energieaufwand verbunden wäre. Folglich entscheidet sich die Person für eine Handlung mit unvollständigen Informationen, da die Opportunitätskosten (Zeit und Energie) den Nutzen des Besitzes dieser spezifischen Informationen übersteigen.

Das Einrichten einfacher Passwörter (oder das Schreiben auf ein Post-It), das Hinauszögern von Sicherheitsaktualisierungen, das Aufbewahren sensibler Informationen in Schließfächern und das Benutzen des Sticks, der im Aufzug gefunden wurde, sind nur einige der unbedachten Konsequenzen. Das Fehlen vollständiger Informationen und die wahrgenommenen hohen Opportunitätskosten in Momenten der Eile und des Drucks werden zunehmend durch Social-Engineering-Angriffe ausgenutzt, bei denen ein Eindringling per Mail oder Telefon ein Szenario schafft, das Handlungsdruck erzeugt, in der Hoffnung, dass der Mitarbeiter, die Mitarbeiterin Sicherheitsprotokolle beiseite lässt und kritische Informationen (z. B. Passwörter, Finanzinformationen usw.) freiwillig preisgibt.

Leider kostet die Einhaltung korrekter Verhaltensweisen im Arbeitsalltag zusätzliche Energie, die in einem produktiven oder hektischen Arbeitsumfeld oft eine knappe Ressource ist. Vor dem Hintergrund etablierter Arbeitsroutinen stellen veränderte Einstellungen, Überzeugungen und schließlich Verhaltensweisen eine große Herausforderung sowohl für das Unternehmen als auch für seine Mitarbeiter*innen dar. Die Schulung, Ausbildung und Sensibilisierung der Mitarbeiter*innen mit dem Ziel, das Bewusstsein für die ständige Bedrohung der wertvollsten Güter des Unternehmens - seines Know-hows und seiner Daten - zu schärfen, ist heute wichtiger als je zuvor. Und da es immer schwieriger wird, Angriffe jeglicher Art zu starten, müssen sich immer mehr KMU mit einer neuen Realität auseinandersetzen: Sie sind bereits oder werden höchstwahrscheinlich gezielten Angriffen ausgesetzt sein. Was kann also getan werden?

3 TeBeISi-Strategie

Das Projekt TeBeISi hat die Situation der Informationssicherheit, auch im Hinblick auf die Umsetzung der Datenschutzgrundverordnung, auf Unternehmensebene in den Partnerländern analysiert. Nach einer Überprüfung der derzeit bestehenden Berufsprofile, formalen Qualifikationen und Zertifizierungen wurde ein Abgleich der derzeit vorhandenen, übertragbaren Kompetenzen mit den aus der quantitativen und qualitativen Analyse generierten Anforderungen durchgeführt.

3.1 Verbindung von Hochschulbildung und beruflicher Bildung

Nach Auswertung aller mittels quantitativer und qualitativer Forschung gesammelten Informationen kam das Projekt zu dem Schluss, dass der Bereich Informationssicherheit prädestiniert ist für eine Mischung aus Berufsausbildung und Hochschulbildung. Dafür gibt es drei Gründe, die für diese Idee sprechen:

1. Operative Tätigkeiten: Die meisten der in einem KMU zu erledigenden Aufgaben sind eher routiniert. Der Grad des Wissenstransfers und der Neukontextualisierung bleibt gering, da Technologie und Prozesse auf einem standardisierten Niveau bleiben und die Unternehmen standardisierte EDV-Software und Kommunikationskanäle nutzen. Die meisten KMU können ihr Sicherheitsniveau deutlich erhöhen, wenn sie sich an die 20:80-Regel (oder ähnlich) halten - sie erreichen 80 % Sicherheit, indem sie 20 % der für 100 % erforderlichen Arbeit leisten. Dies ist natürlich nicht möglich, wenn man den Datenschutz berücksichtigt, der gesetzlich vorgeschrieben ist und für den die Unternehmen verpflichtet sind, die Anforderungen der Datenschutz-Grundverordnung zu erfüllen. Die Folgen dieser Feststellung sind vielfältig: Die Unternehmen müssen berücksichtigen, ob sie eine bestimmte Zertifizierung anstreben (aufgrund der Art ihres Produkts, der Anforderungen des Marktes usw.), ob sie über Ressourcen verfügen, die mehr als routinemäßige Schutzmaßnahmen erfordern, usw. So befinden sich KMU oft in einer Situation, in der die strukturelle Einhaltung grundlegender Sicherheitsmaßnahmen eine deutliche Erhöhung des allgemeinen Sicherheitsniveaus und eine deutliche Verringerung der Risikoexposition in einem kosteneffizienten Kompromiss ermöglicht.

2. Rechtliche Verpflichtungen: Trotz der Möglichkeit, routinemäßige Aufgaben in einer strukturierten Arbeitsumgebung durchzuführen, berühren einige Aspekte der Informationssicherheit auch rechtliche Aspekte, insbesondere hinsichtlich der Umsetzung einer korrekten Datenverarbeitung nach der DSGVO. Aufgrund der Komplexität des Umgangs mit nationalen Vorschriften muss das verantwortliche Personal über die Kompetenz verfügen, sich mit der Gesetzgebung und der korrekten Umsetzung auseinanderzusetzen. Diese Verantwortung beinhaltet ein hohes Maß an Fähigkeit, abstraktes Wissen in einem Arbeitsumfeld zu rekontextualisieren und zu übertragen. Während der Grad der Komplexität bei der unter (1) beschriebenen technischen Seite der Informationssicherheit

überschaubar bleibt, erfordert die rechtliche Seite eine sorgfältige Ausbildung und Ausführung zur Einhaltung der jeweiligen Gesetze.

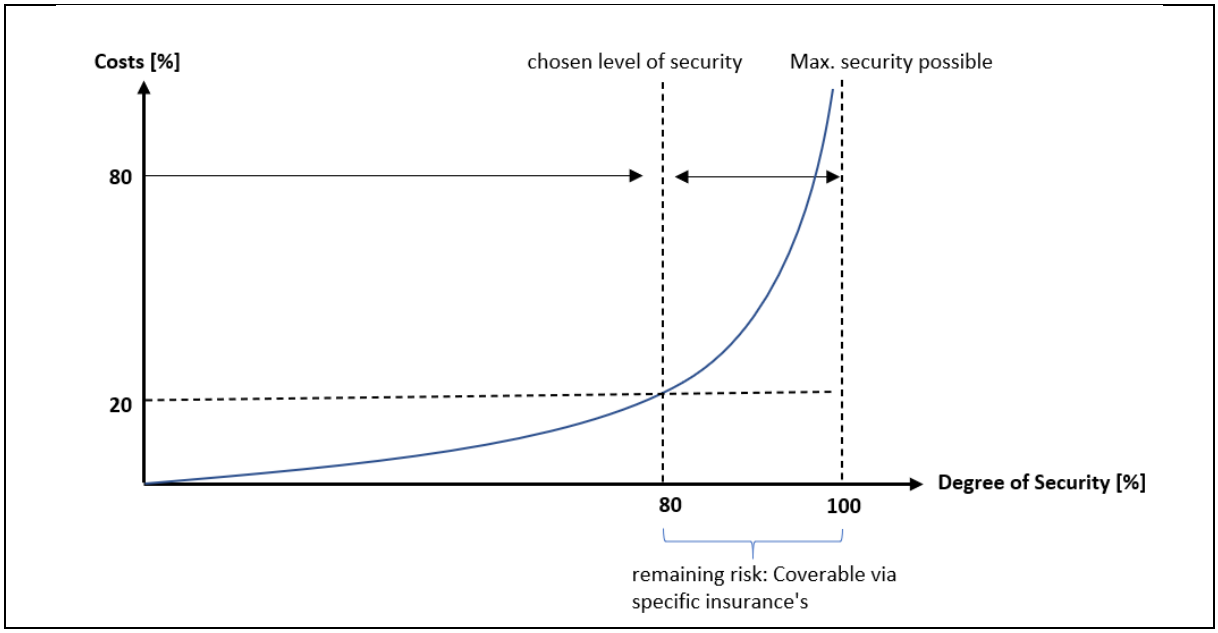

Abbildung 12: Kompromiss zwischen Kosten und Sicherheit bei Investitionen in die Informationssicherheit

3. Die Arbeit von Informationssicherheitsverantwortlichen erfordert vielfältige soziale Kompetenzen. Wie unter 2.3 beschrieben, geht die größte Bedrohung für die Sicherheit eines Unternehmens von seinen Mitarbeitern aus. Die Einstellung der Mitarbeiter*innen zu ändern, ihre Arbeitsroutinen zu beeinflussen und eine Kultur der Informationssicherheit im Unternehmen zu etablieren, stellt wohl die größte Herausforderung bei der Implementierung eines Informationssicherheitssystems dar. Die verantwortliche Person muss Mitarbeiter*innen, Manager*innen und Informationssicherheiten aktivieren, zusammenarbeiten, anleiten, betreuen und miteinander in Einklang bringen. Es ist nicht verwunderlich, dass Unternehmen Fachleute mit Berufserfahrung schätzen - und praktische Erfahrung höher bewerten als jede formale Qualifikation (vgl. Studie "Informationssicherheitsausbildung für KMU"). Eine praxisnahe Ausbildung lehrt die Fallstricke in der täglichen Zusammenarbeit mit Kollegen und die Fähigkeiten, mit den Beteiligten im Unternehmen produktiv zu interagieren.

Die Ausbildung im Bereich der Informationssicherheit, sofern vorhanden, konzentriert sich derzeit stark auf die Vermittlung und Schulung technischer Kompetenzen, entweder im Bereich der IT oder des Rechts. Das Sammeln von praktischen Erfahrungen, insbesondere von effektiven Kommunikationsstrategien, findet nur selten den Weg in die Lehrpläne. TeBeISi schlägt daher vor, das Beste aus beiden Welten miteinander zu verbinden und Bildung durch berufliche Aus- und Weiterbildung und Hochschulbildung zu vermitteln.

3.2 Nutzung der europäischen Instrumente

Die Verbindung von beruflicher Bildung und Hochschulbildung wurde von der Europäischen Kommission innerhalb des Europäischen Qualifikationsrahmens (EQR) als machbar definiert. Außerdem soll das Europäische Leistungspunktesystem für die Berufsbildung (ECVET) eingesetzt werden, um für Transparenz und Vergleichbarkeit in der beruflichen Bildung zu sorgen. Schließlich können einzelne Kompetenzen unter Bezugnahme auf den Europäischen Rahmen für Fähigkeiten, Kompetenzen, Qualifikationen und Berufe (ESCO) so formuliert werden, dass sie in verschiedenen beruflichen Kontexten wiederverwendbar und erkennbar sind.

Die Nutzung europäischer Instrumente hebt einen transparenten Zertifizierungsprozess von dem bereits bestehenden, unübersichtlichen Markt der Zertifizierungen privater Anbieter ab. Es muss noch einmal betont werden, dass es auch im Bereich der KMU vielfältige Zertifizierungen gibt, jedoch bleibt unklar, inwieweit gemeinsame Qualitäts- und Qualitätssicherungsstandards verwendet werden, was zu einem Mangel an Transparenz und Übertragbarkeit zwischen den Ländern führt. Der Nachholbedarf an europaweiten Akkreditierungs-, Qualitätssicherungs- und Kompetenzstandards ermöglicht eine breite und transparente Einführung von Zertifizierungen über Bildungssysteme und institutionalisierte Zertifizierungslandschaften hinweg.

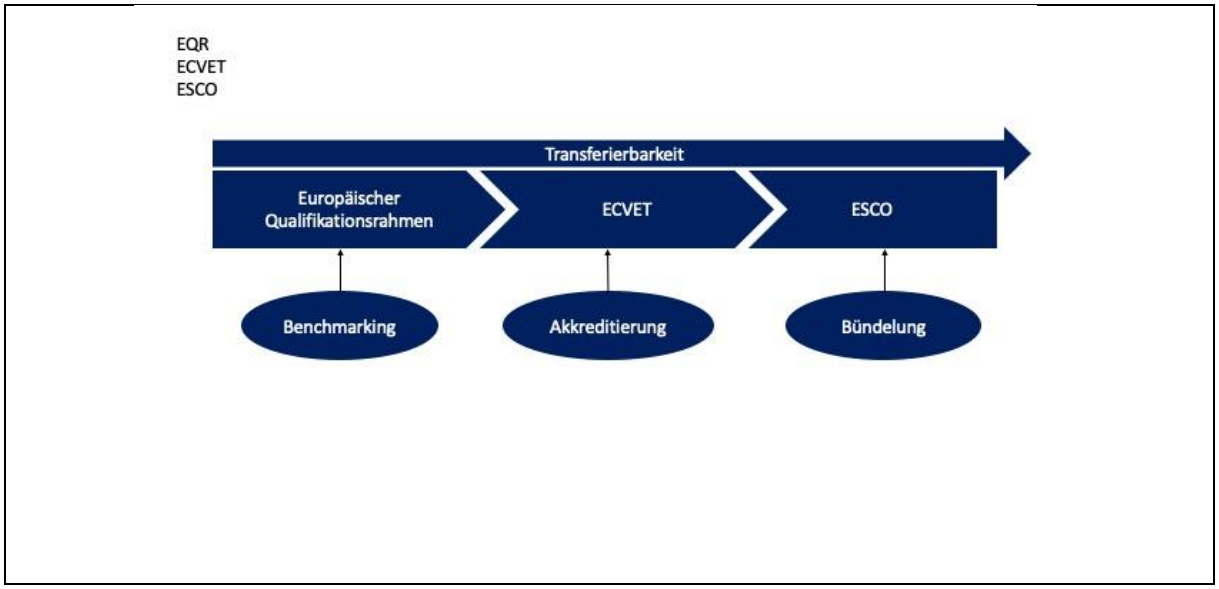

Abbildung 13: Transparenz-Instrumente für die Berufsbildung in der EU

Kurz gesagt, diese Instrumente unterstützen die EU-weite Verbreitung von Kompetenzen und Qualifikationen. Der EQR als Benchmarking-System kategorisiert Qualifikationen nach den ihnen zugrundeliegenden Fähigkeiten, Kompetenzen und Autonomie und bietet die Möglichkeit, jede Qualifikation aus den verschiedenen Bildungssystemen in ein einziges Referenzschema einzuordnen, das die verschiedenen Qualifikationen über unterschiedliche Bildungskontexte hinweg vergleichbar macht. ECVET bietet die Grundlage für die Bündelung von

Lernergebnissen in Lernkredite, die einen Einblick in den Umfang und die Tiefe des Lernens hinter einer Qualifikation geben.

Darüber hinaus unterstützt es die Qualitätssicherung, bietet Weiterbildungsmöglichkeiten in regionalspezifischen Kontexten und fördert die Akkreditierung beruflicher Qualifikationen in verschiedenen systemischen oder nationalen Bildungswegen. Schließlich stellt die ESCO eine vereinheitlichende Datenbank dar, die bestehende Qualifikationen und Kompetenzen aus der gesamten EU zusammenführt. Durch den Rückgriff auf diese Datenbank bei der Erstellung neuer Curricula kann sichergestellt werden, dass die Kompetenzen in unterschiedlichen Lernkontexten verstanden werden.

3.2.1 Europäischer Qualifikationsrahmen

Der Europäische Qualifikationsrahmen stellt eine Systematisierung der formalen Qualifikationen zwischen den Bildungssystemen in der Europäischen Union dar.[2]Ziel dieses Rahmens ist es, Qualifikationen zwischen den Ländern vergleichbar zu machen und somit das Verständnis für den Wert einer Qualifikation im Ausland zu erhöhen. Da sich die Bildungssysteme in den EU-Mitgliedsstaaten stark unterscheiden, kann der EQR als Referenz verwendet werden, um die Gleichwertigkeit der vermittelten Kompetenzen zu gewährleisten. Im TeBeISi-Kontext wurde festgestellt, dass die EQR-Stufe 5 wertvolle Möglichkeiten für Unternehmen und Lernende bietet.

Die für Stufe 5 relevanten Lernergebnisse sind		
Wissen	Fertigkeiten	Zuständigkeiten
umfassende, spezialisierte, faktische und theoretische Kenntnisse in - einem Arbeits- oder Studienbereich und ein Bewusstsein für die Grenzen dieser Kenntnisse	ein umfassendes Spektrum an kognitiven und praktischen Fähigkeiten, die zur Entwicklung kreativer Lösungen für abstrakte Probleme erforderlich sind	Management und Aufsicht in Arbeits- oder Studienkontexten ausüben Tätigkeiten mit unvorhersehbarem Wandel Überprüfung und Weiterentwicklung der eigenen Leistung und der anderer

Tabelle 6: EQF Stufe 5 Lernergebnisse - Kenntnisse - Fertigkeiten - Kompetenzen

Quelle: Europäische Kommission (2008)

In Anbetracht der Tatsache, dass das meiste verfügbare Personal wahrscheinlich für die Bedürfnisse von KMU überqualifiziert ist (was sich auch in den bestehenden Berufsprofilen in ESCO widerspiegelt), müssen geeignete Mittel gefunden werden, um die inhärente Komplexität der Aufgaben im Bereich der Informationssicherheit (d. h. IT-Know-how und rechtliches Wissen) und die Mindestanforderungen von KMU in

[2] c.f. Cedefop 2009

Einklang zu bringen, um neue Lernende in diesem Bereich anzusprechen. Daraus lässt sich schließen, dass aufgrund der Art einiger Aufgaben, insbesondere derjenigen, die mit nicht standardisierten Tätigkeiten verbunden sind oder rechtliche Kompetenzen beinhalten, einige Elemente der Informationssicherheitsausbildung für KMU in der Hochschulbildung verankert werden müssen, was die Lernenden in die Lage versetzt, in einem weniger strukturierten und unabhängigeren Umfeld zu arbeiten. Insbesondere die Kompetenzen im Zusammenhang mit dem Recht, d. h. vor allem mit der DSGVO, fallen in diese Kategorie.

Die Verwendung des EQR 5 bietet mehrere Vorteile, die genutzt werden können. Erstens bietet er vielen Arbeitnehmern mit einer EQR-4-Qualifikation eine Grundlage für den Einstieg in die Weiterbildung. Folglich kann eine Teilvalidierung auf dieser Ebene durch die Anerkennung früherer Berufserfahrung, nicht-formalen und informellen Lernens erleichtert werden. Die Verbindung zum EQR 6 schließt die Lücke und die Anpassungsfähigkeit für Hochschuleinrichtungen, die entweder eine Vollqualifikation im Kontext der Informationssicherheit oder eine Zusatzqualifikation für ihre Studenten anbieten wollen.

3.2.2 ECVET

Aus funktionaler Sicht bedeutet die lernergebnisorientierte Operationalisierung von Kompetenzen einen Perspektivenwechsel von "Was will ich lehren?" zu "Was sollen die Lernenden lernen?". Das Ergebnis des Lernprozesses steht im Mittelpunkt des Lernprozesses und verschafft den Lernenden eine klarere Sicht auf ihren eigenen Lernfortschritt. Durch die Verwendung eines transparenten Leistungspunktesystems können mehrere positive externe Effekte erzielt werden, die den modularisierten Bildungsweg von bestehenden Zertifizierungssystemen unterscheiden.

Die Aufteilung des TeBeISi-Kompetenzprofils eines Beauftragten für Informationssicherheit und Datenschutz in KMU in modularisierte Lernfelder (vgl. "Curriculum") erleichtert die Modularisierung von Lernfeldern und die Anwendung von Credit-Transfer-Systemen wie ECTS oder ECVET. ECVET. Die Modularisierung (Mikro-Credentialisierung) bietet mehrere Vorteile, die in Abbildung 14dargestellt sind und zu einer erhöhten Transparenz, Mobilität und Vertrauenswürdigkeit der Teilqualifikationen führen. Die Module können sowohl für die Aus- und Weiterbildung von Mitarbeitern oder Studierenden genutzt werden als auch als Mittel der Teilvalidierung, indem der Zertifizierungsprozess für Quereinsteiger aus dem Bereich der Informationssicherheit zugänglich gemacht wird.

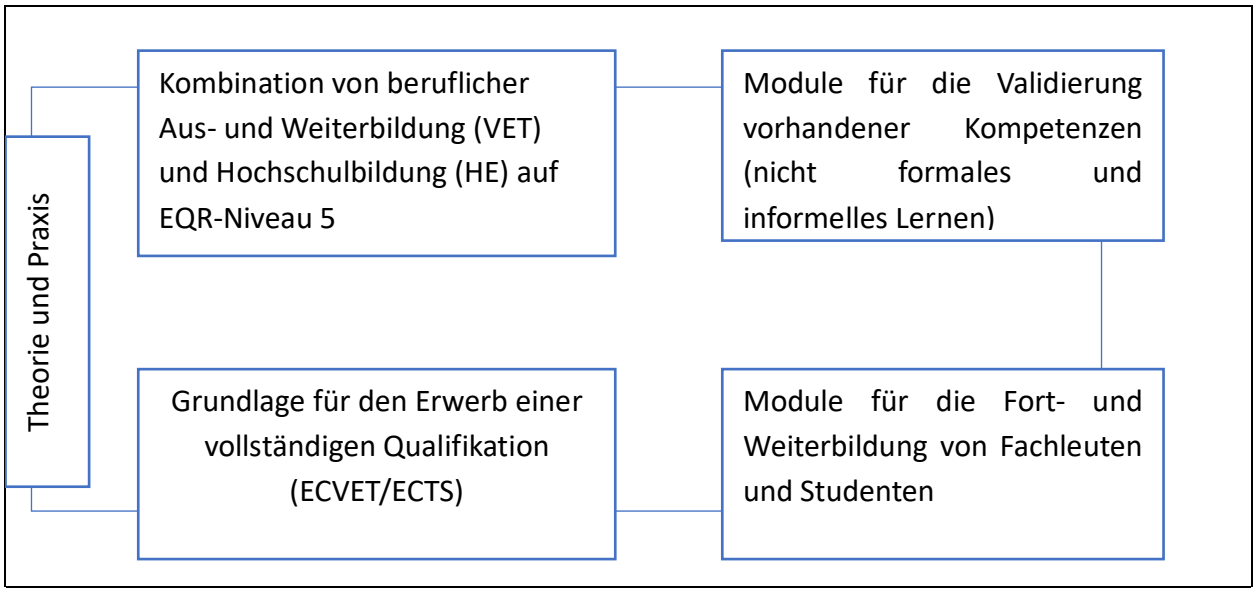

Abbildung 14 : Vorteile der modularisierten Qualifikationen

Bei den bestehenden Validierungssystemen spielt die Vertrauenswürdigkeit eine entscheidende Rolle für die Akzeptanz des Zertifizierungsverfahrens bei Arbeitgebern und Bildungsanbietern. Hier müssen zusätzlich zu den bestehenden Qualitätssicherungsstandards (z. B. EQAVET) spezifische Details zur Kompetenzbewertung berücksichtigt werden, um die höchstmögliche Validität des Validierungsverfahrens zu gewährleisten.

3.3 Messung von Lernergebnissen

Die Messung von Lernergebnissen ist nach wie vor ein stark diskutierter Punkt. Inzwischen gibt es bewährte Verfahren, z. B. VALIKOM oder MySkills aus Deutschland, doch die breite Einführung dieser Methoden kann nicht alle Kritikpunkte von Unternehmen und Bewertungspraktikern ausräumen. Insbesondere bei den Bildungsanbietern stellt sich die Frage, ob Kurz-Assessments geeignet sind, ein ganzes Ausbildungscurriculum zu ersetzen. Um die Validität des Messverfahrens zu erhöhen, müssen mehrere Punkte beachtet werden:

1. Transparente Prozesse. Die Transparenz des gesamten Anerkennungsprozesses ist entscheidend. Ein Anerkennungsgespräch, die Zuweisung eines engagierten Mentors und die angemessene Vorbereitung auf die Beurteilung müssen in einen ganzheitlich durchdachten, schrittweise geplanten Anerkennungsprozess eingebunden sein.
2. Bei der Anerkennung selbst müssen mehrere Maßnahmen berücksichtigt werden, um die größtmögliche Validität der Bewertung zu gewährleisten. Im Allgemeinen sind bestimmte Formen von Bewertungen besser geeignet, um bestimmte Formen von Kompetenzen zu bewerten. Während schriftliche Tests, sei es mit offenen Antworten oder Multiple Choice, geeignet sind, Wissen zu beurteilen, sind Rollenspiele, Post-Box-Übungen oder Pitch-Präsentations-

Spiele darauf ausgerichtet, kommunikative und soziale Kompetenzen wie Gesprächsführung, Rhetorik, Argumentation, Empathie, Durchsetzungsvermögen, Überzeugungskraft, Sensibilität (Verhaltensbeobachtung) zu testen. Sie eignen sich auch zur Beurteilung von Einsatzbereitschaft, Zielorientierung, Frustrationstoleranz, Ausdauer, Problemlösungskompetenz, Analysefähigkeit, Entscheidungsfähigkeit usw. Biografische Methoden wie kriteriengestützte Interviews, Durchsicht eines strukturierten Portfolios und Fachgespräche geben den Bewerbern einen umfassenden Einblick in ihre eigenen Leistungen und lassen sie sich selbst und ihre Qualitäten einschätzen. Schließlich ermöglichen Beobachtungen vor Ort und in einer simulierten Umgebung die Beobachtung von Reaktionen in realen Szenarien, des Selbstverhaltens und des Umgangs mit spontanen Ereignissen. Durch eine Mischung von Beurteilungsmethoden können somit granulare Kompetenzen trianguliert und die Disposition zuverlässig bestimmt werden.

3. Um objektive Beurteilungen durchführen zu können, müssen die Beurteiler darin geschult werden, mit unterschiedlichen Beurteilungsmethoden, unterschiedlichen Beurteilungs-Voreingenommenheiten und unterschiedlichen Kandidaten auf faire, transparente und objektive Weise umzugehen. Die Bewerter müssen sich der unterschiedlichen Lernbiografien und der verschiedenen Ziele der Kandidaten bewusst sein und den gesamten Validierungs- und Anerkennungsprozess verstehen.

4. Selbsteinschätzungen als Schritt zur Beurteilung werden empfohlen, aber Selbsteinschätzungen als Quelle der Beurteilung werden nicht empfohlen. Selbsteinschätzungen in Form von technischen Bewertungen ("Kandidat X weiß..." "Ja", "Nein") oder in Form von Persönlichkeitstests können indikative Ergebnisse liefern, deren Zuverlässigkeit und Objektivität jedoch in Frage zu stellen ist.

Daher müssen eine detaillierte Struktur und ein Qualitätssicherungssystem eingerichtet werden, um eine zuverlässige, objektive und transparente Bewertung zu gewährleisten und Vertrauen zwischen Bildungseinrichtungen und Arbeitgebern zu schaffen.

4 Ausblick und Empfehlungen

Der Mangel an qualifizierten Arbeitskräften im Bereich der Informationssicherheit besteht in der gesamten EU fort. Die technischen Kompetenzen der Fachkräfte werden im Vergleich zu den sozialen und persönlichen Kompetenzen immer unwichtiger. Investitionen in das Humankapital, d. h. in eine angemessene Ausbildung der Mitarbeiter*innen, sind angesichts diffuser Risikosituationen wie multidimensionaler Angriffsvektoren im physischen und digitalen Raum zunehmend rentabel. Die Sicherheit des Firmen-Know-hows und die Bereitschaft interner und externer Dienste ist zunehmend mit neuen Ausbeutungspotenzialen verbunden. Doch alle neuen Technologien und Richtlinien, die eingeführt wurden, um das Risiko feindlicher Übergriffe einzudämmen, werden letztlich zunichte gemacht, wenn die Mitarbeiter*innen des Unternehmens die Sicherheitskultur des Unternehmens nicht akzeptieren und aktiv leben.

Risikobewusstsein und die Einhaltung von Richtlinien sind der Ausgangspunkt für die Verringerung des Risikos von Angriffen jeglicher Art. Um dies zu erreichen, müssen die Werte, Überzeugungen und letztlich das Verhalten der Menschen in einem Unternehmen geändert werden, um eine lebendige Risikokultur zu schaffen. Die Verlagerung der Aufmerksamkeit weg von der technischen Seite des zugrunde liegenden Problems hin zum menschlichen Faktor macht deutlich, dass Bildung und Ausbildung auch aus diesem Blickwinkel betrachtet werden müssen.

Die zunehmenden kriminellen Aktivitäten im Zusammenhang mit privaten und vertraulichen Informationen im digitalen Zeitalter stellen nicht nur die Ausbildung von Fähigkeiten im beruflichen Umfeld und im Arbeitsbereich in Frage, sondern auch den privaten Bereich der europäischen Bürger. Auch wenn Angriffe auf Unternehmen der europäischen Wirtschaft erheblichen Schaden zufügen, ist es wichtig, die Auswirkungen der zunehmenden kriminellen Aktivitäten im Zusammenhang mit vertraulichen Informationen hervorzuheben: Sie richten sich gegen Einzelpersonen, nicht gegen Unternehmen. Folglich würde der Aufbau von Fähigkeiten bei den Bürgern durch Grundschul- und Weiterbildung positive externe Effekte für Unternehmen und die Gesellschaft schaffen. Der Aufbau von Kapazitäten sollte daher nicht nur im Interesse einzelner Unternehmen liegen, sondern im Interesse der breiten Öffentlichkeit. Die Einführung von Sensibilisierungsschulungen, der Umgang mit sensiblen Informationen und das Verständnis für die eigene Gefährdung durch feindliche Angriffe in Schulen, Berufs- und Hochschuleinrichtungen. Im Jahr 2018 hat der Rat der Europäischen Union "Bürgerkompetenz" neu definiert als

> "die Fähigkeit, als verantwortungsbewusste Bürgerinnen und Bürger zu handeln und uneingeschränkt am staatsbürgerlichen und gesellschaftlichen Leben teilzunehmen, auf der Grundlage eines Verständnisses sozialer, wirtschaftlicher, rechtlicher und politischer Konzepte und Strukturen sowie globaler Entwicklungen und Nachhaltigkeit".

Die Teilhabe als mündige Bürgerinnen und Bürger an der Welt von heute und morgen ist eng mit der Fähigkeit verbunden, vorsätzlichen Schaden von alltäglichen Vorfällen zu unterscheiden. Das Aufspüren von Fehlinformationen und Manipulationen, die Wahrung der Privatsphäre und die digitale Sicherheit sind eine Frage der zivilen Belastbarkeit - und sollten nicht zu einer Frage profitabler Ausgaben privater Unternehmen verengt werden. Letztlich liegt dies im Interesse der Europäischen Union und ihrer Mitgliedstaaten - und ist daher eine Frage, die von Bildungsministerien und nicht nur von IT-Abteilungen beantwortet werden muss.

Infolgedessen werden die folgenden Mittel empfohlen, um die Fähigkeiten der europäischen Bürger zu verbessern:

1. Gründung einer europäischen Organisation für den Schutz von privaten Informationen und Daten. Die Einrichtung einer Anlaufstelle, einer Arena für gemeinsame Überzeugungen in einer kritischen Angelegenheit und einer Plattform für den Wissensaustausch und die Interessenvertretung ist ein entscheidender Bestandteil, um die Interessen der Bürger, der Öffentlichkeit und der Unternehmen zu steuern. Das Hauptziel, die Förderung der übrigen, unten aufgeführten Empfehlungen, liegt im Zentrum einer gemeinsamen Organisation.
2. Einführung von "Informationssicherheit" in die Lehrpläne ceteris paribus "Gesundheit und Sicherheit". Es ist wirtschaftlich nicht machbar, menschliche Werte, Überzeugungen und Handlungen zu ändern. Daher ist es wichtig, in den Bildungsprozess einzugreifen und dem Einzelnen die Bedeutung des Bewusstseins gegenüber diffusen Bedrohungsszenarien, einschließlich gezielter Manipulation und Fehlinformation im digitalen Zeitalter, zu vermitteln.
3. Einführung von Micro-Credentials und Teilzertifizierungssystemen für Informationssicherheit für den privaten und beruflichen Empfang. Die derzeitige Situation in der Aus- und Weiterbildung ist intransparent und es fehlt eine strukturierte Vision für die Zukunft. Neben den bestehenden Zertifizierungssystemen bieten vollwertige Curricula, die aus einzelnen und trainierbaren Modulen aufgebaut sind, vielfältige Möglichkeiten der Nutzung und Replikation. Sie können je nach Thema in die Berufsausbildung (EQF 4) und in die Hochschulbildung (EQF 6-7) integriert werden, zu einem einzigen Ausbildungsweg kombiniert werden, der Berufsausbildung und Hochschulbildung (EQF 5) verbindet, oder den Arbeitnehmern als Weiterbildungsmöglichkeiten angeboten werden. Die Modularisierung ermöglicht ein zielgerichtetes, weniger komplexes und ressourcenintensives Ausbildungsmuster, was zu geringeren Kosten und größeren Chancen für KMU führt.
4. Verstärkte Nutzung der europäischen Transparenzinstrumente zur Förderung der Flexibilität auf dem Arbeitsmarkt und zur Gewinnung neuer Talente.

5 Literatur

Andrea Antonelli (2020): Il GDPR in Italia due anni dopo: a che punto siamo? Online verfügbar unter https://blog.osservatori.net/it_it/gdpr-in-italia-stato-adeguamento, zuletzt geprüft am 10.08.2021.

Österreichische Presseagentur (2020): EU-DSGVO: Verständnis ja, Umsetzung schleppend. KSV1870 Unternehmenskommunikation. Wien (OTS0017). Online verfügbar unter https://www.ots.at/presseaussendung/OTS_20200519_OTS0017/eu-dsgvo-verstaendnis-ja-umsetzung-schleppend, zuletzt aktualisiert am 14.07.2021, zuletzt geprüft am 14.07.2021.

Bitkom e.V. (2020): Studie: Datenschutzverordnung & Privacy Shield. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/Studie-Datenschutzgrundverordnung.pdf, zuletzt geprüft am 22.07.2021.

BVerfG (15.12.1983): Volkszählungsurteil. 1 BvR 209/83.

Cedefop (2009): Europäischer Qualifikationsrahmen (EQR). Online verfügbar unter https://www.cedefop.europa.eu/en/events-and-projects/projects/european-qualifications-framework-eqf, zuletzt aktualisiert am 17.06.2021, zuletzt geprüft am 05.07.2021.

datenschutz (2021): EU-Datenschutzgrundverordnung I Datenschutz 2021. Online verfügbar unter https://www.datenschutz.org/eu-datenschutzgrundverordnung/, zuletzt geprüft am 28.07.2021.

Deloitte Services Wirtschaftsprüfungs GmbH (2020): Deloitte Umfrage Bestandsaufnahme nach 18 Monaten EU-DSGVO, 2020. Online verfügbar unter https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/at-eu-dsgvo-umfrage-2020.pdf, zuletzt geprüft am 27.07.2021.

EUR-LEX: NIS-Richtlinie (EU) 2016/1148. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148, zuletzt geprüft am 27.07.2021.

EUR-LEX (1995): Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31995L0046, zuletzt geprüft am 27.07.2021.

Europäische Kommission (Hg.) (2008): Erläuterung des Europäischen Qualifikationsrahmens für lebenslanges Lernen. Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften. Luxemburg. Online verfügbar unter https://europa.eu/europass/system/files/2020-05/EQF-Archives-EN.pdf, zuletzt geprüft am 05.07.2021.

Europäische Kommission (2020a): KOM/2020/66 endgültig. Eine europäische Strategie für Daten. Brüssel.

Europäische Kommission (02.06.2020): Kommission leitet Konsultation zu digitalen Dienstleistungen ein. Online verfügbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962.

Europäische Kommission (2020b): KOM/2020/264 endgültig. Datenschutz als Grundpfeiler der Befähigung der Bürger und das Konzept der EU für den digitalen Wandel - zwei Jahre Anwendung der allgemeinen Datenschutzverordnung. Brüssel.

Eurostat (2021): Kaufkraftbereinigtes BIP pro Kopf. Online verfügbar unter https://ec.europa.eu/eurostat/databrowser/view/sdg_10_10/default/table?lang=en, zuletzt geprüft am 23.07.2021.

Bundesministerium der Finanzen (BMF): Datenschutz. Online verfügbar unter https://www.bmf.gv.at/en/data-protection.html, zuletzt geprüft am 27.07.2021.

GDPD (2020): Relazione annuale 2020. Online verfügbar unter https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9676435, zuletzt geprüft am 10.08.2021.

heyData (2021): Europa im Datenschutz-Ranking. Online verfügbar unter https://www.heydata.eu/europa-im-datenschutz-ranking, zuletzt aktualisiert am 22.07.2021, zuletzt geprüft am 22.07.2021.

KSV1870: DSGVO-Assistent. Online verfügbar unter https://www.ksv.at/spezielle-loesungen/dsgvo-assistent, zuletzt geprüft am 14.07.2021.

Lienhardt, Conrad (2020): Informationspflicht nach DSGVO. Online verfügbar unter https://fokus.genba.org/informationspflichten-dsgvo, zuletzt aktualisiert am 20.02.2020, zuletzt geprüft am 14.07.2021.

May, Sandra (2021): Deutschland ist Europa-Meister in Sachen Datenschutzverstöße. In: *OnlinehändlerNews*, 29.06.2021. Online verfügbar unter https://www.onlinehaendler-news.de/e-recht/gesetze/134980-deutschland-europa-titel-datenschutzverstoesse, zuletzt geprüft am 23.07.2021.

Amt für den Schutz personenbezogener Daten (2018): Personal Data Protection at the Workplace. Guidebook for Employers. Warschau. Online verfügbar unter https://uodo.gov.pl/pl/file/1469.

Rechtsinformationssystem des Bundes (RIS) (1999): Bundesgesetz über den Schutz von Personendaten (DSG). Online verfügbar unter https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1999_1_165, zuletzt aktualisiert am 26.02.2020, zuletzt geprüft am 27.07.2021.

Simon, Herbert A. (1990): Bounded Rationality. In: John Eatwell, Murray Milgate und Peter Newman (Hg.): Utility and Probability. London: Macmillan Reference Books (The new palgrave), S. 15-18.

Statista (2020): Wie weit sind Sie mit der Umsetzung der Datenschutz-Grundverordnung? Online verfügbar unter https://de.statista.com/statistik/daten/studie/917518/umfrage/stand-der-umsetzung-der-dsgvo-durch-unternehmen-in-deutschland/, zuletzt geprüft am 28.07.2021.

Tessian (2021): Die Psychologie des menschlichen Fehlers | Tessian. Online verfügbar unter https://www.tessian.com/research/the-psychology-of-human-error/, zuletzt aktualisiert am 24.02.2021, zuletzt geprüft am 06.07.2021.

Wirtschaftskammer Österreich (2020): IT-Sicherheit, Datensicherheit. Wien. Online verfügbar unter https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html, zuletzt geprüft am 14.07.2021.

Wirtschaftskammer Österreich (2021a): IT-Safe. Wien. Online verfügbar unter https://www.wko.at/site/it-safe/start.html, zuletzt geprüft am 14.07.2021.

Wirtschaftskammer Österreich (2021b): EU-Datenschutz-Grundverordnung (DSGVO). Überblick zum Datenschutz in Österreich. Wien. Online verfügbar unter https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html, zuletzt geprüft am 14.07.2021.

ZFODO (2020): Die 10 größten Fehler bei der Gewährleistung der Einhaltung von RODO. Warschau. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/05/10-najwiekszych-bledow-przy-wdrazaniu-RODO.pdf.

ZFODO (2021): Verstöße gegen den Schutz personenbezogener Daten 2020. Warschau. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/11/Breach-report-2020-ZFODO.pdf, zuletzt geprüft am 07.07.2021 .

Strategiebericht

Wir danken den Co-Autor*innen von:

BF/M-Bayreuth

Mykolas Romeris Universität

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Gefördert durch das Programm Erasmus+ der Europäischen Union

https://information-security-in-sme.eu/.