Report Strategico

Costruire la capacità di sicurezza dell'informazione tra i cittadini e i dipendenti europei

Funded by the
Erasmus+ Programme
of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

Questo documento è stato prodotto all'interno del progetto ERASMUS+ definito "Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi", ID: 2018-1-EN02-KA202-005218

Contenuti

Elenco delle figure

Elenco delle tabelle

1 Introduzione

Quando è entrato in vigore nel 2018, il GDPR ha evocato una deriva nella percezione e nel valore dei dati personali tra i consumatori, le aziende e la società in generale. L'introduzione di norme e leggi vincolanti e sanzionabili riguardanti la raccolta, l'archiviazione e il trattamento dei dati personali avrebbe dovuto rafforzare i diritti dei consumatori, porre dei limiti allo sfruttamento e alla raccolta dei dati e, in definitiva, aumentare e garantire il diritto alla privacy e alla libertà personale nell'era digitale.

Da allora, dopo molte discussioni pubbliche sul senso e l'insensatezza, così come sul cosa fare e cosa non fare, i primi attriti sono stati superati, e l'onda iniziale di attenzione si è appiattita. La protezione dei dati è diventata endemica nel lavoro di ogni organizzazione. Non solo le aziende sono tenute ad assegnare le responsabilità per il corretto svolgimento della protezione dei dati nella loro azienda, ma ogni dipendente deve essere consapevole delle potenziali violazioni della protezione dei dati nella sua routine di lavoro e del rispetto delle procedure stabilite. Infine, i dipendenti stessi hanno interesse alla protezione dei loro dati quando entrano in un rapporto di lavoro, il che è sottointeso nella protezione dei dati dei dipendenti. I dipendenti, come l'anello più debole nella strategia di sicurezza dell'informazione di un'azienda, devono quindi ricevere un'attenzione speciale. Nel frattempo le grandi aziende hanno lanciato con successo una serie di programmi educativi per formare la consapevolezza del loro personale, le priorità nelle PMI per costruire la sicurezza delle informazioni e le capacità di protezione dei dati sono rimaste basse in confronto.

La sicurezza dell'informazione, che in opposizione alla protezione dei dati, non pone una posizione obbligatoria o qualsiasi vincolo legale al lavoro delle organizzazioni. Tuttavia, tocca molti aspetti dell'elaborazione, della raccolta e dell'immagazzinamento dei dati, e richiede quindi un'ampia istruzione e formazione del personale responsabile. L'istruzione e la formazione, soprattutto nel contesto della protezione del know-how di un'impresa, rimane un aspetto centrale per aumentare la sicurezza delle PMI nell'UE. In questo rapporto, miriamo a definire le premesse e le prospettive dell'istruzione e della formazione della sicurezza delle informazioni e delle competenze di protezione dei dati nell'UE e a fornire raccomandazioni sull'ulteriore sviluppo, specialmente in un ambiente di PMI.

2 Protezione dei dati nei paesi partner

2.1 Polonia

Nome dell'istituzione	Breve descrizione	Sito web
Urząd Ochrony Danych Osobowych (UODO) (Ufficio per la protezione dei dati personali)	L'UODO è il principale organo statale che si occupa della protezione dei dati personali. Come parte dei compiti assegnati dall'art. 57 GDPR, questo organismo, tra l'altro: controlla e fa rispettare l'applicazione del GDPR; diffonde la conoscenza del rischio, dei regolamenti, delle garanzie e dei diritti relativi al trattamento nella società, così come la comprensione di questi fenomeni; consiglia il Parlamento nazionale, il governo e altre istituzioni e organi in materia di protezione dei dati, considera i reclami presentati dall'interessato o dall'ente, organizzazione o associazione; conduce procedimenti riguardanti l'applicazione del GDPR, emette decisioni, e se è proporzionato - determina l'importo delle sanzioni amministrative per le violazioni del GDPR e le impone.	https://uodo.gov.pl/
Il Centro "GovTech"	Il centro GovTech ha assunto alcune delle responsabilità del Ministero della digitalizzazione, che è stato liquidato nell'autunno 2020. I destinatari diretti dei servizi GovTech sono l'amministrazione locale e centrale in senso lato, così come altri enti che svolgono compiti pubblici, come ospedali, scuole o aziende di trasporto. I destinatari dei servizi GovTech sono il settore pubblico ma anche le aziende.	https://www.gov.pl/web/govtech
Fondazione "Panoptykon"	La Fondazione Panoptykon monitora le pratiche di sorveglianza. Esamina la legge in vigore, i procedimenti legislativi, le azioni delle autorità pubbliche e delle imprese private. Segue i rapporti dei media e della società civile. Analizzano le informazioni raccolte, diagnosticano i problemi e reagiscono. Danno la loro opinione sulle proposte di nuove leggi, sollevano obiezioni alle leggi esistenti e le loro proposte di cambiamento. Segnalano abusi e negligenze.	www.panoptykon.org
Państwowy Instytut Badawczy NASK	NASK - un istituto di ricerca statale supervisionato dalla Cancelleria del Primo Ministro. La sua missione è quella di cercare e implementare soluzioni che servono allo sviluppo delle reti ICT in Polonia e al miglioramento della loro efficacia e sicurezza. L'istituto conduce ricerche scientifiche, lavori di sviluppo, così come attività operative a beneficio della sicurezza del cyberspazio civile polacco. Un altro elemento importante dell'attività del	www.nask.pl

	NASK è l'educazione degli utenti e la promozione del concetto di società dell'informazione, soprattutto per proteggere i bambini e i giovani dalle minacce legate all'uso delle nuove tecnologie.	
ZFODO (Associazione delle aziende per la protezione dei dati personali)	Le aziende associate nell'Associazione delle aziende di protezione dei dati personali hanno molti anni di esperienza nella consulenza aziendale nel campo della protezione dei dati personali. Forniscono servizi professionali al più alto livello alle più grandi aziende del settore privato, così come alle unità governative locali e centrali. Hanno esperienza in una vasta gamma di settori e industrie, il che permette loro di offrire ai loro clienti soluzioni individuali su misura per le loro esigenze. Hanno molti partner commerciali - studi legali, IT e consulenze di marketing. Questo permette loro di consigliare i loro clienti in modo completo - non solo nell'ambito della protezione dei dati, ma nell'ambito degli affari generali dei loro clienti.	www.zfodo.org.pl
Fondazione „Wiedza To Bezpieczeństwo”	La Fondazione divulga la conoscenza nel campo della sicurezza informatica. Organizza conferenze scientifiche, aiuta a risolvere i problemi che la gente affronta nella vita quotidiana, sia nel privato che negli affari. Conduce campagne sociali di sensibilizzazione. In questo modo mostriamo quali pericoli sono minacciati in relazione all'uso illegale dei nostri dati personali.	https://wtb.org.pl/

Tabella 1: Lista degli Stakeholder della Polonia.

Tra gli errori più comuni in relazione all'implementazione del RODO (equivalente polacco del GDPR) nelle aziende polacche secondo il rapporto "10 biggest mistakes in ensuring compliance with RODO" ZFODO cita più spesso:

- Incomprensione dell'idea di RODO, cioè implementarla solo "sulla carta". Di conseguenza, nessuno conosce e segue le sue procedure. La mancata attuazione può comportare sanzioni da parte dell'autorità di vigilanza.

- Mancanza di un'adeguata consapevolezza della sicurezza delle informazioni. Conduzione dell'analisi dei rischi da parte di personale non qualificato o con poca esperienza, con il risultato di un'analisi mancante o condotta in modo errato. Il risultato sono minacce non identificate, possibilità di perdita di dati, mancanza di sicurezza.

- Area IT inadeguata, mancanza di una politica di conservazione dei dati identificata o mancanza di implementazione delle regole di conservazione nei sistemi ICT. Il risultato può essere la perdita di dati o l'accesso non autorizzato ai dati, e l'incapacità di realizzare i diritti a cui i dati si riferiscono.

Inoltre, sono stati menzionati i seguenti: errata valutazione dell'impatto sulla protezione dei dati, mancata regolamentazione della relazione di affidamento dei dati tra entità, confusione tra i concetti di controllore e processore, mancata attuazione della procedura di obbligo di informazione, mancanza di un coordinatore per l'attuazione delle procedure, mancanza di consapevolezza tra i dipendenti, mancanza di una visione olistica dell'attuazione.

Le aree sopra menzionate sono i "peccati principali", ma ci sono anche altri aspetti dell'attuazione dei nuovi regolamenti che si sono rivelati problematici.

Per esempio, il ruolo del responsabile della protezione dei dati è molto spesso sottovalutato e la sua posizione nell'organizzazione è bassa. Spesso il DPO è una persona "scelta a mano". Il ruolo del DPO è spesso sottovalutato e la sua posizione nella struttura organizzativa è bassa. Il DPO è spesso reclutato, non ha qualifiche appropriate e ha poca influenza sulle decisioni prese dal top management, la sua voce è trattata solo come una voce consultiva. Il rapporto è pubblicato in polacco da ZFODO (2020).

Le informazioni su come RODO è stato implementato nella pratica e l'entità delle violazioni e degli incidenti relativi alla protezione dei dati personali tra le aziende e le istituzioni polacche sono raccontate, tra l'altro, in un rapporto preparato dall'Associazione delle aziende di protezione dei dati (ZFODO).

Il rapporto ha riguardato 454 organizzazioni servite da Aziende affiliate a ZFODO nel periodo maggio 2019-maggio 2020. Tra gli intervistati c'erano organizzazioni e aziende sia del settore privato che pubblico. Le statistiche mostrano che un incidente (data protection incident) si verifica al controllore medio statisticamente 0,65 volte all'anno. Questa è una quantità insufficiente per acquisire la pratica necessaria per evitare o gestire tali incidenti, mentre un errore nella gestione anche di un solo incidente può avere conseguenze disastrose per il business.

Il rapporto mostra che quasi il 70% degli incidenti, non sono stati segnalati all'autorità di vigilanza. Secondo l'articolo 33(1) del RODO, si può non segnalare un incidente all'autorità di vigilanza se "è improbabile che la violazione comporti un rischio di violazione dei diritti o delle libertà delle persone fisiche". Nel 70% dei casi, le persone interessate da questi incidenti non sono state informate. Indipendentemente dalla notifica dell'incidente all'autorità di controllo, secondo l'articolo 34 del RODO, "se una violazione dei dati personali può comportare un rischio elevato di violazione dei diritti o delle libertà delle persone fisiche", allora dobbiamo informare anche le persone interessate.

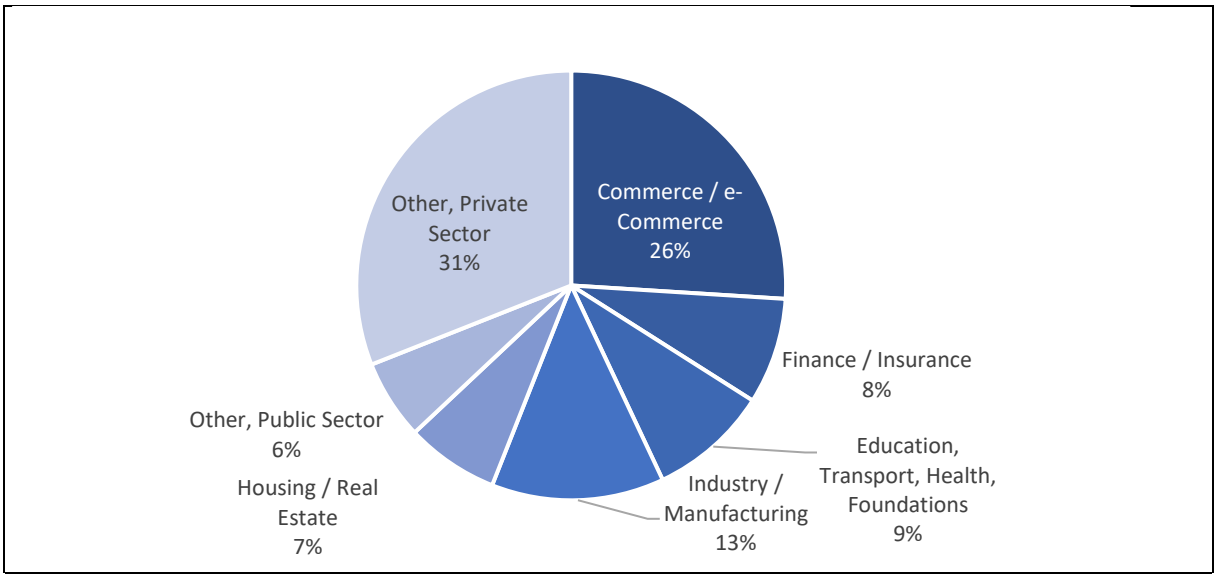

Figura 1: Industrie/rami più a rischio di violazione dei dati personali
Fonte: ZFODO (2021), nostra illustrazione.

Le fonti delle violazioni dei dati personali sono state localizzate sia all'interno dell'azienda/istituzione (68%), sia all'esterno (20%), così come provengono dal cosiddetto processore, cioè un'entità che elabora i dati per conto del controllore (12%). Quelli esterni includono, per esempio, ex dipendenti o hacker, quelli interni - dipendenti e collaboratori dell'organizzazione.

Nel 92% dei casi si è trattato di incidenti involontari (e-mail mal indirizzate, mancanza di una copia nascosta, invio di corrispondenza tradizionale con contenuto errato). Gli incidenti intenzionali includevano: furto di computer portatili o altri supporti di dati, phishing, condivisione di dati con persone non autorizzate. Quasi il 96% degli incidenti sono stati causati da motivi personali. Questi includevano l'azione di un fattore umano. Le cause non personali sono situazioni in cui la violazione è stata causata da un malfunzionamento della tecnologia, situazioni fuori dal controllo della volontà umana.

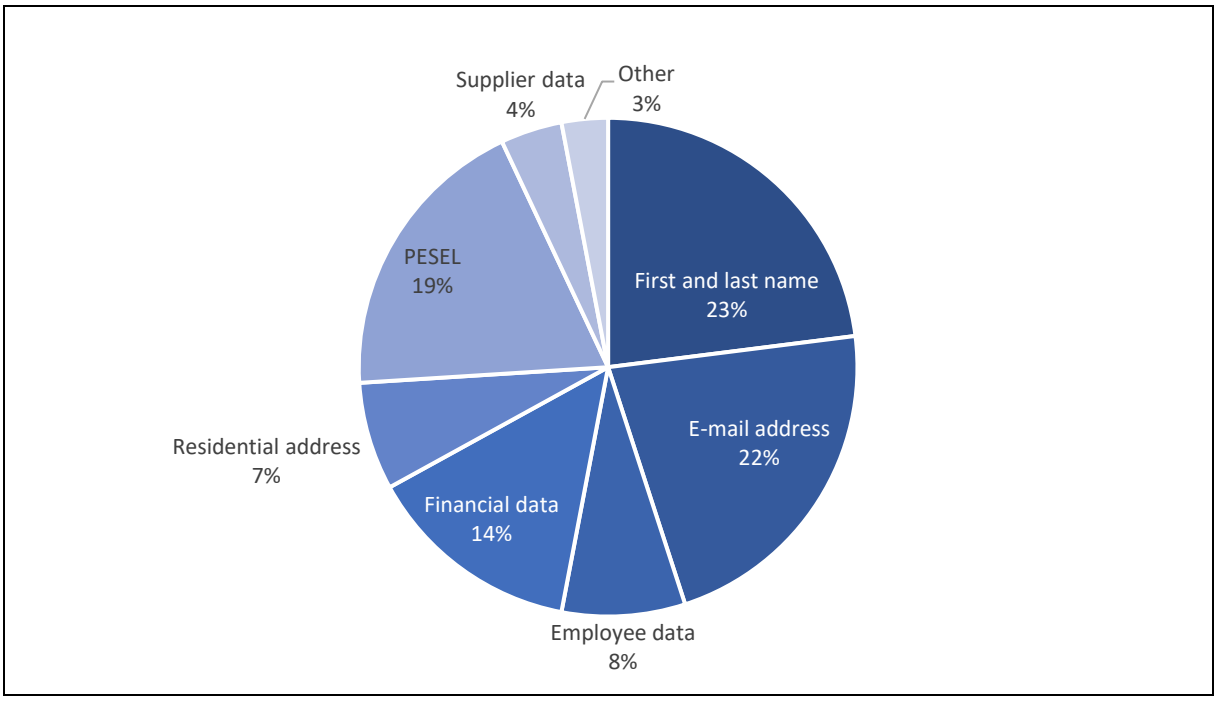

Figura 2: Categorie di dati più frequentemente violate.
Fonte: ZFODO (2021), nostra illustrazione.

Per quanto riguarda la protezione dei dati personali dei dipendenti, purtroppo non è stato trovato alcun rapporto che analizzi la portata e le situazioni più comuni relative a questo tema in Polonia. Per facilitare il processo di assunzione e facilitare la navigazione tra i regolamenti, l'UODO (Ufficio per la protezione dei dati personali) ha rilasciato una pubblicazione intitolata "Protezione dei dati personali sul posto di lavoro. Linee guida per i titolari".

2.2 Austria

Nome dell'istituzione	Breve descrizione	Obiettivi principali	Sito web
WKO – Camera di commercio austriaca	La WKO invita le aziende a sviluppare una strategia di sicurezza appropriata che protegga dalle potenziali minacce.	La sensibilizzazione dei dipendenti è un importante fattore di sicurezza. È stato istituito un dipartimento separato per la sicurezza informatica e la sicurezza dei dati. Le PMI sono sostenute da varie iniziative.	https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
Autorità austriaca per la protezione dei dati	L'autorità austriaca per la protezione dei dati è l'autorità nazionale di controllo per la protezione dei dati nella Repubblica d'Austria.	Il sistema d'informazione giuridica della Repubblica d'Austria (www.ris.bka.gv.at) fornisce la legislazione austriaca nella sua versione attuale (federale e statale), le gazzette legali (federale e statale) e la giurisprudenza.	www.dsb.gv.at
BFI Vienna Formazione sulla protezione dei dati e sicurezza informatica	Offre formazone sulla protezione dei dati e sicurezza informatica	Come istituto di formazione continua riconosciuto dallo Stato, il BFI è autorizzato a rilasciare certificazioni e a presentare procedure di riconoscimento per corsi di formazione non formale all'organo di coordinamento NQF (NKS) - o attraverso i suoi Service Point.	https://www.bfi.wien/edv-und-informationstechnologien/datenschutz-und-informationssicherheit/
Piattaforma KMU	Questa rete di esperti dell'economia e della tecnologia è stata fondata per sostenere le PMI in Austria al fine di accompagnare le aziende nel cambiamento digitale.	Oltre a molti altri servizi, vengono offerti workshop su una vasta gamma di argomenti. Lo slogan "Il terreno comune sostituisce la dimensione" rende chiaro che l'attenzione è sulla cooperazione tra piccole imprese, che a loro volta creano un vantaggio competitivo per se stesse.	https://www.kmu-plattform.eu/
Agenzia di digitalizzazione	All'interno del FFG, l'agenzia per la promozione della ricerca, la "Digitization Agency" è stata creata per assegnare sovvenzioni alle PMI - piccole e medie imprese - in Austria al fine di	Per permettere soprattutto alle piccole e medie imprese (PMI) austriache di sfruttare al meglio le loro opportunità di digitalizzazione, l'"Iniziativa KMU DIGITAL" fornisce un aiuto concreto: Le aziende beneficiano di sovvenzioni per la consulenza, la qualificazione, il trasferimento di conoscenze e la formazione continua.	https://www.ffg.at/dia

	promuovere la digitalizzazione in modo mirato.		
Vienna Business Agency /	Il programma di finanziamento "Wien Digital" sostiene le medie aziende e le PMI nella realizzazione di misure di digitalizzazione.	La Vienna Business Agency offre una consulenza personale e ha una vasta rete di PMI e partner di cooperazione (pubblici). Startup, imprese individuali, piccole e medie imprese nazionali e internazionali o società sono supportate in questioni importanti.	https://wirtschaftsagentur.at/
Business Circle	Fornitore del corso di formazione per un responsabile della protezione dei dati certificato	Le qualifiche acquisite nel corso sono confermate con il certificato degli standard austriaci secondo i criteri della ISO/IEC 17024 dopo un esame finale valutato positivamente.	https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/
1a Beratung e.U. - Ing. Roland Fürbas	Fornitore privato per corsi di formazione GDPR & sicurezza informatica	Sicurezza dati e IT / DSGVO-DSB / Sviluppo degli affari / Servizi online	http://www.1a-beratung.eu
72solutions	Fornitore privato per corsi di formazione GDPR & sicurezza informatica	GDPR - Esperti che forniscono consulenza e sviluppano soluzioni su misura per le misure di protezione dei dati.	https://www.72solutions.eu
TÜV Austria Accademia	Fornitore di corsi di formazione sulla protezione dei dati - esperto di GDPR	Ci sono circa 20 corsi in offerta, che sono strutturati secondo il settore.	https://www.tuv-akademie.at/kursprogramm?s=Datenschutz

Tabella 2: Lista degli Stakeholder dell'Austria.

L'Austria è stato uno dei primi paesi europei con un'autorità per la protezione dei dati, la Commissione per la protezione dei dati. È stata creata con la prima legge sulla protezione dei dati, Gazzetta Ufficiale Federale No. 565/1978. La direttiva europea sulla protezione dei dati 95/46/CE ha posto la legge sulla protezione dei dati su una nuova base in tutta Europa (EUR-LEX 1995). In Austria, questa direttiva è stata attuata dalla legge sulla protezione dei dati del 2000 (DSG 2000) (Rechtsinformationssystem des Bundes (RIS) 1999). Dopo il 25 maggio 2018, il regolamento sulla protezione dei dati di base (GDPR; DSGVO) ha messo la legge sulla protezione dei dati su una nuova base in tutta Europa EUR-LEX (1995). In Austria, questa direttiva è stata attuata dalla legge sulla protezione dei dati del 2000 (DSG 2000) Rechtsinformationssystem des Bundes (RIS) (1999). Dopo il 25 maggio 2018, il regolamento di base sulla protezione dei dati (GDPR; DSGVO) (Ministero

federale delle finanze (BMF)) e la legge riveduta sulla protezione dei dati (DSG) (Ministero federale delle finanze (BMF)) costituiscono la base del diritto sulla protezione dei dati (vedi DSB 2019).

Secondo il codice commerciale austriaco (UGB) e la legge sulle società a responsabilità limitata (GmbHG), la responsabilità della protezione dei dati e della sicurezza informatica è sempre della direzione. Anche se i compiti IT rilevanti per la sicurezza sono affidati ai dipendenti, la responsabilità ultima del rispetto delle disposizioni di legge spetta alla direzione dell'azienda. Con la direttiva NIS (UE) 2016/1148 (EUR-LEX), che è stata attuata in Austria alla fine del 2018 con la legge sulla sicurezza delle reti e dei sistemi informativi (NISG), per la prima volta ci sono regolamenti completi nel settore della sicurezza informatica per aziende strategicamente importanti, fornitori di servizi digitali e autorità a livello europeo e nazionale. Le aziende devono adottare misure tecniche e organizzative appropriate (ad esempio backup dei dati, crittografia, controlli di accesso) per proteggere i dati dalla distruzione accidentale, dalla perdita di dati o dall'uso illegale da parte di terzi. In caso contrario, possono essere comminate pesanti multe.

Il regolamento generale sulla protezione dei dati dell'UE (GDPR) e la legge austriaca sulla protezione dei dati regolano il trattamento dei dati personali (ad esempio nome, data di nascita, indirizzo e-mail, indirizzo IP). Questo significa che tutti gli imprenditori in Austria sono vincolati da norme legali. Di regola, le aziende che hanno raggiunto un certo livello di digitalizzazione le conoscono bene e vengono regolarmente informate, soprattutto dalla Camera di Commercio. Le micro-imprese, che spesso danno meno importanza ai temi dell'IS e del DP per ragioni di tempo e di costi, sono più problematiche.

Particolarmente problematica sembra essere la questione del dovere di informare secondo il GDPR, che, secondo Conrad Lienhardt, spesso non viene applicato in Austria, soprattutto nelle piccole aziende: "Secondo il regolamento generale sulla protezione dei dati (GDPR), i diritti degli interessati, cioè di coloro i cui dati personali vengono trattati, includono un ampio diritto all'informazione. Da parte delle aziende e delle organizzazioni, questo significa ampi obblighi di informazione. Questi sono regolati negli articoli 13 e 14 del GDPR". Lienhardt avverte di non sottovalutare il dovere di informare: "Ci sono aziende e organizzazioni che ottengono dati personali da banche dati pubbliche, come i registri fondiari, gli elenchi di indirizzi, ecc. e poi li elaborano. Molti pensano che non sono soggetti al dovere di informare, soprattutto perché, inoltre, il "trafugamento" di dati da elenchi pubblici molto spesso coinvolge grandi quantità di dati personali. C'è da aspettarsi denunce e azioni private per danni. Perciò: Prendete sul serio il dovere di informare". (Lienhardt 2020).

I dati dei dipendenti secondo il regolamento generale sulla protezione dei dati dell'UE: In Austria non si applica solo la legge sulla protezione dei dati, ma anche le disposizioni del diritto del lavoro e sociale, come sottolinea la WKO: "Si dovrebbe verificare qui su quale base vengono trattati i dati (obbligo legale, necessario per l'esecuzione del contratto di servizio, consenso?) [...] Poiché il contabile delle paghe di solito agisce sulla base di un rapporto di elaborazione contrattuale con il cliente (=

parte responsabile) e il cliente ha l'obbligo di pagare correttamente anche sulla base del rapporto di lavoro, non è necessario il consenso del rispettivo dipendente del cliente per questo. Tuttavia, è necessario stipulare un contratto scritto di elaborazione dell'ordine". (Wirtschaftskammer Österreich 2021b).

La WKO (Wirtschaftskammer Österreich), la Camera di Commercio austriaca, offre anche un supporto per l'attuazione del GDPR con informazioni specifiche per il settore, guide, documenti campione e liste di controllo. La guida sulle misure tecniche e organizzative nel contesto del GDPR fornisce una panoramica pratica di quali misure tecniche di sicurezza sono necessarie e utili e come possono essere implementate in azienda. (c. f. Wirtschaftskammer Österreich (2020)) Infine, "IT Safe" della WKO (Wirtschaftskammer Österreich 2021a) è un'iniziativa ben consolidata e conosciuta per sostenere le PMI nell'attuazione delle misure di sicurezza informatica.

Le aziende in Austria hanno a disposizione numerose fonti di informazione sul GDPR. Tuttavia, è naturale che questi testi legali molto estesi non possono essere afferrati a colpo d'occhio. A questo proposito, i servizi della Camera Economica Federale Austriaca dovrebbero essere evidenziati, che è un importante punto di contatto per tutte - e specialmente per le piccole - imprese. Con "IT Safe" è stata sviluppata una guida completa e vengono offerti numerosi eventi informativi gratuiti. Un'offerta particolarmente importante è un sito web professionale che presenta le basi più importanti del GDPR in modo comprensibile (c.f. Wirtschaftskammer Österreich (2021b))

Un'altra offerta interessante è quella di KSV (Kreditschutzverband), che fornisce alle aziende un supporto economico per l'introduzione del GDPR su diversi livelli: consulenza, formazione e l'app "DSVGO Assistant" (KSV1870).

Nonostante tutti gli sforzi, alla gente in Austria piace ancora parlare del "non amato GDPR"! Abbiamo trovato il seguente - dal nostro punto di vista - appropriato comunicato stampa:

La sobria realtà nelle aziende austriache

In questo comunicato stampa dell'APA (l'agenzia di stampa austriaca) del maggio 2020, si riferisce dell'attuazione del GDPR dell'UE in Austria sotto il titolo: "Comprensione sì, attuazione lenta".

"Nonostante la sensibilità notevolmente aumentata in materia di protezione dei dati, il regolamento dell'UE è stato pienamente implementato solo dal 2018 dal 30% delle imprese nazionali." L'articolo sottolinea il fatto che due anni dopo l'entrata in vigore del regolamento generale sulla protezione dei dati dell'UE (GDPR), le imprese austriache mostrano una comprensione significativamente maggiore del tema della protezione dei dati. In un sondaggio KSV1870, condotto prima della crisi Corona, nell'ambito dell'Austrian Business Check nel febbraio 2020 con circa 600 aziende, il 40% delle aziende intervistate ha dichiarato che negli ultimi tre anni questa è aumentata "su tutta la linea". L'indagine ha mostrato chiaramente che c'è ancora del lavoro da fare prima che il GDPR dell'UE sia pienamente implementato da tutte le

aziende in Austria, dopo che solo il 30% degli intervistati lo ha completamente ancorato nelle loro operazioni finora. La misura più frequentemente attuata per aumentare la protezione dei dati è stata nominata dal 46% dei partecipanti al sondaggio come l'introduzione o l'adattamento delle misure di protezione dei dati e di sicurezza informatica. Come nota positiva, l'autore menziona che la comprensione per una gestione fiduciosa e consapevole delle informazioni nelle aziende austriache è aumentata significativamente negli ultimi tre anni. (Austrian Press Agency 2020) sottolinea il fatto che due anni dopo l'entrata in vigore del regolamento generale sulla protezione dei dati dell'UE (EU GDPR), le aziende austriache mostrano una comprensione significativamente maggiore del tema della protezione dei dati. In un sondaggio KSV1870, condotto prima della crisi di Corona, nell'ambito dell'Austrian Business Check nel febbraio 2020 con circa 600 aziende, il 40% delle aziende intervistate ha dichiarato che negli ultimi tre anni la comprensione è aumentata "su tutta la linea". L'indagine ha mostrato chiaramente che c'è ancora del lavoro da fare prima che il GDPR dell'UE sia completamente implementato da tutte le aziende in Austria, dopo che solo il 30% degli intervistati lo ha completamente ancorato nelle loro operazioni finora. La misura più frequentemente attuata per aumentare la protezione dei dati è stata nominata dal 46% dei partecipanti al sondaggio come l'introduzione o l'adattamento delle misure di protezione dei dati e di sicurezza informatica. Come nota positiva, l'autore menziona che la comprensione per una gestione fiduciosa e consapevole delle informazioni nelle aziende austriache è aumentata significativamente negli ultimi tre anni. (Agenzia di stampa austriaca 2020.

"Così, il 40% delle aziende nazionali conferma che questo sviluppo ha avuto luogo "su tutta la linea" - un altro 32% vede un aumento almeno in aree parziali. Mentre per il 19% un miglioramento non è distinguibile, per il 2% è addirittura diminuito". Il 7% degli intervistati non ha dato alcuna specificazione. (Agenzia di stampa austriaca, 2020). C'è spesso un notevole divario tra la comprensione e l'effettiva attuazione delle necessarie misure di protezione dei dati. Soprattutto in tempi di crescente digitalizzazione a causa della crisi della Corona, è particolarmente preoccupante che nemmeno un terzo delle aziende nazionali abbia attuato pienamente il GDPR dell'UE", spiega Ricardo-José Vybiral, MBA, CEO di KSV1870 Holding AG. Questo include, tra le altre cose, il richiesto "registro delle operazioni di trattamento", che solo il 34% delle aziende intervistate ha implementato con successo finora.

Deloitte Services Wirtschaftsprüfungs GmbH (2020) ha anche pubblicato uno studio sul grado di attuazione del GDPR nelle aziende austriache all'inizio del 2020. 191 rappresentanti aziendali in posizioni esecutive sono stati intervistati in un sondaggio online: "Il risultato: la maggior parte delle aziende sono ancora impegnate nell'attuazione dei requisiti e vedono la loro conformità a lungo termine come una sfida. Ma l'importanza del tema è stata riconosciuta: Quasi tutti gli intervistati ora tengono conto dei requisiti di protezione dei dati quando prendono decisioni aziendali". Anche Deloitte Services Wirtschaftsprüfungs GmbH (2020) ha pubblicato uno studio sul grado di attuazione del GDPR nelle aziende austriache all'inizio del 2020. 191 rappresentanti aziendali in posizioni esecutive sono stati intervistati in un

sondaggio online: "Il risultato: la maggior parte delle aziende sono ancora impegnate nell'attuazione dei requisiti e vedono la loro conformità a lungo termine come una sfida. Ma l'importanza del tema è stata riconosciuta: Quasi tutti gli intervistati ora tengono conto dei requisiti di protezione dei dati quando prendono decisioni aziendali".

Analogamente a KSV, anche Deloitte conclude che il livello di piena attuazione del GDPR nelle aziende austriache è poco meno di un terzo: "La maggior parte delle aziende (54%) è ancora in dirittura d'arrivo nell'attuazione del GDPR UE, come un anno fa. Mentre quasi un terzo (32%) degli intervistati ha ora completato l'implementazione della direttiva, circa il 12% è ancora nel mezzo del processo e ha un bisogno acuto di recuperare il ritardo." Deloitte afferma nel rapporto che non ci dovrebbero più essere scuse per non aver implementato la direttiva. Si raccomanda urgentemente che le aziende interessate affrontino attivamente questo problema e, se necessario, cerchino un aiuto esterno per accelerare l'attuazione.

Alla domanda sullo stato di attuazione del GDPR, le aziende hanno risposto come segue:

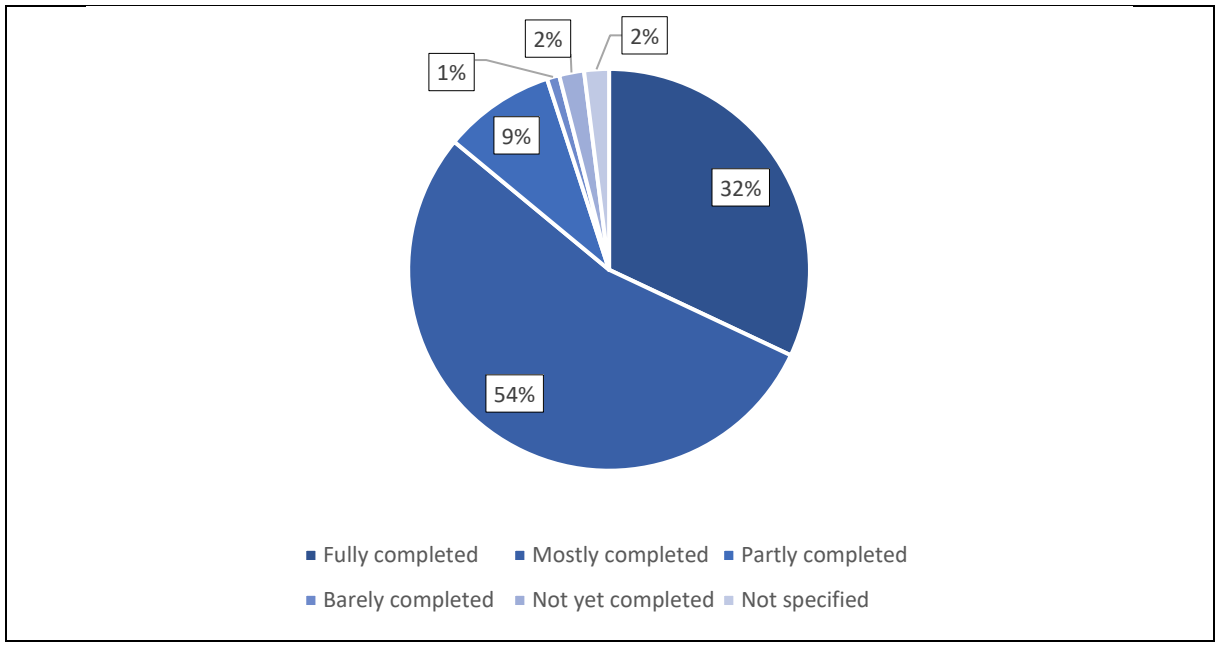

Figura 3: Implementazione del GDPR in Austria

Fonte: nostra Illustrazione. Dati usati da Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Nel 2020, come è stato riportato dai media, c'è stato un aumento delle multe per il mancato rispetto delle norme sulla protezione dei dati. Deloitte ha quindi chiesto alle aziende come queste notifiche hanno influenzato il comportamento in azienda: "Solo in un quarto delle aziende le decisioni dell'autorità di protezione dei dati hanno avuto un'influenza sulla gestione del GDPR dell'UE finora. Di queste, la maggioranza ha utilizzato i risultati per valutare o migliorare lo stato nella propria azienda." La domanda era formulata come segue: Le recenti decisioni dell'autorità austriaca per la protezione dei dati hanno influenzato il vostro approccio al GDPR dell'UE?

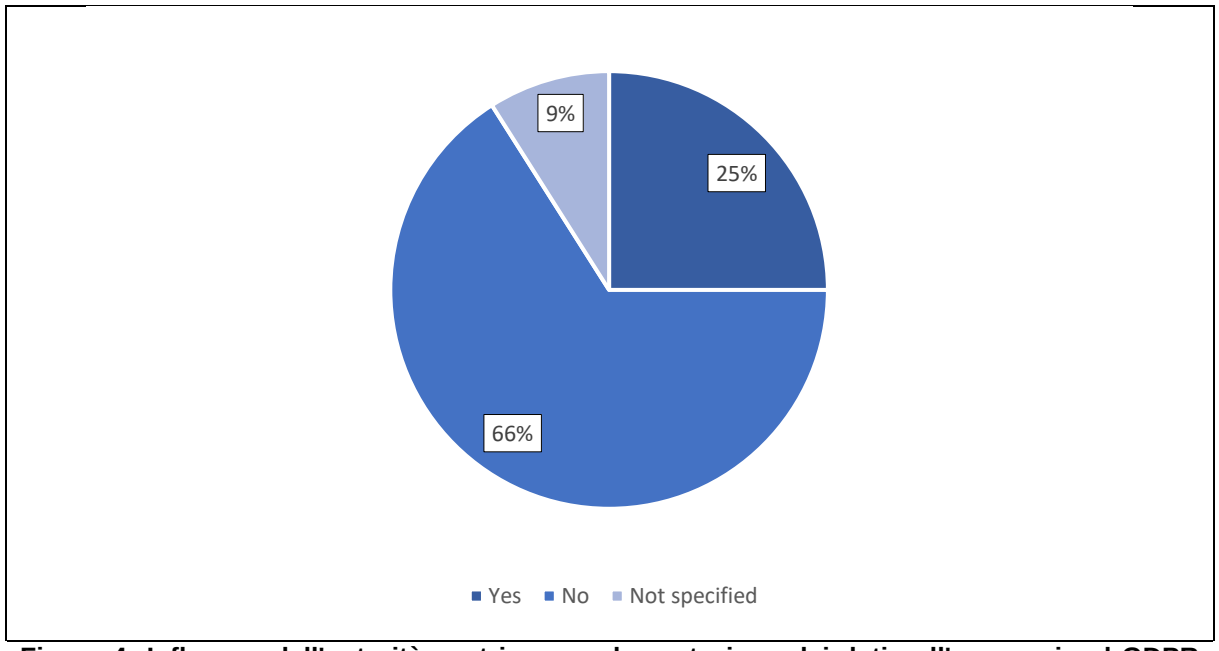

Figura 4: Influenza dell'autorità austriaca per la protezione dei dati sull'approccio al GDPR dell'UE

Fonte: nostra Illustrazione. Dati usati da Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Lo studio di Deloitte sottolinea che molte aziende in Austria hanno purtroppo fallito nel fare i loro compiti negli ultimi anni. Spesso manca una classificazione strutturata dei dati, che ridurrebbe significativamente lo sforzo. La seguente valutazione della prossima domanda è interessante: Quanto sforzo stima che ci vorrà per conformarsi ai requisiti del GDPR dell'UE in futuro?

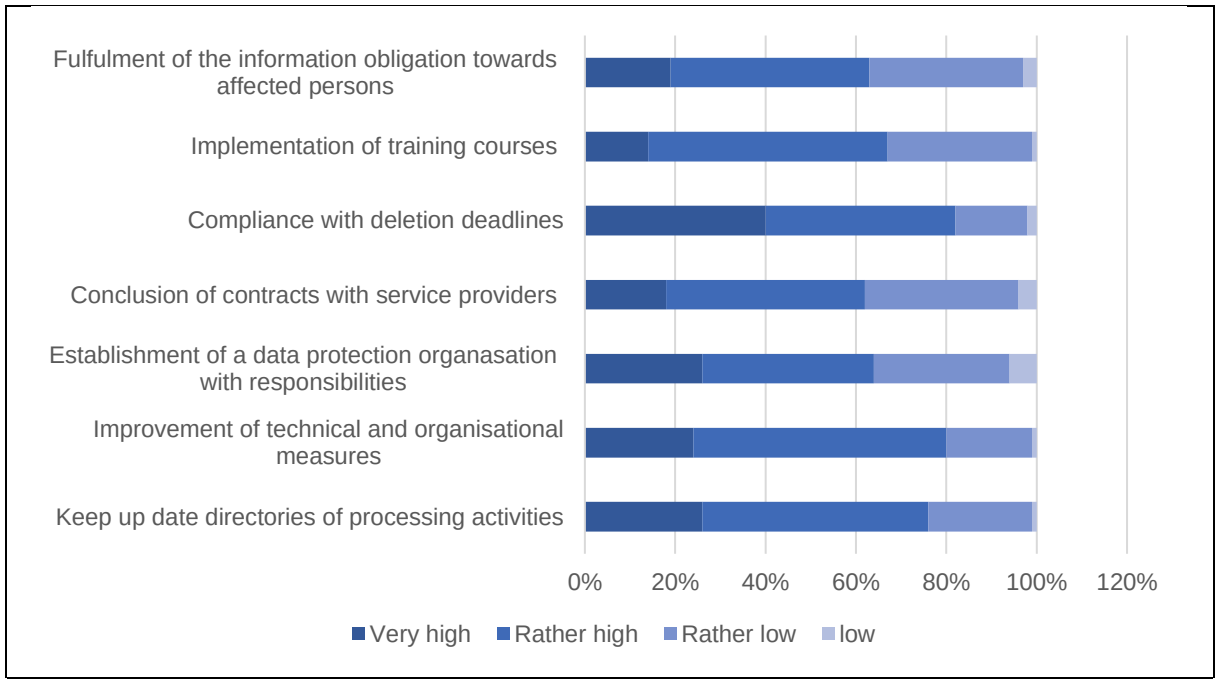

Figura 5: Sforzi potenzialmente spesi per conformarsi ai requisiti del GDPR dell'UE

Fonte: nostra Illustrazione. Dati usati da Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Il rapporto mostra che per la maggior parte delle aziende, la conformità a lungo termine con il GDPR è vissuta come una sfida. Gli intervistati percepiscono lo sforzo maggiore nel considerare i termini di cancellazione.

Un'altra domanda interessante di Deloitte è se ci sono abbastanza dipendenti formati per i compiti di protezione dei dati: "Più di un quarto delle aziende intervistate non ha le risorse umane per conformarsi al GDPR dell'UE e implementare il lavoro relativo. Questo rende un altro supporto ancora più importante: così, sempre più aziende austriache si rivolgono al supporto tecnologico per essere in grado di soddisfare i requisiti del GDPR dell'UE. Mentre il 39% non aveva uno strumento l'anno scorso, attualmente è intorno al 30%".

Il rapporto Deloitte conclude: "Dopo le incertezze iniziali, le aziende austriache hanno un quadro molto più chiaro della necessità di azione esistente. Tuttavia, alcuni dei temi chiave identificati comportano cambiamenti completi. Anche la cultura aziendale è interessata". Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Dal punto di vista di Hafelekar possiamo riassumere la situazione in Austria come segue: Si può dire che ci sono leggi chiare in Austria sul tema dell'implementazione del GDPR, anche se non sono sempre formulate in modo facile da capire. Ci sono diversi enti pubblici, primo fra tutti la WKO, a cui le aziende possono rivolgersi per avere supporto nell'attuazione del GDPR.

In Austria, la responsabilità per tutti i comportamenti scorretti riguardo alla protezione dei dati e alla sicurezza informatica è della direzione, anche se delegano i compiti ai dipendenti.

L'implementazione non funziona ancora in modo soddisfacente e come abbiamo già stabilito con il nostro gruppo di esperti in Austria, la mancanza di tempo nelle PMI è probabilmente decisiva per questa lenta implementazione.

In ogni caso, secondo il nostro gruppo direttivo TeBeISi, c'è un grande interesse in Austria per un'ulteriore formazione accessibile sui temi della protezione dei dati e della sicurezza informatica. C'è ancora molto lavoro da fare.

2.3 Germania

Nome dell'istituzione	Breve descrizione	Obiettivi principali	Sito web
Deutsche Vereinigung für Datenschutz e.V. (DVD)	Il DVD è responsabile della pubblicazione di messaggi relativi alla protezione dei dati (DANA). Anche le relazioni pubbliche e il lavoro con i media su temi attuali, le conferenze stampa e i comunicati stampa fanno parte dei compiti. Inoltre, vengono organizzati incontri in collaborazione con organizzazioni partner e seminari. Il DVD partecipa anche ai premi annuali del Grande Fratello.	Il DVD ha lo scopo di consigliare e informare il pubblico sui rischi dell'uso del trattamento elettronico dei dati e la possibile restrizione del diritto all'autodeterminazione informativa.	https://www.datenschutzverein.de
Gesellschaft für Datenschutz und Datensicherheit (GDD)	Fondato nel 1977, il GDD conta oggi più di 3.800 membri. Ci sono 34 circoli per lo scambio di nuove esperienze a livello nazionale con più di 3.500 partecipanti e più di 10.000 responsabili della protezione dei dati sono già stati formati nell'accademia GDD.	La protezione dei dati, la sicurezza dei dati e la corretta elaborazione dei dati hanno lo scopo di proteggere tutte le parti interessate dal pericolo e di garantire la libertà di informazione e l'equilibrio delle informazioni. Gli obblighi legali riguardano tutte le aziende e le unità amministrative, indipendentemente dalle dimensioni e dal settore. Il GDD vuole dare un contributo importante.	https://www.gdd.de/
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfG)	Circa 700 persone della scienza e della pratica lavorano alla FIfG, specialmente professionisti dell'informatica e della tecnologia dell'informazione. L'obiettivo è di permettere uno scambio tra tutti coloro che si	La FiFG mette in guardia il pubblico sugli sviluppi dannosi nel campo della sicurezza dell'informazione. Inoltre, l'associazione combatte contro l'uso della tecnologia dell'informazione per il controllo e la sorveglianza. FiFG sostiene anche la parità di diritti per le persone con disabilità nella progettazione e nell'uso della tecnologia dell'informazione e lavora per combattere la discriminazione contro le donne	https://www.fiff.de/

	occupano di informatica e tecnologia dell'informazione. La FIFG è aperta a tutti coloro che vogliono partecipare o semplicemente informarsi.	nell'informatica.	
Digitalcourage e.V.	L'associazione è stata fondata nel 1987. Tra le altre cose, Digitalcourage e.V. sostiene i diritti fondamentali e la protezione dei dati, svolge un lavoro educativo attraverso le relazioni pubbliche, ad esempio attraverso campagne e progetti, ed è responsabile per l'assegnazione annuale del BigBrotherAward.	Una parte importante del lavoro consiste nell'organizzazione di progetti e campagne, ma anche nell'organizzazione di congressi politici. Inoltre, l'associazione è a disposizione della stampa e dei media come oratori ed esperti in materia di protezione dei dati. L'obiettivo principale è quello di impegnarsi per i diritti fondamentali, la protezione dei dati e un mondo degno di essere vissuto nell'era digitale.	https://digitalcourage.de/
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDi)	I compiti principali dell'istituzione fondata nel 1978 sono il monitoraggio e l'applicazione del GDPR, il BDSG e altri regolamenti sulla protezione dei dati. Inoltre, si tratta di aumentare la consapevolezza e le relazioni pubbliche.	L'obiettivo principale è la salvaguardia e lo sviluppo della protezione dei dati. Dal 2006, chiunque consideri che il suo diritto di accesso alle informazioni secondo la legge sulla libertà d'informazione (IFG) sia stato violato, può rivolgersi all'Incaricato federale. La carica è attualmente ricoperta dal Prof. Ulrich Kelber.	https://www.bfdi.bund.de/

Tabella 3: Lista degli Stakeholder della Germania.

Il regolamento generale europeo sulla protezione dei dati (GDPR) è entrato in vigore il 24 maggio 2016. A partire dal 25 maggio 2018, i requisiti di protezione dei dati in esso contenuti sono obbligatori nei rispettivi stati membri anche senza una trasposizione separata nel diritto nazionale. Il regolamento europeo sulla protezione dei dati mira a rafforzare in particolare i diritti dei consumatori. Le agenzie di elaborazione dati devono aspettarsi regolamenti più severi. Il mancato rispetto del GDPR può costare all'azienda in questione fino a 20 milioni di euro di multa o fino al 4% del suo fatturato globale (a seconda di quale valore è più alto) (datenschutz 2021). Lo stato di attuazione del GDPR da parte delle aziende in Germania è

mostrato nella figura 3. La statistica è stata pubblicata nell'autunno dello scorso anno.

È lo studio più recente disponibile per quanto riguarda l'attuazione del GDPR. Al momento del sondaggio, il 37% degli intervistati ha dichiarato di aver già implementato le linee guida del GDPR.

Più della metà dei partecipanti ha dichiarato che la linea guida è parzialmente implementata o completamente implementata e stabilita per un ulteriore sviluppo (Statista 2020).Il regolamento generale europeo sulla protezione dei dati (GDPR) è entrato in vigore il 24 maggio 2016. A partire dal 25 maggio 2018, i requisiti di protezione dei dati in esso contenuti sono obbligatori nei rispettivi stati membri anche senza una trasposizione separata nel diritto nazionale.

Il regolamento europeo sulla protezione dei dati mira a rafforzare in particolare i diritti dei consumatori. Le agenzie di elaborazione dati devono aspettarsi regolamenti più severi. Il mancato rispetto del GDPR può costare all'azienda in questione fino a 20 milioni di euro di multa o fino al 4% del suo fatturato globale (a seconda di quale valore è più alto) Datenschutz (2021).

Lo stato di attuazione del GDPR da parte delle aziende in Germania è mostrato nella figura 3. La statistica è stata pubblicata nell'autunno dello scorso anno.

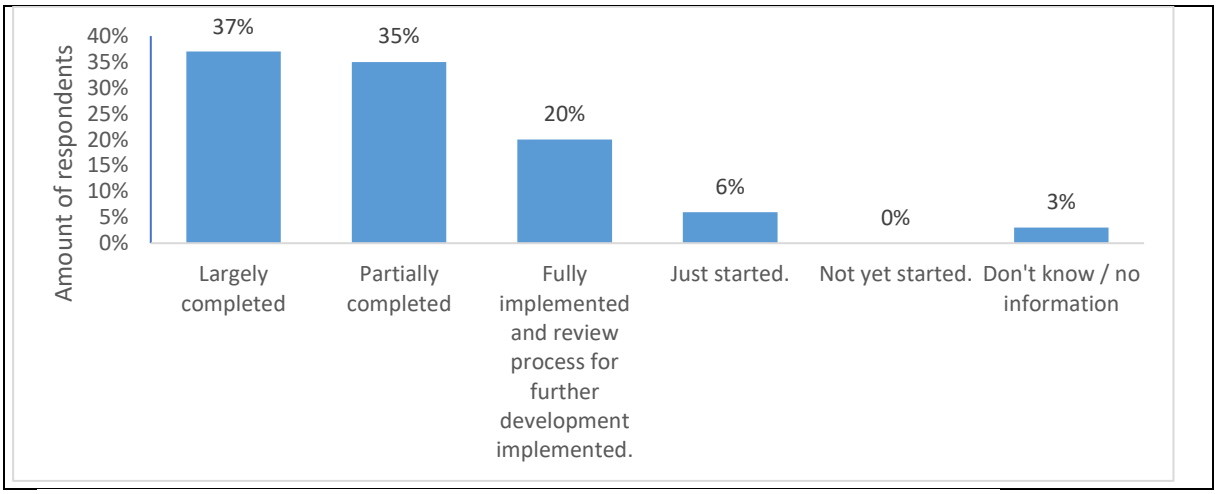

Figura 6: Stato di attuazione del GDPR da parte delle aziende in Germania (09/2020)

Considerando che sono passati circa 5 anni dalla pubblicazione e 3 anni dall'entrata in vigore, si può dedurre che gravi ostacoli impediscono alle imprese di attuare pienamente il GDPR. Le ramificazioni specifiche sono state dettagliate nello studio condotto da Bitkom e.V. (2020). Una delle ragioni per cui le aziende lottano con l'implementazione può essere attribuita alla grande quantità di sforzo necessario, a partire da una spesa extra iniziale (e singolare) (63%), l'aspettativa di una spesa extra permanente (rispetto allo stato giuridico precedente, 29%) e la necessità di personale extra (26%).

Il bisogno di personale si riflette anche nella decisione delle imprese di acquistare il servizio di protezione dei dati da fornitori di servizi, sia sotto forma di consulenza legale esterna (40%), consulenza esterna sulla protezione dei dati (31%) o revisioni esterne (28%). Tuttavia, il GDPR è percepito dalla maggioranza delle aziende come un contributo positivo al funzionamento e alla performance dell'azienda. Considerando l'effetto sugli ambienti competitivi uniformi in tutta l'UE (57%).

Di fronte ai complessi cambiamenti normativi, tuttavia, diversi aspetti suscitano dubbi sull'effetto positivo sull'attività economica. Tra gli altri, le preoccupazioni riguardanti il miglioramento a lungo termine dell'ambiente giuridico (43%), l'ostacolo all'innovazione (35%) e la complicazione dei processi aziendali (25%) diventano prevalenti. I rischi dell'implementazione del GDPR si riflettono anche nelle misure che ricevono più urgenza, come si può vedere nella figura 4.

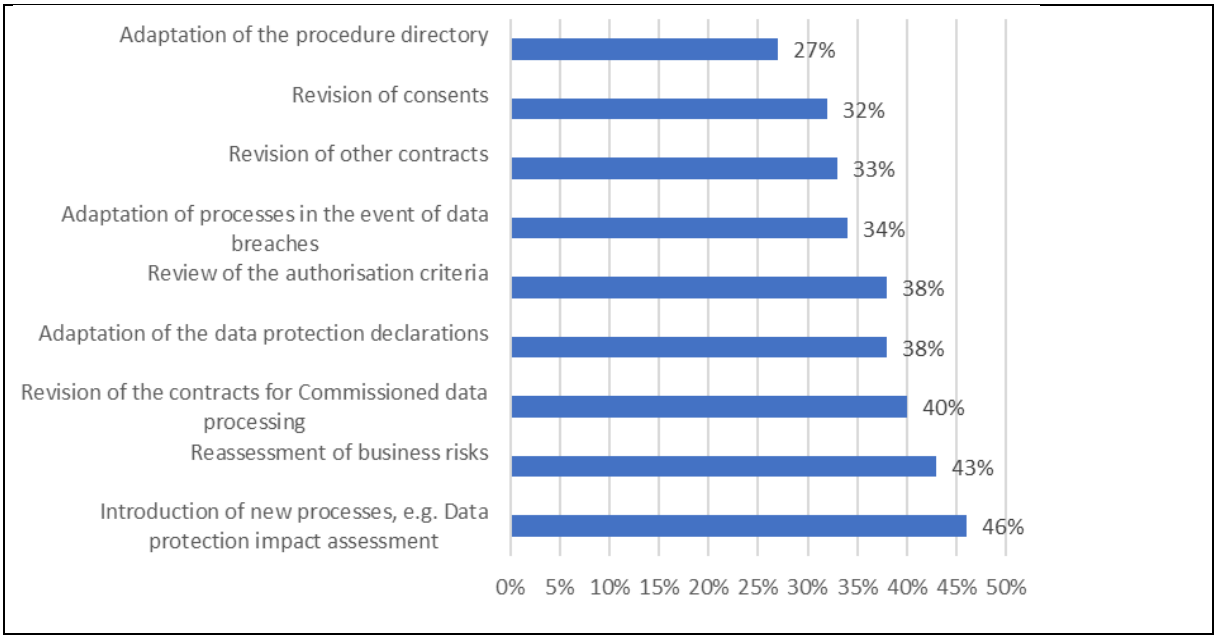

Figura 7: Quali misure per l'attuazione del GDPR implementerete con grande urgenza? Fonte: Bitkom e.V. (2020)

Uno studio condotto nel 2021 evidenzia una priorità generalmente alta della protezione dei dati in Germania, classificandola al secondo posto tra tutti i paesi europei nel trattamento generale e adeguato della protezione dei dati (heyData 2021). Di tutte le categorie considerate, è degno di nota il fatto che le "aziende" si collocano al livello più basso rispetto alle "forze dell'ordine", alla "competenza in materia di protezione dei dati" e al "sentimento pubblico", mentre i "privati" si collocano relativamente al livello più alto. Ogni categoria può essere scomposta in diversi criteri, che fanno luce su specifici punti di forza e di debolezza. Esaminando la situazione delle imprese, come si può vedere nella figura 5, diventa evidente che solo il 17% delle imprese ha una formazione continua obbligatoria rispetto al 24,29% della media UE. Una seconda grande lacuna rispetto al resto dell'UE diventa evidente in termini di protezione assicurativa, dove la Germania ottiene 4 punti in meno rispetto alla media UE.

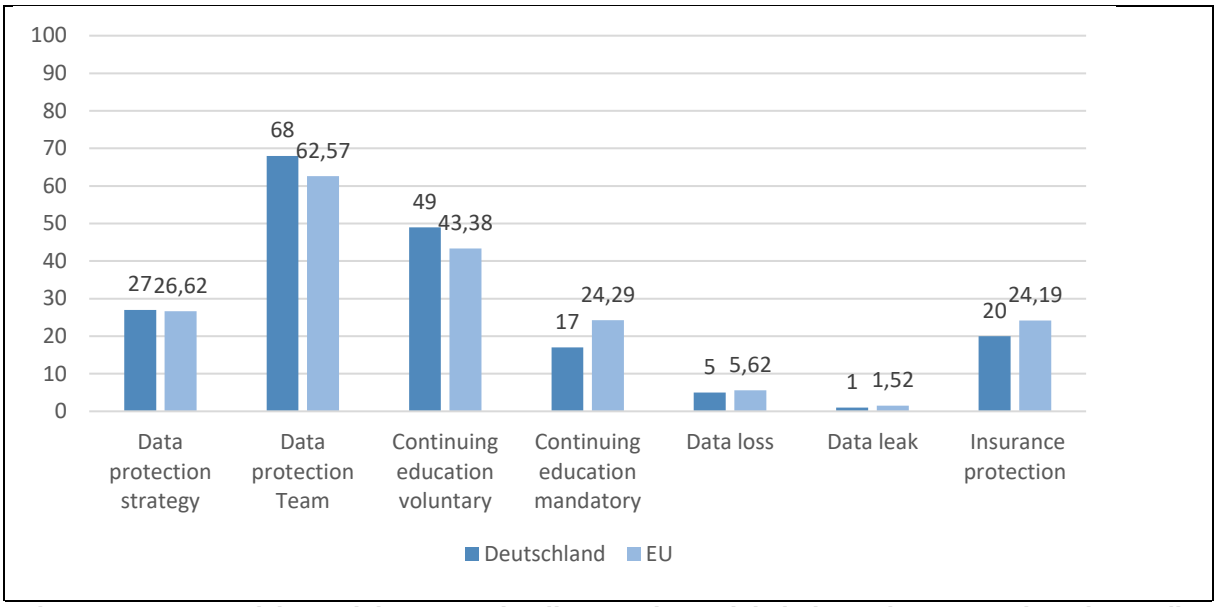

Figura 8: **Composizione del punteggio di protezione dei dati per la Germania e la media dell'UE in valore percentuale**
Fonte: heyData (2021). Nostra illustrazione.

Considerando le violazioni della privacy dei dati, in Germania vengono emesse severe punizioni. Con circa 69 milioni di euro di multe nel 2020, le violazioni dei dati vengono punite severamente. Questa constatazione va di pari passo con il fatto che in Germania è stata riportata la più alta quantità totale di violazioni della protezione dei dati. Soprattutto in tempi di home-office durante la pandemia, le violazioni hanno sperimentato un'impennata di circa il 76% rispetto all'anno precedente. La ramificazione di questa scoperta è spiegata come segue: "Rispetto al resto d'Europa, le aziende in Germania per la maggior parte si comportano in modo molto esemplare. Tuttavia, questo è anche necessario. L'applicazione della legge in Germania è gestita rigorosamente" (Milos Djurdjevic, CEO heyData, (maggio 2021)).

Considerando questi dati, non c'è da meravigliarsi se sono state fondate diverse associazioni che si occupano specificamente della corretta attuazione della protezione dei dati nella sfera pubblica e aziendale. Il "diritto all'autodeterminazione informativa" (BVerfG 15.12.1983) e la protezione dei diritti personali contro la crescente enfasi sugli interessi di sicurezza è parte integrante del lavoro di queste associazioni. La minaccia verso la protezione dei dati e la sicurezza dell'informazione non è quindi percepita solo tra entità criminali e ostili, ma anche dal governo federale e dai suoi interessi di sicurezza.

2.4 Italia

Nome dell'istituzione	Breve descrizione	Obiettivi principali	Sito web
Apindustria Vicenza	Circa 1.000 membri (la maggior parte sono micro/piccole imprese, con meno di 20 lavoratori). Offrono servizi come: collegamento con le autorità locali e regionali (dipartimento regionale, camere, politiche regionali); servizi fiscali e legali per i membri; corsi di formazione; servizi specifici (es. per l'esportazione, rete, sostenibilità, questioni legali, progetti UE, certificazioni, ecc.) Persona di contatto: Manuel Maraschin (Direttore; mail: m.maraschin@apindustria.vi.it)	Alcune aziende (associate ad Apindustria Vicenza) hanno già al loro interno un responsabile IT e DP. In questo caso, potremmo verificare e pilotare un processo di certificazione (parziale) con questi manager, verificando i percorsi formativi attraverso i contenuti di IO3 (questionario on line). Viceversa, con esperti esterni (consulenti, fornitori IT, avvocati, ecc.) che stanno supportando le PMI, potremmo verificare se la certificazione si adatta al loro lavoro quotidiano. Apindustria Vicenza è disponibile ad organizzare alcuni incontri con le PMI locali e, allo stesso tempo, a proporre ai responsabili IT e DP alcune interviste che potrebbero essere utili per le OI del progetto. Apindustria non è un ente pubblico, ma una sorta di organizzazione "intermedia", che rappresenta anche gli interessi collettivi locali/regionali. Apindustria Vicenza, come associazione di categoria, partecipa ad alcuni tavoli tecnici e di lavoro regionali. Questi incontri sono anche focalizzati sul profilo professionale, sulla definizione di competenze specifiche, sui processi di certificazione (parziale), ecc. Apindustria potrebbe quindi supportare l'implementazione di questo nuovo profilo, anche perché rappresenta diverse PMI locali. Grazie ad alcuni corsi FSE - Fondo Sociale Europeo, Apindustria potrebbe implementare, alla fine del progetto, anche percorsi formativi specifici, che potrebbero essere (in parte) certificati dal nostro ufficio regionale di formazione. Tempistica: la nuova programmazione UE 2021 - 2027 è ancora in discussione. Al momento, ci sono diversi incontri tecnici a livello regionale (obiettivo principale della strategia di formazione, nuovi contenuti, armonizzazione dei profili professionali a livello nazionale ed europeo, priorità ESCO, ecc.) Ma Apindustria potrebbe anche informare l'autorità regionale sui contenuti del progetto. Così, grazie a questo, alcuni risultati del progetto potrebbero essere implementati in nuovi programmi.	WWW. apindustria.vi.it
CPV – Fondazione CentroProduttivitàVeneto	È uno dei più grandi fornitori di formazione nella Regione Veneto, con quasi 70 anni di esperienza. CPV offre una vasta gamma di corsi di formazione, per PMI, lavoratori, manager, consulenti e disoccupati. Negli ultimi 2/3 anni hanno anche organizzato diversi corsi di formazione sui temi del progetto. Persona di contatto: Enrico Bressan, (director della formazione e dei progetti EU; mail: bressan@cpv.org). È anche un esperto esterno	Bressan ha una vasta esperienza (grazie ad alcuni progetti regionali, nazionali e transnazionali) nella piattaforma ESCO, nel quadro Ecvet, negli schemi EQF, ecc. Potrebbe sostenere il progetto, scambiando la sua esperienza. Inoltre, CPV è in grado di coinvolgere diverse piccole imprese locali. Come fornitore di formazione, CPV ha costruito una forte rete regionale, nel campo della formazione professionale e dell'educazione degli adulti. E ha un ampio numero di esperti (per esempio consulenti e formatori) che potrebbero controllare e convalidare alcune liste di competenze. CPV è in grado di coinvolgere le piccole imprese locali, organizzando per esempio interviste con potenziali candidati e incontri (workshop) con le imprese. CPV sta anche gestendo un "gruppo di studio" (dall'anno 1985) focalizzato su IT, informatica, protezione dei dati, digitalizzazione,	www.cpv.org

	per l'agenzia di formazione permanente di Roma.	ecc. I risultati intermedi e finali del progetto potrebbero essere presentati a loro. Come istituzione "pubblica/privata", CPV siede in diversi tavoli tecnici a livello regionale (per esempio il comitato del gruppo di esperti per il riconoscimento e la valutazione delle competenze e dei profili professionali). Potrebbe rivedere il nostro piano di adattamento regionale e, in seguito, fare attività di lobbying con le nostre autorità regionali.	
Cesar srl	È il centro di formazione, a Vicenza, per l'associazione locale dell'artigianato (che conta più di 20.000 micro e piccole imprese). Offre una vasta gamma di servizi di formazione, tra cui corsi di sicurezza informatica, protezione dei dati, GDPR, ecc. Referente: Daniela Bucci, (vice-direttrice della formazione; mail: d.bucci@confartigianatovicenza.it).	Cesar lavora solo con micro e piccole imprese (sotto i 10 dipendenti). Normalmente, queste aziende non hanno un esperto interno come il responsabile o il responsabile della sicurezza informatica e della protezione dei dati. Grazie ai corsi di formazione (finanziati o meno) Cesar è in grado di supportare il processo di certificazione (parziale). Cesar potrebbe essere coinvolto in diverse fasi, come: coinvolgimento delle piccole imprese; analisi dei bisogni; definizione delle competenze chiave; pilotaggio e formazione. In futuro, potrebbero anche offrire alle aziende locali corsi certificati TEBEISI, con tutti i risultati del progetto. Cesar fa parte della rete regionale di centri di formazione, per micro e piccole imprese, composta da 7 province (75.000 membri in totale). Cesar è, molto spesso, coinvolto in diversi tavoli tecnici regionali e gruppi di lavoro sui profili professionali e sul processo di certificazione. Potrebbe conoscere la nostra autorità regionale su obiettivi e risultati dei progetti, soprattutto per le microimprese.	www.confartigianatovicenza.it
Camera di Commercio di Vicenza	È un ente pubblico in Italia, e offre un servizio obbligatorio per tutte le aziende. Per esempio, ogni azienda locale deve essere registrata nella banca dati locale (per tutte le fasi del business, dall'inizio alla chiusura del percorso). La Camera di Vicenza rappresenta oltre 90.000 imprese, la maggior parte delle quali sono micro o piccole. Referente: Diego Rebesco (direttore dell'ufficio statistico e promozione; mail: diego.rebesco@vi.camcom.it).	La Camera offre una vasta gamma di servizi, che comprende più o meno tutte le esigenze delle aziende (compiti amministrativi, formazione, esportazione, certificazioni, brevetti, ecc.) La Camera è anche attiva nel campo del riconoscimento dei profili professionali, per esempio attraverso il Ministero dell'Istruzione e del Lavoro a Roma. Gestisce anche stage per giovani (delle scuole superiori) che frequentano brevi esperienze in azienda, attraverso alcuni corsi certificati che, alla fine, vengono valutati. Potrebbe essere coinvolta non solo nella promozione e diffusione del progetto (come newsletter o workshop locali) ma anche nel processo di certificazione, grazie al legame con il nostro Ministero nazionale. Come minimo, potrebbe essere informato sull'andamento del progetto. Ma potrebbe anche costituire un gruppo di lavoro locale (provincia di Vicenza). Questo organismo potrebbe, alla fine del progetto, presentare il processo di certificazione finale (parziale) TEBEISI alla nostra autorità regionale, per un pieno riconoscimento. Potrebbe essere il nostro ente pubblico che verifica e certifica l'intero piano di adattamento regionale, come parte della sua funzionalità e obiettivo. Più in dettaglio, potrebbe controllare il calendario, i ruoli dei singoli partecipanti e, soprattutto, convalidare i contenuti principali del piano, anche in termini di futura legislazione specifica nel tema del progetto, o di esigenze specifiche che potrebbero essere inserite nei programmi di formazione regionale.	www.vi.camcom.it
Proservizi srl	È il centro di formazione regionale di	Proservizi srl ha, come clienti, solo consulenti (non aziende). Quindi, sono in grado di	www.proservizi.it

	ConfProfessioni Veneto (che conta più di 45.000 iscritti, come avvocati, fiscalisti, notai, consulenti, ecc.) Offre una vasta gamma di servizi di formazione, tra cui corsi di sicurezza informatica, protezione dei dati, GDPR, ecc. Persona di contatto: Greta Cosentino, (direttrice della formazione; mail: greta.cosentino@proservizi.it).	coinvolgere un gran numero per esempio di avvocati specializzati in sicurezza informatica e legislazione sulla protezione dei dati. Inoltre, offrono molto spesso corsi di formazione (base e avanzati) su GPPR e codice della privacy. Quindi, sono in grado di verificare e confrontare i percorsi progettuali (ad esempio in termini di elenco di competenze specifiche) e ciò che il mercato (le aziende) richiede. Proservizi è già stato coinvolto in attività di progetto. Per esempio alcuni membri (per esempio avvocati) hanno fatto interviste al progetto. Offrono anche corsi di formazione finanziati (grazie al FSE - Fondo Sociale Europeo, e/o sovvenzioni specifiche dal loro sistema di formazione, chiamato "Fondo ConfProfessioni"). Quindi, sono in grado di finanziare il corso di profilo TEBEISI nel prossimo futuro. Proservizi potrebbe sostenere soprattutto le fasi di pilotaggio, coinvolgendo cioè alcuni avvocati locali con alcune piccole imprese (loro clienti) proprio per verificare i contenuti del progetto. Ma anche per acquisire nuove competenze nel campo della sicurezza informatica e del responsabile della protezione dei dati. Potrebbero anche organizzare un percorso di formazione specifico per i soci, che comprenda tutti gli esiti e i risultati di TEBEISI. Proservi è coinvolta, molto spesso, in diversi gruppi di lavoro regionali, nel campo dei bisogni formativi e del riconoscimento delle competenze. Quindi, potrebbe suggerire alla nostra autorità regionale per la formazione, ad esempio, nuovi input per il prossimo programma FSE (che coprirà il periodo 2021 - 2027).	
SATEF srl	È il centro di formazione regionale. Offre una vasta gamma di servizi di formazione, tra cui corsi di sicurezza informatica, protezione dei dati, GDPR, ecc. È anche specializzato nel settore della salute e della sicurezza, compresi i centri di assistenza agli anziani. Persona di contatto: Paolo Pedron, (fdirettore e fondatore; mail: pedron@satef.com).	Il signor Pedron, il direttore, è un esperto ESCCO / Ecvet, a livello regionale e nazionale. Ha creato una piattaforma di formazione specifica per il riconoscimento e la certificazione (parziale) delle competenze. Al momento, la sta gestendo in due settori: salute e sicurezza e turismo. Quindi, potremmo testare e pilotare i contenuti del nostro progetto nella sua piattaforma. Questo test potrebbe coinvolgere anche le piccole imprese e alcuni consulenti/esperti. Satef potrebbe testare i contenuti del progetto, per esempio nel campo del turismo. Infatti, grazie a precedenti esperienze, la piattaforma esiste già, anche in termini di percorso formativo. Quindi, i contenuti della formazione TEBEISI potrebbero essere testati, ma anche un (parziale) processo di certificazione potrebbe essere fatto, anche a livello regionale. Pedron partecipa ad alcuni gruppi di lavoro regionali sulla "certificazione e valutazione dei profili professionali". Quindi, è in grado di supportare fortemente la nostra fase di implementazione. Grazie al suo ruolo, a livello regionale, Pedron è in grado di promuovere presso la nostra autorità pubblica i contenuti e i risultati del progetto (comprese le fasi di test). Potrebbe anche, informalmente, valutare il nostro "piano di adattamento regionale", appena prima di inviarlo (per una discussione finale) al nostro dipartimento regionale di formazione e lavoro a Venezia.	www.satef.com
ENGIM Veneto	È il più grande fornitore di formazione nella Regione	Fochesato ha una vasta esperienza (grazie ad alcuni progetti regionali, nazionali e	www.engimvi.it

	Veneto, con quasi 90 anni di esperienza. ENGIM offre una vasta gamma di corsi di formazione, per PMI, lavoratori, manager, consulenti e disoccupati. Negli ultimi 2/3 anni hanno anche organizzato diversi corsi di formazione sui temi del progetto. Persona di contatto: r Manuel Fochesato, (direttore formazione e progetto EU; mail: manuel.fochesato@engimvi.it).	transnazionali) nella piattaforma ESCO, nel quadro Ecvet, negli schemi EQF, ecc. Potrebbe sostenere il progetto, scambiando la sua esperienza. Inoltre, ENGIM è in grado di coinvolgere diverse piccole imprese locali, ma anche consulenti, formatori ed esperti. Engim agisce anche come VET; così parte dei corsi di formazione sono focalizzati sui giovani, sugli adulti che hanno bisogno di formazione supplementare e, soprattutto, sui disoccupati. Engim gestisce già (e ha pianificato) diverse piattaforme di formazione, che includono non solo materiali formativi (cioè corsi on line per una vasta gamma di esigenze educative) ma anche sistemi informatici che riconoscono, in parte, competenze specifiche. Engim può, fortemente, supportare l'implementazione dei profili professionali, in diversi modi: trovare utenti finali (piccole imprese e/o consulenti/esperti); coinvolgere tirocinanti (giovani e/o adulti) che sono alla ricerca di una nuova specializzazione lavorativa e, non ultimo, discutere e scambiare con gli enti di formazione locali (regionali). Grazie al ruolo e all'esperienza di Fochesato, a livello regionale, è in grado di promuovere presso il nostro ente pubblico i contenuti e i risultati del progetto (comprese le fasi di sperimentazione). Engim potrebbe anche condividere il piano di adattamento regionale con diversi stakeholder pubblici. Ma potrebbe anche impostare nuovi contenuti nelle loro piattaforme di formazione on line, compresi i contenuti TEBEISI.	
Veneto lavoro	È l'agenzia pubblica regionale che gestisce tutti i contenuti relativi al mercato del lavoro (corsi, certificazioni, centri di lavoro locali per disoccupati, ecc.) Persona di contatto: Mirco Casteller, (responsabile dipartimento welfare e progetto EU; mail: mirco.casteller@venetolavoro.it).	La Regione Veneto, attraverso Veneto Lavoro, gestisce il "Dipartimento Lavoro e Formazione"; quindi l'ente pubblico che gestisce tutti i fondi (es. FSE - Fondi Sociali Europei) per lavoratori, aziende, manager e consulenti/formatori. Veneto Lavoro gestisce anche il "RRSP - Repertorio Regionale Standard Professionali" (la banca dati / repertorio regionale per gli standard professionali e le qualifiche). Come ente pubblico, Veneto Lavoro è lo stakeholder più importante a livello regionale, soprattutto perché gestisce l'RRSP. E il signor Casteller è il nostro contatto principale per questo scambio e discussione strategica. Veneto Lavoro gioca un ruolo cruciale nella realizzazione del profilo TEBEISI, soprattutto nelle ultime fasi del progetto (dove il partner italiano dovrebbe diffondere alcune linee guida e raccomandazioni). Come ufficio indipendente e pubblico, Veneto Lavoro non può essere direttamente coinvolto nel processo, ma potrebbe agire come "consulente pubblico". Veneto Lavoro può convalidare il nostro "piano di adattamento regionale" passo dopo passo. Nel senso che potremmo informare, fin dall'inizio, Veneto Lavoro sui progressi del progetto e, alla fine, proporre questo nuovo profilo professionale che potrebbe essere (in parte) certificato e inserito nel database regionale per gli standard professionali (RRSP).	www.venetolavoro.it
INAPP	È la nuova agenzia a livello nazionale, che gestisce e controlla tutti i progetti nazionali (ed europei) che sono collegati alla valutazione e	Come il precedente stakeholder menzionato (Veneto Lavoro) INAPP potrebbe sostenere fortemente il nostro progetto, in termini di scambio e suggerimenti per l'intero processo di certificazione. In particolare, INAPP gestisce il nuovo "Atlante del lavoro e delle qualifiche".	www.inapp.org

	alla certificazione delle competenze.. Contatto: urp@inapp.org oppure atlante_lq@inapp.org)	L'Atlante è il database / repertorio generale (nazionale) per gli standard professionali e le qualifiche. Include anche un profilo per gli studenti (scuole superiori e università) e linee guida per i centri di formazione professionale e i centri di formazione. Recentemente, l'INAPP ha lanciato anche l'"Atlante per i professionisti" (come consulenti, formatori, avvocati, ecc.) e potrebbero controllare i progressi del progetto in termini di nuovi profili di "TEBEISI IT secury and DP managers". E, nel medio termine, inserire e promuovere anche questo nuovo profilo. INAPP potrebbe anche controllare i contenuti del progetto in termini di futuri corsi di formazione FSE - Fondi Sociali Europei - (programma: 2021 _ 2027) basati sui risultati di TEBEISI. INAPP potrebbe essere informato sui progressi, a livello regionale. E controllare, dando alcuni feedback/suggerimenti, in termini di coerenza e sostenibilità del progetto a medio termine. E potrebbe anche valutare i materiali di formazione, incluso soprattutto il processo di certificazione delle competenze (parte), almeno a livello nazionale. Il NAPP gestisce decine di gruppi di lavoro a livello nazionale. Molte volte, questi gruppi funzionano anche a livello regionale. Quindi, potremmo incontrare e discutere con alcuni membri del gruppo, proponendo loro o un piano di adattamento regionale, prima della chiusura del progetto.	
AIPSI	Associazione italiana dei professionisti sicurezza informatica. È il capitolo italiano di ISSA, un'organizzazione internazionale no-profit di professionisti ed esperti. Con la partecipazione attiva dei singoli membri e dei loro capitoli in tutto il mondo, AIPSI, come capitolo di ISSA, fa parte della più grande associazione no-profit di professionisti della sicurezza con oltre 13.000 in tutto il mondo. Persona di contatto: Yvette Agostini (Director, info@aipsi.org)	L'AIPSI è una delle più importanti associazioni italiane di esperti di sicurezza informatica. Ma lavora anche con i responsabili della protezione dei dati. Offre una vasta gamma di servizi, utili per il progetto TEBEISI, come: indagini e ricerche, rapporti, formazione e consulenza e, naturalmente, (parte) attività di valutazione e certificazione dei profili professionali. La maggior parte dei loro corsi (gratuiti o a pagamento) hanno già ottenuto la certificazione da un ente nazionale o regionale. Fa anche parte di una rete internazionale più ampia; quindi potrebbe darci una visione più ampia e ulteriori informazioni. L'AIPSI potrebbe controllare i contenuti del progetto e le fasi di valutazione. In particolare, potrebbe accettare e verificare alcuni nuovi materiali di formazione, per esempio alcune competenze specifiche (come le soft skills o le abilità personali). L'AIPSI ha diversi membri che provengono anche dal Veneto (c'è anche un ufficio locale a Venezia; la maggior parte dei membri locali sono ingegneri informatici). Con loro potremmo scambiare alcuni contenuti e, soprattutto, controllare le versioni finali. Inoltre, il nostro progetto potrebbe collegare i membri del Clusit (che sono professionisti) con le PMI. L'AIPSI partecipa già a diversi gruppi di lavoro tecnici, a livello nazionale (Ministero dell'Innovazione e dell'Educazione in particolare) e a diverse task force regionali. In particolare, i loro rapporti e pubblicazioni sono la base scientifica per ulteriori miglioramenti legislativi nel campo del riconoscimento dei (nuovi) profili professionali. Per la nostra Regione, il presidente o il direttore locale dell'AIPSI potrebbe rappresentare gli esperti scientifici e tecnici.	www.aipsi.org
CLUSIT	Associazione Italiana per	Clusit è una delle più importanti associazioni	www.clusit.it

	la sicurezza informatica. CLUSIT Italia nasce sulla base delle esperienze di altre associazioni europee per la sicurezza informatica come CLUSIB (Belgio), CLUSIF (Francia), CLUSIS (Svizzera) CLUSIL (Lussemburgo) che da oltre 20 anni sono un punto di riferimento per la sicurezza informatica nei rispettivi paesi. Obiettivo principale: Diffondere la cultura della sicurezza informatica alle aziende, alla pubblica amministrazione e ai cittadini. Persona di contatto: Gabriele Faggioli (Presidente; president@clusit.it)	italiane di esperti di sicurezza informatica. Ma lavora anche con i responsabili della protezione dei dati. Offre una vasta gamma di servizi, utili per il progetto TEBEISI, come: indagini e ricerche, report, formazione e consulenza e, naturalmente, attività di (parte) valutazione e certificazione dei profili professionali. La maggior parte dei loro corsi (gratuiti o a pagamento) hanno già ottenuto la certificazione da un ente nazionale o regionale. Clusit potrebbe controllare i contenuti del progetto e le fasi di valutazione. In particolare, potrebbe accettare e verificare alcuni nuovi materiali formativi, per esempio alcune competenze specifiche (come le soft skills o le abilità personali). Il Clusit ha diversi membri che provengono anche dal Veneto (la maggior parte di loro sono ingegneri informatici). Con loro, potremmo scambiare alcuni contenuti e, soprattutto, controllare le versioni finali. Inoltre, il nostro progetto potrebbe collegare i membri del Clusit (che sono professionisti) con le PMI. Il Clusit partecipa già a diversi gruppi di lavoro tecnici, a livello nazionale (Ministero dell'Innovazione e dell'Educazione in particolare) e in diverse task force regionali. In particolare, i loro rapporti e pubblicazioni sono la base scientifica per ulteriori miglioramenti legislativi nel campo del riconoscimento dei (nuovi) profili professionali.	
Università di Padova – dipartimento di informatica	Negli ultimi anni hanno fatto diverse indagini sui temi del progetto. Persona di contatto: Prof. Antonio Scipioni (scipioni@unipd.it).	L'Università di Padova organizza già master di secondo livello su temi progettuali (data protection manager, esperto di sicurezza informatica, ecc. I loro contenuti e percorsi formativi potrebbero essere utili per la selezione delle competenze e dei profili professionali. Potrebbero coinvolgere manager, esperti e PMI, ad esempio per fare colloqui, workshop, ecc. Come Università, potrebbero "garantire" un approccio scientifico e le giuste metodologie. Come ateneo potrebbero coinvolgere anche diversi dipartimenti (economia, diritto, IT - informatica, management, ecc.) L'università è un ente pubblico, che prende parte a diversi comitati direttivi regionali e gruppi di lavoro, compresi anche gruppi di esperti sui temi del progetto. Quindi, se sono a conoscenza dei progressi del progetto, potrebbero sostenere il processo di certificazione a livello regionale.	www.unipd.it
APCO – Associazione italiana dei consulenti di management	È l'associazione italiana dei consulenti di direzione, fondata nel 1968; oggi conta oltre 400 soci. APCO offre diversi servizi per i soci, come: formazione, iniziative di networking, lobby con le istituzioni, ecc. Referente: Cesara Pasini (Presidente; mail: presidenza@apcoitalia.it)	APCO ha diverse "comunità di pratica" che si concentrano in diversi argomenti. In particolare, due di esse (trasformazione digitale / innovation manager e compliance / norme ISO) potrebbero aiutarci nella certificazione parziale. APCO ha promosso un'apposita legge nazionale (n. 4, anno 2013) che riconosce anche i consulenti che non sono iscritti a un ordine professionale (per legge); ma che hanno una certificazione professionale e una formazione continua. APCO è disponibile ad organizzare alcuni incontri (anche on line), con alcuni membri che stanno lavorando su temi di progetto. APCO non è un ente pubblico; ma una sorta di organizzazione "intermedia", che rappresenta anche interessi collettivi locali/regionali. Per esempio, c'è la delegazione "Nord Est" (Veneto, Trentino Alto Adige e Friuli Venezia Giulia) che potrebbe essere coinvolta in alcune attività del	www.apcoitalia.it

		progetto. La delegazione locale (regione Veneto, Paolo Ferrarese come coordinatore) potrebbe fare un po' di lobby con le nostre autorità locali (Regione, dipartimento lavoro e formazione).	

Tabella 4: Lista degli Stakeholder dell'Italia.

Il GDPR in Italia è ufficialmente applicabile da tempo, esattamente dal 25 maggio 2018. Poi, il 19 settembre 2018, è entrato in vigore il testo che adegua la normativa italiana al General Data Protection Regulation, ovvero il Decreto 101/2018.

GDPR italiano: a che punto siamo, dopo tre anni?

Nel giugno 2021, l'"Ufficio dell'autorità di controllo della privacy" ha pubblicato un rapporto sulla sua attività nei tre anni di applicazione del Regolamento ed è emerso che c'è stato un aumento della consapevolezza degli interessati in relazione ai loro diritti con circa 27.192 reclami e segnalazioni di violazione al Garante. (GDPD 2020) L'elevato numero di segnalazioni, circa 24 al giorno, 365 giorni l'anno per tre anni, dimostra che l'adozione del GDPR ha sicuramente aumentato la consapevolezza degli interessati in relazione all'esistenza dei loro diritti e alla richiesta della loro tutela.

Il numero di notifiche è salito a 2839 nel trimestre tra il 1° gennaio e il 31 marzo 2021, segno che l'anno pandemico con la digitalizzazione di molte attività ha portato anche a una maggiore attenzione degli utenti al tema della protezione dei dati personali.

Allo stesso modo, le notifiche di data breach sono state 3.873 (circa 3,5 al giorno), poche se paragonate alle statistiche sui cyber-attacchi, ma comunque indicative dell'importanza di adottare politiche e strumenti di sicurezza che aiutino a prevenirle. Un aspetto fondamentale, in ogni caso, è la formazione e la sensibilizzazione del personale sul tema della sicurezza e sul comportamento da adottare in caso di richieste non conformi alle procedure aziendali.

Sono stati comunicati i nominativi di 59.838 responsabili della protezione dei dati (detti anche DPO), e non tutti dalle Pubbliche Amministrazioni che, in base al Regolamento, sono obbligate a nominare un DPO. Questo dimostra come la necessità di avere una figura di coordinamento, sorveglianza e contatto tra l'autorità di controllo, gli interessati e il titolare del trattamento sia vista come un requisito importante.

Sul fronte delle sanzioni, in Europa sono stati effettuati 654 procedimenti per un totale di 283.757.083 euro, (fonte), guardando le statistiche divise per paesi, l'Italia si colloca al primo posto per l'ammontare complessivo delle sanzioni comminate per 76.298.601 euro in 79 provvedimenti, a conferma dell'attività del Garante italiano e dell'attenzione con cui vengono gestiti reclami e segnalazioni. Questo conteggio, ovviamente, considera solo le sanzioni comminate ai sensi dell'articolo 83 GDPR e non tiene conto di eventuali risarcimenti o indennizzi corrisposti agli interessati i cui diritti sono stati violati. Come dichiarato dai membri dell'Autorità di vigilanza in occasione dell'anniversario del regolamento UE, c'è ancora molta strada da fare per coniugare la digitalizzazione degli Stati membri con una gestione sicura delle

infrastrutture. L'aumento del perimetro di vulnerabilità delle aziende, dovuto all'adozione più o meno forzata di soluzioni di lavoro a distanza, impone ai proprietari di ripensare i flussi di dati e le procedure di sicurezza all'interno delle loro organizzazioni.

Ma cosa significa questo per le imprese del nostro paese? Fortunatamente, la tendenza sembra positiva. A quasi due anni dalla sua piena applicazione, in Italia si stanno facendo progressi significativi in termini di adeguamento alla normativa, con aumenti del budget a disposizione delle organizzazioni e crescita della maturità, in termini di concretezza dei progetti e di cambiamenti organizzativi mirati.

Tuttavia, la complessità e l'importanza della materia richiedono uno sforzo continuo da parte delle aziende per adeguarsi ai principi imposti dalla normativa sulla protezione dei dati e per rispondere alle richieste delle autorità. A questo proposito, in diversi paesi europei sono state comminate le prime multe per violazioni del regolamento. In Italia, invece, l'atteggiamento dell'Autorità di controllo è stato inizialmente accomodante, anche a causa dei ritardi nell'elezione del nuovo Collegio dell'Autorità di controllo. Tuttavia, il periodo più recente ha visto un'intensificazione dei controlli e delle ispezioni e l'applicazione delle prime sanzioni previste dalla normativa locale e sovranazionale sulla protezione dei dati. Grazie alla ricerca condotta dall'Osservatorio Cyber Security & Data Protection, possiamo vedere come questa normativa stia cambiando il contesto italiano.

Lo stato di conformità al GDPR italiano

Per esplorare i cambiamenti in atto nelle aziende italiane in materia di Data Protection, l'Osservatorio ha considerato quattro aspetti:

- stato dei progetti di compliance

- budget dedicato

- azioni attuate

- criticità riscontrate

Dallo studio emerge che quasi tutte le aziende italiane hanno implementato o perfezionato progetti di compliance al GDPR. Più della metà delle organizzazioni ha dichiarato di aver rispettato i requisiti della normativa e, allo stesso tempo, è diminuito il numero di aziende che ha dichiarato di non essere a conoscenza delle implicazioni del GDPR.

Su quest'ultimo punto, però, va precisato che si tratta di aziende in cui il tema della protezione dei dati non ha ancora raggiunto i vertici, ma è comunque noto a funzioni specialistiche come IT Security, Legal e Compliance. Un altro segnale positivo della maturità e della consapevolezza del GDPR in Italia è la bassa percentuale di aziende (5%) che sono ancora in fase di analisi dei requisiti e di definizione dei piani di compliance, mentre due anni fa questa quota raggiungeva il 34%. Il quadro è positivo anche in termini di budget dedicato alle misure di conformità al GDPR: Il 45% delle

aziende italiane ha aumentato il budget dedicato. Se questo numero è positivo, è anche vero che il focus deve ancora spostarsi su attività specifiche come gli audit periodici, l'aggiornamento delle procedure e delle tecnologie di sicurezza e protezione dei dati. (fonte: Andrea Antonelli 2020)

Azioni di conformità DPR

In concreto, cosa stanno facendo le aziende italiane per adeguarsi al GDPR? Va ricordato che il processo di adeguamento deve necessariamente essere composto da più fasi, che attualmente hanno diversi livelli di adozione:

- Creazione del registro dei trattamenti (85%): creazione obbligatoria di un registro dove tenere traccia di tutti i trattamenti effettuati;

- Identificazione dei ruoli e delle responsabilità (81%): identificazione e contrattualizzazione di tutti i responsabili del trattamento;

- Modifica della modulistica (76%): aggiornamento della modulistica secondo i requisiti del GDPR;

- Procedura di Data Breach Notification (68%): processo di notifica all'Autorità di controllo delle violazioni di dati riservati;

- Definizione delle politiche di sicurezza e valutazione dei rischi (66%): adozione di misure per garantire la conformità del trattamento al Regolamento;

- Data Protection Impact Assessment (56%): valutazione d'impatto sulla protezione dei dati (DPIA) obbligatoria quando il trattamento può comportare un rischio elevato per i diritti e le libertà degli interessati;

- Attuazione dei processi per l'esercizio dei diritti degli interessati (54%): azioni per far valere i diritti riconosciuti agli interessati dal trattamento. (Andrea Antonelli 2020)

Oltre a queste azioni, è necessario considerare anche l'inserimento nelle aziende della figura del Data Protection Officer (DPO). Questa figura, la cui nomina è prevista dal GDPR in diversi casi, è presente nel 65% delle organizzazioni. Questo dato è sicuramente positivo, in quanto rivela un aumento del numero di aziende che hanno introdotto questa figura.

Quali criticità comporta il GDPR per le aziende italiane?

Se è vero che il quadro sullo stato della compliance al GDPR italiano è generalmente positivo, è anche vero che le organizzazioni hanno incontrato alcune difficoltà. Infatti, molte aziende stanno ancora incontrando difficoltà dal punto di vista organizzativo, ad esempio nell'identificazione di ruoli e responsabilità all'interno dell'azienda, mentre altre segnalano un significativo rallentamento delle attività quotidiane.

Tuttavia, questi elementi negativi sono di poco conto rispetto a uno scenario maturo in cui le aziende italiane si stanno dimostrando non solo orientate ad affrontare le sfide in termini di protezione dei dati, ma anche consapevoli dell'intera questione.

2.5 Lituania

Nome dell'istituzione	Breve descrizione	Obiettivi principali	Sito web
Alytus Business Consulting Centre (AVKC)	Alytus Business Consulting Center (AVKC) è il primo centro di consulenza aziendale in Lituania, registrato il 13 maggio 1993. come un'organizzazione non-profit che è stato successivamente ri-registrato come un ente pubblico. Alytus Business Consulting Centre - Alytus partecipante strategia di sviluppo regionale in cooperazione internazionale di sviluppo nello sviluppo regionale con la svedese Jonkompingo County, Polonia, Danimarca, Ungheria, Italia autorità regionali, Ministero delle agenzie di sviluppo aziendale esistenti, Alytus contea comuni e strutture associate del promotore.	La missione di Alytus Business Consulting Center - promuovere e sviluppare le piccole e medie imprese, fornendo formazione aziendale, consulenza, informazione, nuove iniziative di sviluppo aziendale nello sviluppo e nell'implementazione dello sviluppo del networking nella regione di Alytus.	https://www.avkc.lt/lt/
Associazione dei capi delle istituzioni di assistenza sociale dei comuni	Associazione dei capi delle istituzioni di assistenza sociale dei comuni - un'organizzazione indipendente e volontaria senza scopo di lucro, che comprende 30 istituzioni di assistenza dei comuni	Scopo dell'Associazione - aiutare a risolvere i problemi degli utenti dell'assistenza sociale di tutti i gruppi di persone migliorando la loro qualità e l'integrazione nella società.	http://ssgivasociacija.blogspot.com/
Studio legale ALIANT Tarvainyte Vilys Bitinas	Il team ALIANT® in Lituania fornisce servizi legali integrati in tutti i processi di gestione e sviluppo degli affari e nelle controversie commerciali presso le istituzioni giudiziarie nazionali e internazionali. Lavorano anche nel campo della protezione dei dati	Il team ALIANT® in Lituania fornisce servizi legali integrati in tutti i processi di gestione e sviluppo degli affari e nelle controversie commerciali in istituzioni giudiziarie nazionali e internazionali.	www.aliantlaw.lt
LDAPA - Associazione lituana dei responsabili della protezione dei dati	La priorità dei membri di LDAPA è di creare una piattaforma innovativa, di nuova generazione e non commerciale per i professionisti della protezione	La priorità dei membri di LDAPA è di creare una piattaforma innovativa, di nuova	https://ldapa.lt/

soluzioni.	dei dati personali per condividere conoscenze legali specializzate, buone pratiche, pratiche e nuove	generazione e non commerciale per i professionisti della protezione dei dati personali per condividere conoscenze legali specializzate, buone pratiche, pratiche e nuove	
Centro sicurezza informatica	Per raggiungere gli obiettivi operativi del Centro, i responsabili e gli incaricati del trattamento sono consultati sull'attuazione di misure tecniche e organizzative adeguate per la protezione dei dati. Gli interessati sono consultati sull'attuazione dei diritti umani nel campo della protezione dei dati.	L'obiettivo dell'Information Security Center è quello di migliorare la consapevolezza del pubblico sui temi del trattamento sicuro dei dati personali, della protezione delle informazioni e della sicurezza informatica.	https://infosec.mobi/

Tabella 5: Lista degli Stakeholder della Lituania.

La legge sullo sviluppo delle piccole e medie imprese della Repubblica di Lituania (2017) specifica che le entità di piccole e medie imprese sono medie, piccole e piccolissime imprese che soddisfano determinati requisiti (numero di dipendenti, reddito, indipendenza) e persone fisiche aventi diritto al lavoro autonomo. commerciale e altre attività simili. Nel corso del 2019, il numero di piccole e medie imprese è aumentato dello 0,4%. (registrate 11153). La quota maggiore - 83% - delle PMI erano imprese molto piccole (0-9 dipendenti). Le piccole imprese rappresentavano il 14% (10-49 dipendenti), le medie imprese (50-249 dipendenti) - 3% nel 2019. Nel corso dell'anno, il numero di persone che lavorano nelle PMI è aumentato del 2,2%.

Nonostante i progressi nel settore delle piccole e medie imprese, il miglioramento dell'ambiente aziendale generale e la riduzione delle barriere all'ingresso nel mercato, le dinamiche dell'imprenditoria in Lituania rimangono deboli. Le procedure amministrative per la creazione di nuove imprese sono complesse, e gli imprenditori mancano di capitale iniziale e di competenze gestionali e finanziarie, di marketing e di esportazione e di informazioni. Le decisioni per superare una crisi pandemica, rilanciare l'economia e migliorare l'ambiente imprenditoriale sono difficili da attuare e non producono i risultati attesi.

La ricerca del progetto TebeISi in Lituania mostra che si presta troppo poca attenzione a questo problema. Non si presta sufficiente attenzione al settore pubblico e alle piccole e medie imprese. La mancanza di attenzione è legata alla mancanza di fondi. Una maggiore attenzione alla sicurezza dell'informazione viene data dalla parte della società che è esposta alla sicurezza dell'informazione in un modo o nell'altro. Secondo gli esperti, molta attenzione è data alle istituzioni statali. Per

quanto riguarda il business - l'attenzione è molto meno significativa, poiché non molte persone capiscono pienamente la questione. L'attenzione pubblica alla sicurezza delle informazioni sta aumentando anche a seguito di incidenti di sicurezza pubblica. La ricerca mostra che le PMI non prestano abbastanza attenzione alla formazione interna.

Questo di solito dipende dall'iniziativa dei dipendenti stessi nel trovare e partecipare alla formazione. Recentemente, gli esperti hanno anche collegato la mancanza di formazione alla difficile situazione della pandemia COVID-19, quando molte aziende sono state sospese e si sono concentrate sulla sopravvivenza.

Uno studio quantitativo condotto da M. Lipinskienes (2019) Uno studio quantitativo condotto da M. Lipinskienes (Austrian Press Agency 2020) (2019) sull'attuazione del regolamento generale sulla protezione dei dati nelle aziende lituane ha rivelato che le aziende partecipanti all'indagine in Lituania, che trattano direttamente i dati personali e hanno affidato il trattamento dei dati a un responsabile del trattamento, sono sufficientemente conformi al GDPR. Durante il sondaggio del questionario, gli intervistati hanno risposto all'affermazione: "l'azienda che rappresento ha effettivamente implementato i requisiti del GDPR" da 1 "fortemente in disaccordo" a 100 "fortemente d'accordo". Le risposte sono state codificate nel programma SPSS su una scala di intervallo ed è stato calcolato il punteggio medio degli intervistati. Un totale di 77 intervistati ha risposto alla dichiarazione, la valutazione più bassa era 0, la più alta era 100, e il punteggio medio era 77 su una scala di 100 punti, che significa "sono d'accordo". Gli intervistati più spesso hanno valutato le loro aziende con 100 punti - 23 intervistati, 8 intervistati - con 95 punti, 6 - 90 punti, 7 - 85 punti, 6 - 80 punti. Fino a un punteggio di 80, le risposte sono valutate "fortemente d'accordo", il che significa piena conformità al GDPR. C'erano 50 aziende di questo tipo su 77 intervistati, che è il 65%. Più della metà dei rappresentanti delle aziende sono d'accordo con l'affermazione che l'azienda è conforme allo standard GDPR come "completamente d'accordo".

L'indagine ha rivelato che, secondo l'opinione degli intervistati, il regolamento è piuttosto astratto, laconico, difficile da leggere e difficile da capire per i non addetti ai lavori. Le aziende che elaborano i dati da sole non hanno la conoscenza e la comprensione del GDPR, il che porta all'ignoranza e all'esitazione. Tuttavia, la formazione interna è importante e significativa per ogni dipendente dell'azienda e per l'azienda stessa. Per rispettare il GDPR, il responsabile del trattamento dei dati deve scoprire quali dati personali vengono conservati, dove, per quale scopo, per quanto tempo, come vengono elaborati e conservati. Solo comprendendo ciò che si ha, il responsabile del trattamento saprà come comportarsi e gestire. Questo è stato confermato dalla ricerca a tavolino del progetto TebeISi (IQ1), dalle valutazioni sul trattamento dei dati e sulla protezione dei dati personali come opportunità per identificare le informazioni ridondanti e rivedere i processi aziendali. In questo modo, i processi di business efficienti verrebbero riconosciuti nelle aziende, le fasi di processo inefficienti e ridondanti verrebbero ridotte o eliminate. Questo aiuterebbe le aziende a garantire la sicurezza delle informazioni e la protezione dei dati personali.

Situazione della formazione

In Lituania, c'è una vasta gamma di formazione (da 1,5 ore a diversi giorni) sulla sicurezza dei dati e delle informazioni. Il più delle volte la formazione è fornita da istituzioni private, per esempio: Cyber Security Academy fondata da UAB "Hermitage Solutions" che ha lo scopo di formare specialisti IT in grado di risolvere complicati problemi di sicurezza informatica in modo tempestivo ed efficiente e di valutare la vulnerabilità dell'infrastruttura IT della sua organizzazione. UAB "Atea" che è il principale fornitore baltico di soluzioni e servizi IT e assiste i clienti con competenze specialistiche, prodotti, servizi e soluzioni nell'ambito delle infrastrutture IT, sviluppo di software e sicurezza. NRD Cyber Security che è una società di consulenza tecnologica di cybersecurity, incident response e ricerca applicata. L'azienda si concentra sui servizi per i fornitori di servizi pubblici specializzati (forze dell'ordine, CERT nazionali, telecomunicazioni, regolatori nazionali di comunicazione, infrastrutture critiche nazionali), l'industria finanziaria e le aziende con alta sensibilità dei dati. UAB "Competence Development", che offre corsi di formazione per preparare le certificazioni più popolari, che sono la base per lavorare con le attrezzature di altri produttori, quindi queste certificazioni sono spesso preferite dai datori di lavoro non solo in Lituania ma anche all'estero.

La formazione sulla sicurezza informatica è organizzata per diversi gruppi target: sia principianti, sia utenti informatici avanzati, sia professionisti informatici. Gli argomenti principali della formazione informatica sono: "Formazione sulla sicurezza delle informazioni"; "Formazione sulla sicurezza informatica"; "Formazione sulla sicurezza delle informazioni per non professionisti". Un gruppo separato di formazione sulla sicurezza delle informazioni si concentra sui professionisti IT. Sono formati su argomenti come: "Fondamenti di sicurezza informatica"; "Hack IT to Defend IT"; "Ethical hacker practitioner"; "Safe programming"; "IT security practitioner"; "Cyber security incident management" e "IT security awareness training".

La formazione professionale a diversi livelli sui temi della protezione dei dati è principalmente per i professionisti IT. I principali argomenti di tale formazione sono legati alla protezione dei dati personali nel contesto della formazione sui requisiti del GDPR. La formazione sulla sicurezza dei dati è organizzata anche per avvocati aziendali, amministratori, manager, responsabili del personale. Tale formazione è introdotta al GDPR; "Protezione dei dati personali e responsabilità delle violazioni del GDPR"; "Protezione dei dati personali e violazioni della legislazione sui dati personali nel 2018".

Il GDPR e le attività economiche

Con l'avvio del GDPR nel 2018, la Commissione europea ha stabilito dei guardrail coerenti che garantiscono il diritto fondamentale alla protezione dei dati e forniscono

le basi per la realizzazione della Carta dei diritti fondamentali dell'Unione europea. Il GDPR ha spronato molti altri paesi del mondo a diventare attivi nella loro regolamentazione della protezione dei dati e a seguire il percorso dell'UE, influenzando la posizione e il comportamento di tutte le parti interessate a beneficio dei cittadini europei.

Tuttavia, l'adozione della strategia europea dei dati (Commissione europea 2020a) incontra diversi ostacoli, riportati dalla Commissione europea in una comunicazione sull'attuazione del GDPR (Commissione europea 2020b). Nel frattempo, la consapevolezza generale per il valore dei dati personali è aumentata tra i cittadini e i diritti procedurali hanno rafforzato la capacità di segnalare casi di cattiva condotta, soprattutto nell'uso transfrontaliero dei dati rimangono lacune. A questo proposito, il diritto alla portabilità dei dati tra i servizi a beneficio dell'uso dei beni pubblici deve essere esplorato e i fattori limitanti scoperti. (Commissione europea 02.06.2020).

Per quanto riguarda il bisogno delle PMI, il GDPR ha aumentato le possibilità di libero flusso di dati all'interno e migliorato il flusso di dati con le imprese senza l'UE, favorendo così l'innovazione e le attività economiche. Le PMI, tuttavia, hanno bisogno di affrontare l'attuazione relativamente impegnativa del GDPR per partecipare a queste nuove opportunità - poiché il rischio di violazione dei dati non diminuisce con le dimensioni di un'operazione. Gli sforzi per fornire strumenti pratici e facili da usare per le PMI devono quindi essere aumentati. La Commissione mira a sostenere specificamente le PMI fornendo modelli di contratti e clausole conformi al GDPR.

In definitiva, il successo dell'implementazione si riflette nel successo dell'applicazione da parte delle autorità nazionali di protezione dei dati. Come si può vedere nella Figura 6, grandi differenze diventano evidenti tra gli stati membri.

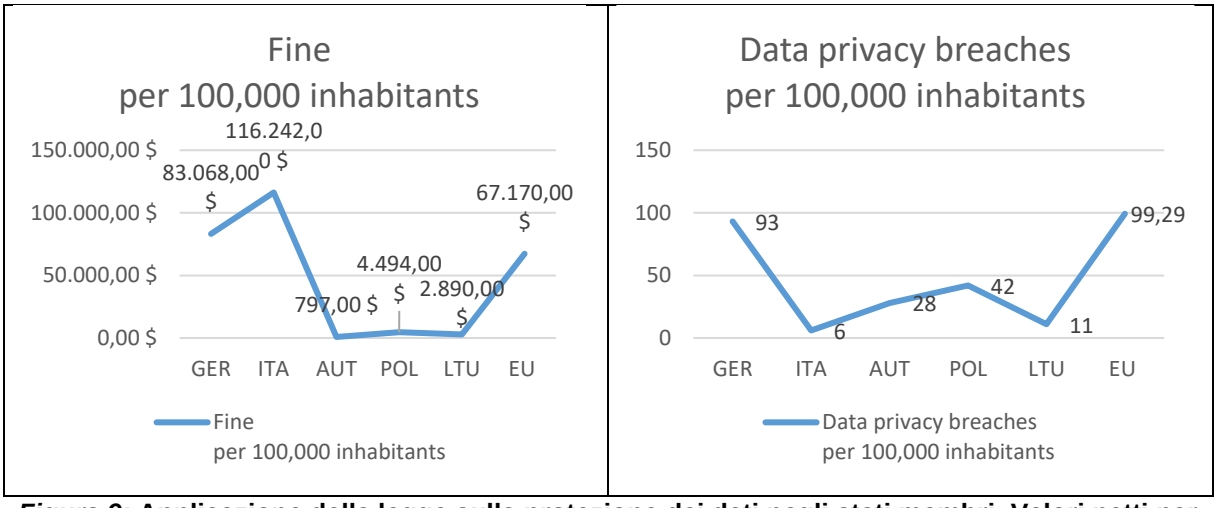

Figura 9: **Applicazione della legge sulla protezione dei dati negli stati membri. Valori netti per 100.000 abitanti.**
Fonte: heyData (2021). Nostra illustrazione.

Nel frattempo tutti i paesi rimangono al di sotto della media UE del totale delle violazioni dei dati per 100.000 abitanti, che è dominata dai grandi numeri riportati per l'Irlanda (245), Danimarca (325) e Paesi Bassi (382), picchi significativi possono essere riportati per le multe pagate. Per capire meglio la relazione tra l'importo delle multe pagate e il numero di violazioni, i valori netti sono stati aggiustati per la parità di potere d'acquisto per garantire la comparabilità tra i paesi. I risultati illustrano che la Germania è vicina al tasso di rilevamento medio dell'UE, mentre l'Italia, l'Austria, la Polonia e la Lituania si trovano ben al di sotto. Risultati simili possono essere osservati per le multe pagate, con l'eccezione prominente dell'Italia, dove le multe vengono pagate quasi raddoppiando la media europea e superando quelle della Germania di circa il 40%. Questo picco porta ad un'ulteriore analisi, calcolando i costi di una violazione dei dati aggiustati dalla parità del potere d'acquisto Figura 7 (a sinistra) e di nuovo per il rischio di rilevamento, mentre il livello di rischio medio è stato calcolato impostando il valore medio dell'UE a 1.

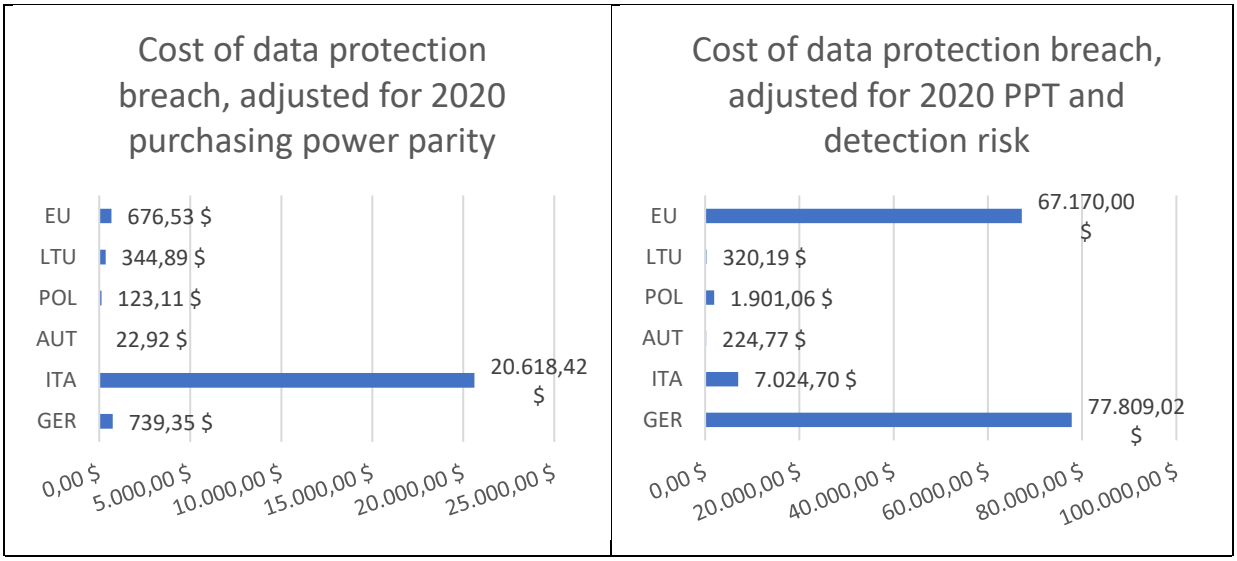

Figura 10: Costo delle violazioni della protezione dei dati aggiustato per la parità di potere d'acquisto e il rischio di rilevamento
Fonte: heyData (2021). Nostra illustrazione.

Nel frattempo l'osservazione degli aggiustamenti ppt chiarisce che per ogni caso riportato si osserva un picco estremo in Italia, l'aggiustamento del rischio chiarisce che si tratta di pochissimi casi con grandi multe. Tuttavia, si può notare che esistono grandi discrepanze per il calcolo del rischio-costo delle violazioni della protezione dei dati, con solo punizioni marginali in Austria, Lituania e Polonia e punizioni severe in Germania. Si può quindi concludere che l'applicazione della legge ha ancora molta strada da fare per essere ugualmente efficace in tutti gli stati membri.

Considerando le situazioni individuali nei paesi partner, in particolare per le PMI le sfide nel processo di attuazione diventano eminenti. Soprattutto la mancanza di tempo e la mancanza di risorse sono state identificate come ragioni primarie per la lenta attuazione. Soprattutto l'allineamento dei processi e il controllo delle informazioni significative per il GDPR nell'azienda sono aree in cui in tutti i paesi le PMI hanno spazio per miglioramenti. In definitiva, la questione della corretta

implementazione è strettamente legata alla disponibilità di personale e alla necessità di corsi di formazione orientati alla pratica. La forte domanda di corsi di formazione continua (sia volontari che obbligatori) ha illustrato il gap di mercato per corsi concisi, trasferibili e trasparenti, come suggerito dall'agenda di ricerca TeBeISi.

2.6 L'anello più debole: il ruolo dei dipendenti e il calcolo della privacy

Alla luce degli sforzi delle imprese, delle organizzazioni non governative e delle autorità pubbliche per mettere in atto il GDPR, un'implementazione di successo deve affrontare gli stessi limiti dell'implementazione della sicurezza delle informazioni: il fattore umano. Come è stato mostrato nel capitolo 2.6, esiste una forte domanda di personale e soprattutto di corsi di formazione continua. I dipendenti, essendo la causa principale della perdita di informazioni e delle violazioni della protezione dei dati, giocano un ruolo fondamentale nella condotta e nella conformità della protezione dei dati e della sicurezza delle informazioni.

Le aziende hanno molte possibilità per assicurare la protezione dei loro dati, sia a livello organizzativo che tecnico. Da un punto di vista organizzativo, possono implementare processi che assicurano che solo una quantità marginale di dati venga raccolta, che gli archivi fisici e digitali siano protetti, che l'accesso ai dati sia limitato al personale rilevante, ecc. L'analisi e l'implementazione di queste misure sono di competenza del responsabile della sicurezza dell'informazione in collaborazione e con l'appoggio della direzione dell'azienda.

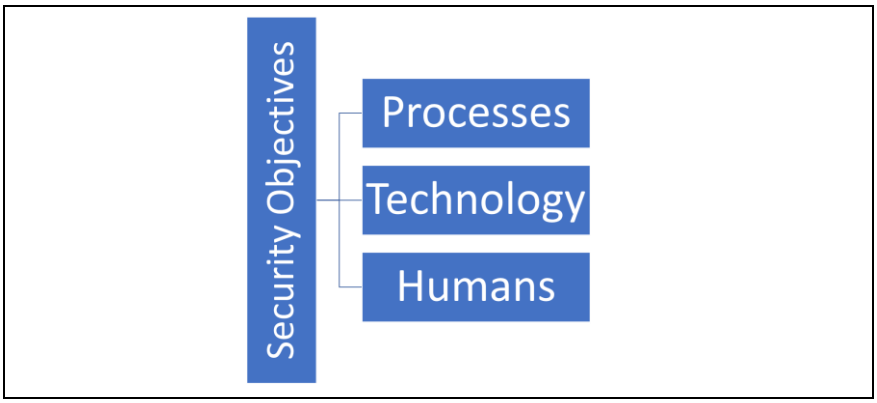

Figura 11: Dimensioni di rischio per gli obiettivi di sicurezza

A livello tecnico, si possono progettare programmi e applicazioni che assicurano la conformità con la legge sulla protezione dei dati e i regolamenti specifici dell'azienda, cioè la privacy by design. I fornitori di servizi hanno iniziato a fare modello di business dalle piattaforme Software as a Service (SaaS), implementando la Privacy as a Service (PaaS). In questo modo, con il consenso dell'utente, l'archiviazione e l'elaborazione delle informazioni si concentra su un comportamento corretto secondo l'esigenza individuale. Inoltre, l'importanza di un software sicuro ha sperimentato un forte aumento negli ultimi anni, poiché le perdite diventano più facilmente note al pubblico e possono danneggiare la reputazione delle aziende. Di conseguenza, le aziende hanno guadagnato un interesse nella progettazione di software sicuro e nella costruzione della fiducia tra i loro utenti - ottenendo un vantaggio competitivo sul mercato.

Infine, le imprese devono rispettare la dimensione umana nel contesto della protezione del loro know how e dei dati critici. È l'utente e l'attore dell'azienda, che aziona macchine e tecnologie, svolge compiti e supervisiona i processi. Mentre sia la tecnologia che i processi dispongono di un'affidabilità molto alta, gli impiegati

tendono a commettere errori, poiché sono soggetti alla "razionalità limitata" (Simon 1990). Infatti, circa l'88% delle violazioni di dati o perdite di informazioni può essere attribuito a errori umani, rendendo questa dimensione la più importante per garantire la sicurezza dei dati in un'azienda. (Tessian 2021)

In breve, il concetto di razionalità limitata rifiuta l'assunzione che il pensiero, il comportamento e l'azione degli esseri umani siano guidati da una razionalità completa, poiché ciò richiederebbe una capacità cognitiva illimitata per elaborare ogni informazione disponibile immediatamente e prendere decisioni pienamente informate. Invece, si assume che gli esseri umani massimizzino la loro utilità individuale, cioè scelgono un'azione che soddisfa maggiormente il loro bisogno percepito (il cosiddetto "Satisficing"). Infine, una persona potrebbe anche giungere alla conclusione che le mancano informazioni per prendere una decisione, ma che la ricerca di queste informazioni comporterebbe una quantità significativa di tempo ed energia. Di conseguenza, la persona decide di intraprendere un'azione con informazioni incomplete, poiché i costi di opportunità (tempo ed energia) superano l'utilità di avere quelle specifiche informazioni.

Tra queste azioni, impostare password facili (o scriverle in un post-it), ritardare gli aggiornamenti di sicurezza, conservare informazioni sensibili negli armadietti, usare quel bastone trovato in ascensore sono solo alcune delle conseguenze sconsigliate. L'assenza di informazioni complete e gli alti costi di opportunità percepiti nei momenti di fretta e pressione sono sempre più sfruttati dagli attacchi di ingegneria sociale, in cui un intruso crea uno scenario via mail o via telefono, che evoca l'urgenza di agire nella speranza che il dipendente lasci da parte i protocolli di sicurezza, fornendo volontariamente informazioni critiche (es. password, informazioni finanziarie ecc.).

Sfortunatamente, aderire a una condotta corretta nella vita lavorativa quotidiana richiede un'energia extra - che è spesso una risorsa scarsa in ambienti di lavoro produttivi o frenetici. Sullo sfondo delle routine di lavoro stabilite, cambiare gli atteggiamenti, le credenze e infine il comportamento rappresenta una grande sfida sia per l'azienda, ma anche per i suoi dipendenti. Finora, l'insegnamento, la formazione e la sensibilizzazione dei dipendenti al fine di aumentare la consapevolezza della costante minaccia ai beni più preziosi delle aziende - il suo know-how e i suoi dati - è più importante che mai. E con la diminuzione delle difficoltà di lanciare qualsiasi tipo di attacco, sempre più PMI devono affrontare una nuova realtà: sono già, o molto probabilmente saranno, soggette ad attacchi mirati. Quindi, cosa si può fare?

3 Strategia TeBeISi

Il progetto TeBeISi ha analizzato la situazione della sicurezza delle informazioni, anche rispetto all'attuazione del GDPR, a livello aziendale negli stati membri partner. Dopo aver esaminato i profili professionali attualmente esistenti, le qualifiche formali e le certificazioni, è stata condotta una corrispondenza tra le competenze trasferibili attualmente esistenti e i requisiti generati dall'analisi quantitativa e qualitativa.

3.1 Collegare l'istruzione superiore e la formazione sul lavoro

Dopo aver esaminato tutte le informazioni raccolte attraverso la ricerca quantitativa e qualitativa, il progetto è giunto alla conclusione che la sicurezza dell'informazione è predestinata a fornire un mix di formazione professionale e istruzione superiore. Ci sono tre ragioni che alimentano questa idea:

1. Attività operative: La maggior parte dei compiti richiesti in una PMI sono di natura piuttosto routinaria. Il grado di trasferimento delle conoscenze e di ricontestualizzazione rimane basso, poiché la tecnologia e i processi rimangono ad un livello standardizzato, con le aziende che fanno uso di software EDP e canali di comunicazione standardizzati. La maggior parte delle PMI può ottenere un aumento significativo del proprio livello di sicurezza attenendosi alla regola del 20:80 (o simile) - si raggiunge l'80% di sicurezza facendo il 20% del lavoro necessario per raggiungere il 100%. Naturalmente, questo non è possibile considerando la protezione dei dati, che è obbligatoria per legge e per la quale le aziende sono obbligate a soddisfare le richieste del GDPR. Le conseguenze di questa constatazione sono molteplici: le aziende devono prendere in considerazione se vogliono raggiungere una certificazione specifica (a causa della natura del loro prodotto, i requisiti del mercato, ecc), se possiedono risorse che richiedono misure di protezione più che routinarie, ecc. Così, le PMI si trovano spesso in una posizione in cui l'aderenza strutturale alle misure di sicurezza di base fornisce un significativo aumento del livello di sicurezza generale e una significativa diminuzione dell'esposizione al rischio in un trade-off efficace dal punto di vista dei costi.
2. Obblighi legali: Nonostante la possibilità di svolgere compiti routinari in un ambiente di lavoro strutturato, alcuni aspetti della sicurezza delle informazioni toccano anche aspetti legali, soprattutto per quanto riguarda l'attuazione di un corretto trattamento dei dati a seguito del GDPR. A causa della complessità di trattare con le normative nazionali, al personale responsabile è richiesto di possedere la competenza per affrontare la legislazione e la corretta implementazione. Questa responsabilità comporta un alto grado di capacità di ricontestualizzare e trasferire la conoscenza astratta in un ambiente di lavoro. Mentre il grado di complessità rimane superabile per quanto riguarda la parte tecnica della sicurezza dell'informazione descritta al punto (1), la parte legale

richiede una formazione e un'esecuzione diligente per conformarsi alle rispettive leggi.

3.

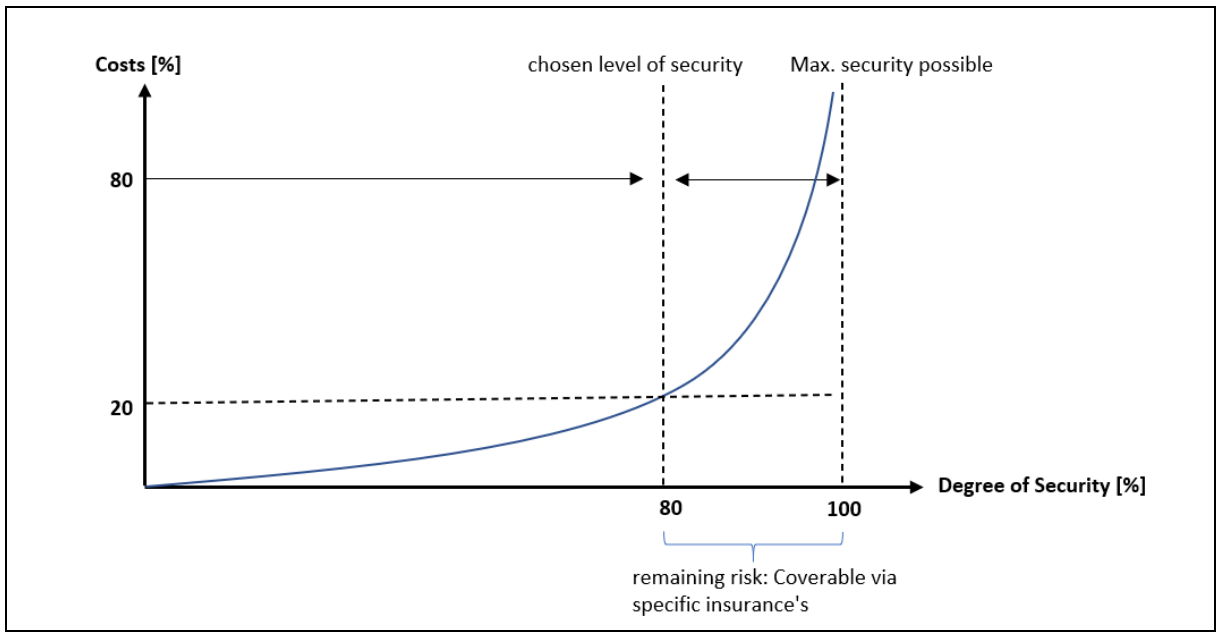

Figura 12: Trade-off costo-sicurezza degli investimenti nella sicurezza delle informazioni

Il lavoro dei responsabili della sicurezza delle informazioni richiede molteplici abilità sociali. Come descritto al punto 2.3, la più grande minaccia alla sicurezza di un'azienda è rappresentata dai suoi impiegati. Cambiare l'atteggiamento dei colleghi, influenzare le loro routine di lavoro e stabilire una cultura della sicurezza delle informazioni nell'azienda rappresentano, senza dubbio, la più grande sfida nell'implementazione di un sistema di sicurezza delle informazioni. Il responsabile è tenuto ad attivare, collaborare, guidare, fare da mentore e conciliare dipendenti, manager e sicurezza dell'informazione. Non sorprende che le imprese apprezzino i professionisti con esperienza sul lavoro - e che valutino l'esperienza pratica più di qualsiasi qualifica formale (cfr. lo studio "Information Security Education for SMEs"). Ricevere una formazione pratica insegna le insidie della collaborazione quotidiana con i colleghi e le competenze per interagire in modo produttivo con gli stakeholder dell'azienda.

L'educazione alla sicurezza dell'informazione, quando esiste, attualmente si concentra fortemente sull'insegnamento e la formazione di competenze tecniche, sia nel campo dell'informatica che del diritto. L'acquisizione di esperienze pratiche, specialmente strategie di comunicazione efficaci, solo raramente trova la sua strada nei curricula educativi. TeBeISi suggerisce quindi di connettere il meglio dei due mondi, e di fornire un'educazione attraverso l'istruzione e la formazione professionale e l'istruzione superiore.

3.2 Utilizzare gli strumenti europei

La connessione tra l'istruzione e la formazione professionale e l'istruzione superiore è stata definita dalla Commissione Europea come fattibile all'interno del Quadro Europeo delle Qualifiche (EQF). Inoltre, il sistema europeo di crediti per l'istruzione e la formazione professionale (ECVET) deve essere utilizzato per fornire trasparenza e comparabilità nell'istruzione e formazione professionale. Infine, facendo riferimento al quadro europeo delle abilità/competenze, qualifiche e occupazioni (ESCO), le singole competenze possono essere formulate in modo da renderle riutilizzabili e riconoscibili in diversi contesti professionali.

L'uso di strumenti europei distingue un processo di certificazione trasparente dal già esistente e disorganizzato mercato delle certificazioni di fornitori privati. Va ribadito che esistono molteplici credenziali, anche nel campo delle PMI, tuttavia non è chiaro fino a che punto vengano utilizzati standard comuni di qualità e garanzia della qualità, il che comporta una mancanza di trasparenza e trasferibilità tra i paesi. L'arretratezza dei sistemi europei di accreditamento, garanzia di qualità e standard di competenza permette un'ampia e trasparente diffusione delle certificazioni attraverso i sistemi educativi e i paesaggi di certificazione istituzionalizzati.

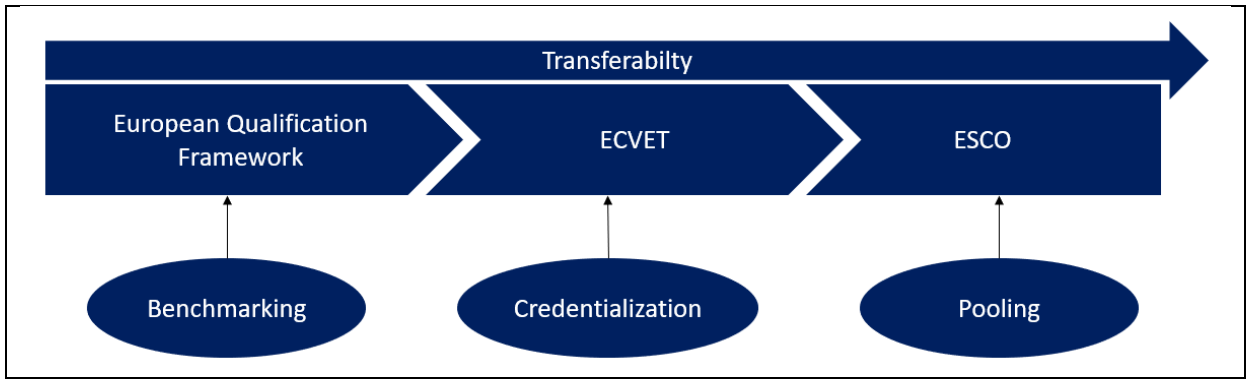

Figura 13: Strumenti di trasparenza per VET nell'UE

In breve, questi strumenti sostengono la diffusione delle competenze e delle qualifiche in tutta l'UE. L'EQF come sistema di benchmarking categorizza le qualifiche secondo le loro abilità, competenze e autonomia sottostanti e fornisce la possibilità di inserire ogni qualifica dei diversi sistemi educativi in un unico schema di riferimento, che rende le diverse qualifiche comparabili tra i diversi contesti educativi. ECVET, nel frattempo, fornisce la base per raggruppare i risultati dell'apprendimento in crediti di apprendimento, fornendo una visione del volume e della profondità dell'apprendimento dietro una qualifica. Inoltre, supporta la garanzia della qualità, fornisce possibilità di formazione continua in contesti regionali specifici e supporta il riconoscimento delle qualifiche professionali in diversi sistemi o percorsi educativi nazionali. Infine, ESCO rappresenta un database unificante che riunisce le qualifiche e le competenze esistenti in tutta l'UE. Ritornando a questo database quando si creano nuovi curricula, si può garantire che le competenze siano comprese in diversi contesti di apprendimento.

3.2.1 EQF – Quadro Europeo delle Qualifiche

Il Quadro Europeo delle Qualifiche stabilisce una sistematizzazione delle qualifiche formali tra i sistemi educativi dell'Unione Europea. Lo scopo di questo quadro è di rendere le qualifiche comparabili tra i paesi e, di conseguenza, aumentare la comprensione del valore di una qualifica all'estero. Poiché i sistemi educativi variano ampiamente tra gli stati membri dell'UE, l'EQF può essere usato come riferimento per assicurare l'equivalenza delle competenze insegnate. Nel contesto TeBeISi, il livello 5 dell'EQF è stato identificato per fornire preziose opportunità alle aziende e agli studenti.

I risultati di apprendimento rilevanti per il livello 5 sono		
Saperi	Abilità	Competenze
una conoscenza completa, specializzata, fattuale e teorica in un campo di lavoro o di studio e una consapevolezza dei limiti di tale conoscenza	una gamma completa di abilità cognitive e pratiche necessarie per sviluppare soluzioni creative a problemi astratti	- esercitare la gestione e la supervisione in contesti di lavoro o di studio - attività in cui c'è un cambiamento imprevedibile rivedere e sviluppare le prestazioni di sé e degli altri

Tabella 6: EQF Levello 5 Risultati dell'apprendimento - Saperi - Abilità - Competenze

Fonte: Commissione Europea (2008)

Considerando un avvertimento chiave del progetto, che la maggior parte del personale disponibile è probabilmente sovraqualificato per le esigenze delle PMI (che si riflette anche nei profili professionali esistenti nelle ESCO), devono essere trovati mezzi adeguati per allineare la complessità intrinseca dei compiti di sicurezza delle informazioni (cioè il know-how IT e la conoscenza giuridica), e i requisiti minimi delle PMI al fine di indirizzare i nuovi discenti nel campo. Si può concludere che a causa della natura di alcuni compiti, specialmente quelli relativi ad attività non standardizzate o che coinvolgono competenze legali, alcuni elementi dell'educazione alla sicurezza dell'informazione per le PMI hanno bisogno di essere radicati nell'istruzione superiore, che permette agli allievi di operare in un ambiente meno strutturato e più indipendente. In particolare, le competenze relative al diritto, cioè soprattutto il GDPR, rientrano in questa categoria.

L'uso di EQF 5 fornisce diversi vantaggi che possono essere sfruttati. In primo luogo, fornisce un terreno per molti dipendenti con qualificazione EQF 4 per trovare un ingresso nella formazione continua. Di conseguenza, la convalida parziale a questo livello può essere facilitata dal riconoscimento dell'esperienza lavorativa precedente, dell'apprendimento non formale e informale. La connessione all'EQF 6 colma il divario e l'adattabilità per le istituzioni di istruzione superiore, che mirano a fornire o una qualifica completa nel contesto della sicurezza dell'informazione o una qualifica aggiuntiva ai loro studenti.

3.2.2 ECVET

From a functional perspective, the learning outcome-oriented operationalization of competences represents a shift in perspective from “What do I want to teach?” to “What should learners learn?”. The result of the learning process represents the focus of the learning process and provides learners with a clearer view on their own learning progress. With the usage of a transparent credit system, several positive externalities can be realized which differentiate the modularized education path from existing certification systems.

The dispersion of the TeBeISi competence profile of an information security and data protection officer in SME into modularized learning fields (c.f. “Curriculum”) facilitates the modularization of learning fields and the application of credit transfer systems like ECTS or ECVET. ECVET. The modularization (micro-credentialization) provides several advantages, illustrated in Figura 14, leading to increased transparency, mobility and trustworthiness of the partial qualifications. The modules can both be used for training and education purposes of employees or students or used as a means of partial validation by making the certification process available to lateral entrants from the field of information security.

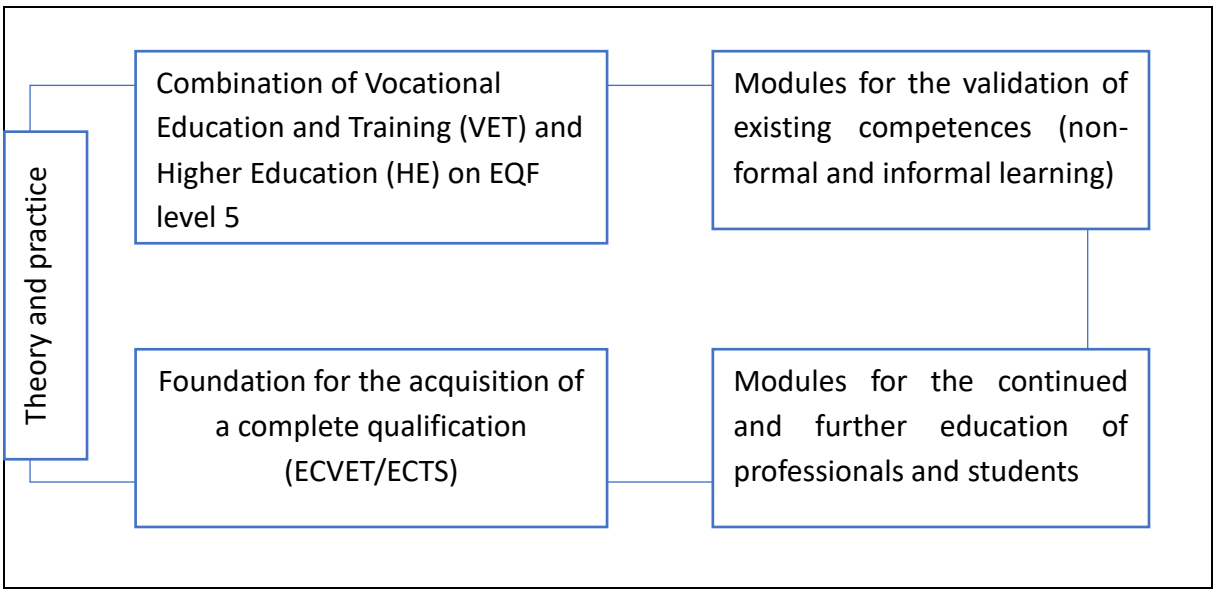

Figura 14: Vantaggi delle qualifiche modularizzate

Considerando i sistemi di validazione esistenti, l'affidabilità gioca un ruolo cruciale nell'accettazione del processo di certificazione tra i datori di lavoro e i fornitori di formazione. Lì, oltre agli standard di garanzia della qualità esistenti (per esempio EQAVET), devono essere presi in considerazione dettagli specifici riguardanti la valutazione delle competenze per assicurare la massima validità possibile della procedura di validazione.

3.3 Misurare i risultati dell'apprendiment

La misurazione dei risultati dell'apprendimento rimane un punto di forte discussione, nel frattempo esistono le migliori pratiche, ad esempio VALIKOM o MySkills dalla Germania, l'ampia adozione di questi metodi non può rispondere a tutte le critiche sollevate dalle aziende e dai professionisti della valutazione. In particolare, tra i fornitori di formazione rimane la questione se le valutazioni brevi siano una forma adatta a sostituire un intero curriculum di formazione. Per aumentare la validità del processo di misurazione, devono essere presi in considerazione diversi punti:

1. Processi trasparenti. La trasparenza dell'intero processo di riconoscimento è fondamentale. Una discussione di ingresso, l'assegnazione di un mentore dedicato e la preparazione adeguata per la valutazione devono essere inclusi in un processo di riconoscimento olistico e pianificato passo dopo passo.

2. Il riconoscimento stesso deve prendere in considerazione diverse misure per assicurare la massima validità possibile della valutazione. In generale, forme specifiche di valutazione sono più adatte a valutare forme specifiche di competenze. Mentre i test scritti, che siano a risposta aperta o a scelta multipla, sono adatti a valutare le conoscenze, i giochi di ruolo, gli esercizi di post box o il pitch presentation gaming sono orientati a testare le competenze comunicative e sociali come il colloquio, la retorica, l'argomentazione, l'empatia, l'assertività, la persuasività, la sensibilità (osservazione comportamentale). Sono anche utili per valutare la prontezza operativa, l'orientamento all'obiettivo, la tolleranza alla frustrazione, la persistenza, la capacità di risolvere i problemi, la capacità analitica, la capacità di prendere decisioni ecc. I metodi biografici come le interviste basate sui criteri, l'esame di un portfolio strutturato e le discussioni tecniche i candidati ottengono una visione completa dei propri risultati e imparano a valutare se stessi e le loro qualità. Infine, le osservazioni a vista e in un ambiente simulato permettono di osservare le reazioni in scenari di vita reale, la condotta personale e l'approccio agli eventi spontanei. Quindi, con una miscela di metodi di valutazione, le competenze granulari possono essere triangolate e la disposizione affidabile determinata.

3. Per condurre valutazioni obiettive, i valutatori devono essere addestrati a trattare con diversi metodi di valutazione, diversi pregiudizi di valutazione e diversi candidati in modo equo, trasparente e obiettivo. I valutatori devono essere consapevoli delle diverse biografie di apprendimento e dei diversi obiettivi dei candidati e comprendere l'intero processo di validazione e riconoscimento.

4. Le autovalutazioni come passo verso la valutazione sono raccomandate, ma le autovalutazioni come fonte di valutazione non sono raccomandate. Le autovalutazioni sia sotto forma di valutazioni tecniche ("il candidato X sa..." "sì", "no") o sotto forma di test di personalità possono dare risultati indicativi, tuttavia l'affidabilità e l'obiettività di questi risultati sono da mettere in dubbio.

Pertanto, una struttura dettagliata e un sistema di assicurazione della qualità devono essere messi in atto per garantire una valutazione affidabile, obiettiva e trasparente e per creare fiducia tra le istituzioni educative e i datori di lavoro.

4 Tendenze e racommandazioni

La carenza di manodopera qualificata nel settore della sicurezza dell'informazione rimane persistente in tutta l'UE. Le competenze tecniche dei professionisti sono sempre più irrilevanti rispetto alle competenze sociali e personali. Gli investimenti nel capitale umano, cioè la formazione adeguata dei dipendenti, sono sempre più redditizi di fronte a situazioni di rischio diffuse, come i vettori di attacco multidimensionali nello spazio fisico e digitale. La sicurezza del know-how di un'azienda e la prontezza dei servizi interni ed esterni è sempre più abbinata a nuovi potenziali di sfruttamento. Ma alla fine, tutte le nuove tecnologie e le linee guida introdotte per contenere il rischio di violazioni ostili sono vanificate se i dipendenti dell'azienda non acconsentono e vivono attivamente la cultura della sicurezza aziendale.

La consapevolezza dei rischi e l'aderenza alle politiche sono il punto di partenza per diminuire i rischi di qualsiasi tipo di attacco. Per ottenere questo, i valori, le credenze e, in ultima analisi, il comportamento delle persone in un'azienda devono essere cambiati al fine di stabilire una cultura del rischio vitale. Lo spostamento dell'attenzione dalla parte tecnica del problema di fondo verso il fattore umano rende chiaro che l'istruzione e la formazione devono essere pensate anche da questo punto di vista.

L'aumento dell'attività criminale in relazione alle informazioni private e confidenziali nell'era digitale pone questioni non solo alla formazione delle capacità negli ambienti professionali e nell'ambito lavorativo, ma anche alla sfera privata dei cittadini europei. Anche se gli attacchi contro le aziende causano danni significativi all'economia europea, è importante sottolineare le ramificazioni dell'aumento dell'attività criminale nel contesto delle informazioni riservate: si rivolge agli individui, non alle aziende. Di conseguenza, costruire capacità tra i cittadini attraverso l'istruzione primaria e la formazione creerebbe esternalità positive per le imprese e la società. Lo sviluppo delle capacità non dovrebbe quindi essere considerato solo l'interesse delle singole imprese - ma del pubblico in generale. L'introduzione di una formazione di consapevolezza, la conduzione di informazioni sensibili e la comprensione della propria esposizione ad attacchi ostili nelle scuole, negli istituti di formazione professionale e superiore. Nel 2018, il Consiglio dell'Unione europea ha ridefinito la "competenza civica" come

"la capacità di agire come cittadini responsabili e di partecipare pienamente alla vita civica e sociale, sulla base di una comprensione dei concetti e delle strutture sociali, economiche, giuridiche e politiche, così come degli sviluppi globali e della sostenibilità".

La partecipazione come cittadini maturi nel mondo di oggi e di domani è strettamente legata alla capacità di separare il danno intenzionale dagli incidenti quotidiani. Individuare la disinformazione, la manipolazione, la tutela della privacy e la sicurezza digitale sono una questione di resilienza civica - e non dovrebbero essere limitate a una questione di spesa redditizia in società private. In definitiva, è nell'interesse dell'Unione europea e dei suoi stati membri - e quindi una domanda a cui devono rispondere i ministeri dell'educazione - non solo i dipartimenti IT.

Di conseguenza, i seguenti mezzi sono raccomandati per costruire capacità tra i cittadini europei:

1. Fondazione di un'organizzazione europea per la protezione delle informazioni e dei dati privati. L'implementazione di un punto di contatto, un'arena per le convinzioni condivise in una questione critica e una piattaforma per lo scambio di conoscenze e per le campagne di interesse è una parte cruciale per guidare l'interesse civico, pubblico e aziendale. L'obiettivo principale, la promozione delle restanti raccomandazioni elencate di seguito, sono il cuore di un'organizzazione comune.

2. Introdurre la "sicurezza delle informazioni" nei curricula di apprendistato ceteris paribus "salute e sicurezza". È economicamente impossibile cambiare i valori, le credenze e le azioni umane. Pertanto, è importante impegnarsi nel processo di formazione, e insegnare agli individui l'importanza della consapevolezza verso scenari di minacce diffuse, tra cui la manipolazione mirata e la disinformazione nell'era digitale.

3. Introdurre Micro-Credenziali e schemi di certificazione parziale per la Sicurezza dell'Informazione per la ricezione privata e professionale. La situazione attuale nella formazione continua rimane poco trasparente e manca di una visione strutturata verso il futuro. Accanto agli schemi di certificazione esistenti, curricula completi, costruiti da moduli singoli e formabili, forniscono molteplici opportunità di utilizzo e replica. Possono essere integrati nella formazione VET (EQF 4) e nell'istruzione superiore (EQF 6-7) a seconda della materia, combinati in un unico percorso formativo che collega la formazione sul lavoro e l'istruzione superiore (EQF5), o essere offerti ai dipendenti come opportunità di formazione continua. La modularizzazione permette un modello di formazione mirato e meno complesso e dispendioso in termini di risorse, con minori costi e maggiori opportunità per le PMI.

4. Aumentare l'uso degli strumenti di trasparenza europei per sostenere la flessibilità sul mercato del lavoro e attrarre nuovi talenti.

5 Letteratura

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.

Austrian Press Agency (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): European qualifications framework (EQF). 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 Directive (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.

European Commission (Hg.) (2008): Explaining the European Qualifications Framework for Lifelong Learning. Office for Official Publications of the European Communities. Luxembourg. Online verfügbar unter https://europa.eu/europass/system/files/2020-05/EQF-Archives-EN.pdf, zuletzt geprüft am 05.07.2021.

European Commission (2020a): COM/2020/66 final. A European strategy for data. Brussels.

European Commission (02.06.2020): Commission launches consultation to seek views on Digital Services. Online verfügbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962.

European Commission (2020b): COM/2020/264 final. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. Brussels.

Eurostat (2021): Purchasing power adjusted GDP per capita. Online verfügbar unter https://ec.europa.eu/eurostat/databrowser/view/sdg_10_10/default/table?lang=en, zuletzt geprüft am 23.07.2021.

Federal Ministry of Finance (BMF): Data Protection. 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.

Office for Personal Data Protection (2018): Personal Data Protection at the Workplace. Guidebook for Employers. Warsaw. Online verfügbar unter https://uodo.gov.pl/pl/file/1469.

Rechtsinformationssystem des Bundes (RIS) (1999): Federal Act concerning the Protection of Personal Data (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): The Psychology of Human Error | 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): The 10 biggest mistakes in ensuring compliance with RODO. Warsaw. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/05/10-najwiekszych-bledow-przy-wdrazaniu-RODO.pdf.

ZFODO (2021): Breaches in personal data protection 2020. Warsaw. Online verfügbar unter https://www.zfodo.org.pl/wp-content/uploads/2020/11/Breach-report-2020-ZFODO.pdf, zuletzt geprüft am 07.07.2021.

Strategic Report

Ringraziamo i co-autori:

BF/M-Bayreuth

Mykolas Romeris University

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Co-finanziato dal programma Erasmus+ dell'Unione Europea

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