# Raport strategiczny

Budowanie potencjału w zakresie bezpieczeństwa informacji wśród obywateli i pracowników europejskich

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union



Niniejszy dokument powstał w ramach projektu ERASMUS+ "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi", ID projektu: 2018-1-EN02-KA202-005218

# Spis treści

# Spis wykresów



# Spis tabel

# 1 Wprowadzenie

Wchodząc w życie w 2018 r., Rozporządzenie o Ochronie Danych Osobowych (RODO) wywołało zmianę w postrzeganiu i wartości danych osobowych wśród konsumentów, firm i całego społeczeństwa. Wprowadzenie wiążących i sankcjonowalnych standardów i przepisów dotyczących gromadzenia, przechowywania i przetwarzania danych osobowych miało wzmocnić prawa konsumentów, wyznaczyć granice wykorzystywania i gromadzenia danych, a ostatecznie zwiększyć i zapewnić prawo do prywatności i wolności osobistej w erze cyfrowej.

Od tego czasu, po wielu publicznych dyskusjach na temat sensu i bezsensu oraz za i przeciw, pierwsze tarcia zostały przezwyciężone, a początkowa fala zainteresowania uległa wyhamowaniu. Ochrona danych stała się nieodłącznym elementem pracy każdej organizacji. Nie tylko firmy są zobowiązane do przydzielenia odpowiedzialności za prawidłowy przebieg ochrony danych w firmie, ale każdy pracownik musi być świadomy potencjalnych naruszeń ochrony danych w swojej pracy i przestrzegania ustalonych procedur. Wreszcie, sami pracownicy są zainteresowani ochroną swoich danych w momencie nawiązywania stosunku pracy, co jest objęte ochroną danych osobowych pracowników. Pracownicy jako najsłabsze ogniwo w strategii bezpieczeństwa informacji firmy muszą więc być przedmiotem szczególnej uwagi. W międzyczasie duże korporacje z powodzeniem uruchomiły szereg programów edukacyjnych w celu podniesienia świadomości swoich pracowników, natomiast priorytety małych i średnich przedsiębiorstw (MŚP) w zakresie budowania bezpieczeństwa informacji i zdolności ochrony danych pozostały na niskim poziomie.

Bezpieczeństwo Informacji, w przeciwieństwie do Ochrony Danych Osobowych, nie stanowi pozycji obligatoryjnej, ani nie nakłada żadnych prawnie wiążących obciążeń na pracę organizacji. Dotyka ono jednak wielu aspektów przetwarzania, gromadzenia i przechowywania danych, a tym samym wymaga szerokiego wykształcenia i przeszkolenia odpowiedzialnego personelu. Edukacja i szkolenie, szczególnie w kontekście ochrony know-how firmy, pozostaje głównym aspektem zwiększania bezpieczeństwa MŚP w UE. W niniejszym raporcie staramy się przedstawić założenia i perspektywy kształcenia i szkolenia w zakresie bezpieczeństwa informacji i kompetencji ochrony danych w UE oraz przedstawić zalecenia dotyczące dalszego rozwoju, szczególnie w środowisku MŚP.

# 2 Ochrona danych w krajach partnerskich

## 2.1 Polska

| Nazwa Instytucji | Krótki Opis | Strona internetowa |
|---|---|---|
| Urząd Ochrony Danych Osobowych (UODO) | UODO jest głównym organem państwowym zajmującym się ochroną danych osobowych. W ramach zadań wyznaczonych przez art. 57 RODO, organ ten m.in.: monitoruje i egzekwuje stosowanie RODO; upowszechnia w społeczeństwie wiedzę o ryzyku, regulacjach, zabezpieczeniach i prawach związanych z przetwarzaniem danych, a także zrozumienie tych zjawisk; doradza parlamentowi, rządowi oraz innym instytucjom i organom w sprawach ochrony danych, rozpatruje skargi złożone przez osoby lub instytucje, których dane dotyczą; prowadzi postępowania dotyczące stosowania RODO, wydaje decyzje, a jeśli jest to właściwe - ustala wysokość administracyjnych kar pieniężnych za naruszenia RODO i je nakłada. | https://uodo.gov.pl/ |
| Centrum GovTech | Centrum GovTech przejęło część obowiązków od Ministerstwa Cyfryzacji, które zostało zlikwidowane jesienią 2020 roku.<br>Bezpośrednimi odbiorcami usług GovTech jest szeroko rozumiana administracja samorządowa i centralna, a także inne podmioty realizujące zadania publiczne, takie jak szpitale, szkoły czy firmy transportowe. Odbiorcami usług GovTech jest sektor publiczny, ale także przedsiębiorstwa. | https://www.gov.pl/web/govtech |
| Fundacja Panoptykon | Fundacja Panoptykon monitoruje praktyki inwigilacji. Bada obowiązujące prawo, skłonności legislacyjne, działania władz publicznych i firm prywatnych. Śledzi doniesienia medialne i obywatelskie. Analizuje zebrane informacje, diagnozuje problemy i reaguje. Opiniuje propozycje nowych przepisów, zgłasza zastrzeżenia do istniejącego prawa i własne propozycje zmian. Wskazuje na nadużycia i zaniedbania. | www.panoptykon.org |
| Państwowy Instytut Badawczy NASK | NASK - państwowy instytut badawczy nadzorowany przez Kancelarię Prezesa Rady Ministrów.<br>Jego misją jest poszukiwanie i wdrażanie rozwiązań służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa. Instytut prowadzi badania naukowe, prace rozwojowe, a także działalność operacyjną na rzecz bezpieczeństwa polskiej cyberprzestrzeni cywilnej. Ważnym elementem działalności NASK jest również edukacja użytkowników i propagowanie idei społeczeństwa informacyjnego, głównie w celu | www.nask.pl |

| | | |
|---|---|---|
| | ochrony dzieci i młodzieży przed zagrożeniami związanymi z korzystaniem z nowych technologii. | |
| ZFODO Związek Firm Ochrony Danych Osobwych | Firmy zrzeszone w Związku Firm Ochrony Danych Osobowych posiadają wieloletnie doświadczenie w doradztwie biznesowym w zakresie ochrony danych osobowych.<br>Świadczą profesjonalne usługi na najwyższym poziomie dla największych firm z sektora prywatnego, a także jednostek administracji samorządowej i rządowej.<br><br>Posiadają doświadczenie w wielu sektorach i branżach, dzięki czemu mogą zaoferować swoim klientom indywidualne rozwiązania dostosowane do ich potrzeb. Posiadają wielu partnerów biznesowych - kancelarie prawne, firmy doradcze z zakresu IT i marketingu. Dzięki temu są w stanie kompleksowo doradzać swoim klientom - nie tylko w zakresie ochrony danych osobowych, ale także w obszarze całego biznesu ich klientów. | www.zfodo.org.pl |
| Fundacja Wiedza To Bezpieczeństwo | Fundacja popularyzuje wiedzę z zakresu bezpieczeństwa informacji. Organizuje konferencje naukowe, pomaga rozwiązywać problemy, z którymi ludzie spotykają się w życiu codziennym, zarówno prywatnym, jak i biznesowym.<br>Prowadzi kampanie społeczne mające na celu podnoszenie świadomości. W ten sposób pokazuje jakie niebezpieczeństwa grożą w związku z bezprawnym wykorzystaniem danych osobowych. | https://wtb.org.pl/ |

**Tabela 1: Interesariusze z Polski.**

Wśród najczęstszych błędów w związku z wdrożeniem RODO w polskich firmach według raportu "10 największych błędów w zapewnieniu zgodności z RODO" Związek Firm Ochrony Danych Osobowych (ZFODO) wymienia najczęściej:

- Niezrozumienie idei RODO, czyli wdrażanie jej tylko "na papierze". W efekcie nikt nie zna i nie przestrzega jego procedur. Brak wdrożenia może skutkować sankcjami ze strony organu nadzorczego.
- Brak odpowiedniej świadomości w zakresie bezpieczeństwa informacji. Przeprowadzanie analizy ryzyka przez osoby niewykwalifikowane lub ze zbyt małym doświadczeniem, co skutkuje brakiem lub nieprawidłowym przeprowadzeniem analizy. Efektem tego są niezidentyfikowane zagrożenia, możliwość utraty danych, brak bezpieczeństwa.
- Nieodpowiedni obszar IT, brak zidentyfikowanej polityki retencji danych lub brak wdrożenia zasad retencji w systemach teleinformatycznych. Efektem może być utrata danych lub nieuprawniony dostęp do danych oraz brak możliwości realizacji uprawnień, których dane dotyczą.

Ponadto wymieniano: nieprawidłową ocenę skutków dla ochrony danych, nieuregulowanie relacji powierzenia danych pomiędzy podmiotami, mylenie pojęć

administratora i podmiotu przetwarzającego, brak wdrożenia procedury obowiązku informacyjnego, brak koordynatora wdrażania procedur, brak świadomości pracowników, brak całościowego spojrzenia na wdrożenie.

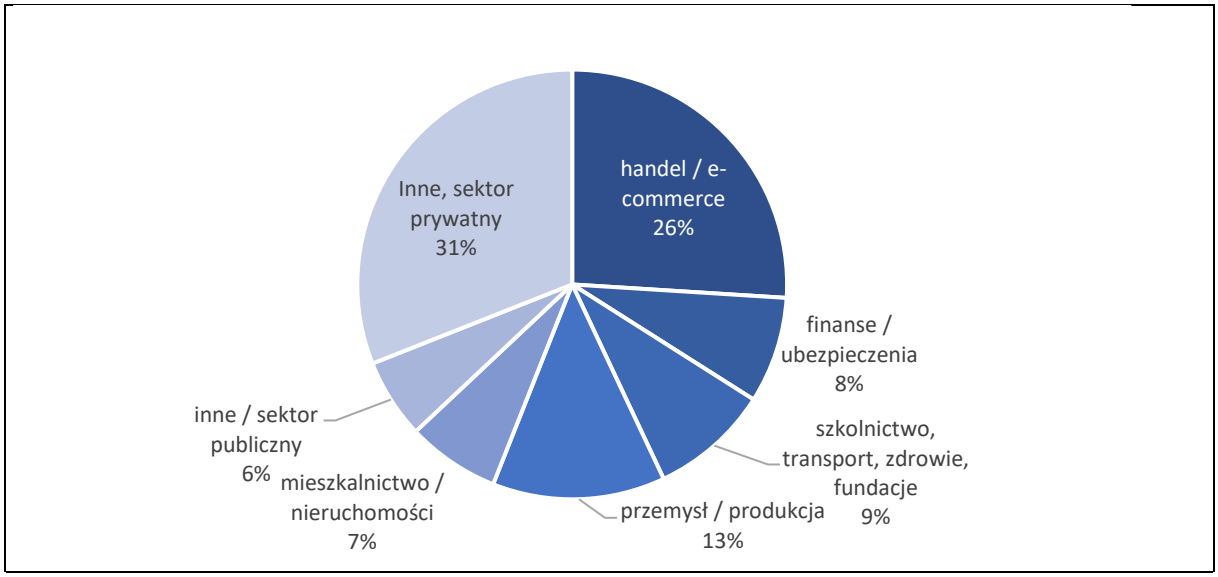
Wymienione wyżej obszary to "grzechy główne", ale są też inne aspekty wdrożenia nowych regulacji, które okazały się problematyczne.

Przykładowo, najczęściej niedoceniana jest rola inspektora ochrony danych, a jego pozycja w organizacji jest niska. Często IOD jest osobą wybraną "z ręki". Rola IOD jest często niedoceniana, a jego pozycja w strukturze organizacyjnej jest niska. IOD jest często rekrutowany, nie posiada odpowiednich kwalifikacji i ma niewielki wpływ na decyzje podejmowane przez najwyższe kierownictwo, jego głos jest traktowany jedynie jako doradczy. Raport został opublikowany w języku polskim przez (ZFODO 2020) ZFODO (2020).

O tym, jak RODO zostało wdrożone w praktyce oraz o skali naruszeń i incydentów związanych z ochroną danych osobowych wśród polskich firm i instytucji opowiada m.in. raport przygotowany przez Związek Firm Ochrony Danych Osobowych (ZFODO).

Raport objął 454 organizacje obsługiwane przez Firmy zrzeszone w ZFODO w okresie maj 2019 - maj 2020. Wśród badanych znalazły się organizacje i firmy zarówno z sektora prywatnego, jak i publicznego. Ze statystyk wynika, że incydent (incydent ochrony danych) zdarza się przeciętnemu administratorowi statystycznie 0,65 razy w ciągu roku. Jest to niewystarczająca ilość, aby zdobyć niezbędną praktykę w unikaniu lub zarządzaniu takimi incydentami, podczas gdy błąd w obsłudze nawet pojedynczego incydentu może mieć katastrofalne skutki dla biznesu.

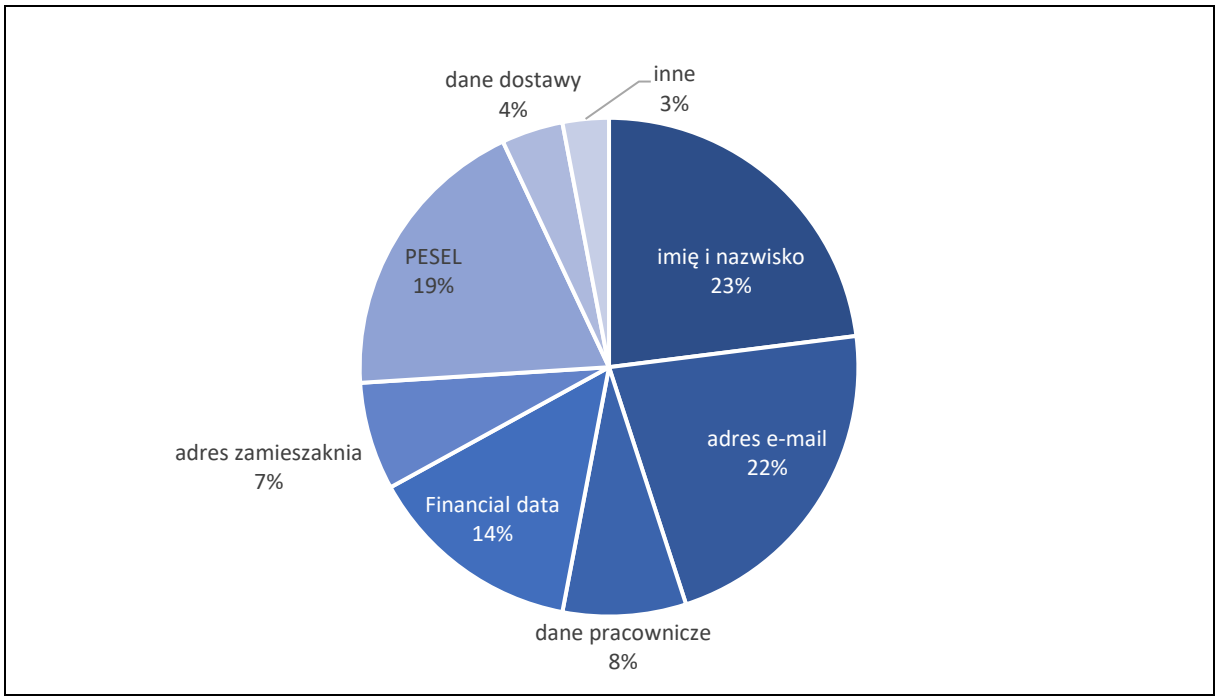
Z raportu wynika, że blisko 70% incydentów nie zostało zgłoszonych do organu nadzorczego. Zgodnie z art. 33 ust. 1 RODO, można nie zgłaszać incydentu do organu nadzorczego, jeżeli "jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych". W 70% przypadków osoby, których dotyczyły te incydenty, nie zostały poinformowane. Niezależnie od zgłaszania incydentu do Regulatora, zgodnie z art. 34 RODO "Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych", to osoby dotknięte naruszeniem powinny zostać poinformowane.




**Wykres 1: Branże najbardziej narażone na ryzyko naruszeń ochrony danych osobowych**
Źródło: ZFODO (2021),ilustracja własna, dane pochodzą z ZFODO.

Źródła naruszeń danych osobowych były zlokalizowane zarówno wewnątrz firmy/instytucji (68%), na zewnątrz (20%), jak również pochodziły od tzw. procesora, czyli podmiotu przetwarzającego dane w imieniu administratora (12%). Do zewnętrznych należą np. byli pracownicy lub hakerzy, do wewnętrznych - pracownicy i współpracownicy organizacji.

W 92% przypadków były to incydenty nieumyślne (źle zaadresowane e-maile, brak ukrytej kopii, wysyłanie tradycyjnej korespondencji o niewłaściwej treści). Incydenty celowe obejmowały: kradzież laptopów lub innych nośników danych, phishing, udostępnianie danych osobom nieuprawnionym. Prawie 96% incydentów spowodowanych było przyczynami osobistymi. Należało do nich działanie czynnika ludzkiego. Przyczyny nieosobiste to sytuacje, w których do naruszenia doszło w wyniku nieprawidłowego działania technologii, sytuacji niezależnych od woli człowieka.




**Wykres 2: Najczęściej naruszane kategorie danych.**
Źródło: ZFODO (ZFODO 2021), ilustracja własna, dane pochodzą z ZFODO.

Jeśli chodzi o ochronę danych osobowych pracowników brak raportu analizującego skalę i najczęstsze sytuacje związane z tym zagadnieniem w Polsce. Aby ułatwić proces rekrutacji i ułatwić poruszanie się wśród przepisów, UODO (Urząd Ochrony Danych Osobowych) wydał publikację "Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców" (Urząd Ochrony Danych Osobowych 2018).

## 2.2 Austria

| Nazwa Instytucji | Krótki Opis | Główne cele | Strona internetowa |
|---|---|---|---|
| WKO – Austriacka Izba Handlowa / WKO Wirtschafts-kammer | WKO wzywa firmy do opracowania odpowiedniej strategii bezpieczeństwa, chroniącej przed potencjalnymi zagrożeniami. | Ważnym czynnikiem bezpieczeństwa jest podnoszenie świadomości pracowników. Utworzono osobny dział zajmujący się bezpieczeństwem IT i bezpieczeństwem danych. MŚP są wspierane przez różne inicjatywy. | https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html |
| Austriacki Urząd Ochrony Danych / Österreichische Datenschutzbehörde (DSB) | Austriacki Urząd Ochrony Danych jest krajowym organem nadzorczym w zakresie ochrony danych w Republice Austrii. | System Informacji Prawnej Republiki Austrii (www.ris.bka.gv.at) udostępnia austriackie ustawodawstwo w jego aktualnej wersji (federalne i krajowe), dzienniki ustaw (federalne i krajowe) oraz orzecznictwo. | www.dsb.gv.at |
| BFI Wien<br><br>Szkolenie Ochrona danych i Bezpieczeństwa Informacji | Dostawca szkoleń z zakresu ochrony danych i bezpieczeństwa informacji | Jako uznana przez państwo instytucja kształcenia ustawicznego, BFI jest uprawniona do wydawania certyfikatów i składania procedur uznawania szkoleń nieformalnych do organu koordynującego (NKS) - lub poprzez swoje punkty usługowe. | https://www.bfi.wien/edv-und-informationstechnologien/datenschutz-und-informationssicherheit/ |
| KMU Platform | Ta sieć ekspertów z dziedziny biznesu i technologii została założona w celu wspierania małych i średnich przedsiębiorstw w Austrii, aby towarzyszyć firmom w cyfrowej zmianie. | Oprócz wielu innych usług oferowane są również warsztaty o szerokim zakresie tematycznym. Hasło "Wspólna płaszczyzna zastępuje wielkość" jasno pokazuje, że w centrum uwagi znajduje się współpraca między małymi przedsiębiorstwami, które w ten sposób tworzą dla siebie przewagę konkurencyjną. | https://www.kmu-plattform.eu/ |
| Agencja cyfryzacji / Digitalisierungs-agentur | W ramach FFG, Agencji Wspierania Badań Naukowych, utworzono "Agencję ds. cyfryzacji", której zadaniem jest przyznawanie dotacji małym i średnim przedsiębiorstwom w Austrii w celu | Aby umożliwić austriackim małym i średnim przedsiębiorstwom (MŚP) jak najlepsze wykorzystanie możliwości digitalizacji, "Inicjatywa KMU DIGITAL" zapewnia konkretne wsparcie: przedsiębiorstwa korzystają z dotacji na doradztwo, podnoszenie kwalifikacji, transfer wiedzy i dalsze kształcenie. | https://www.ffg.at/dia |

| | | | |
|---|---|---|---|
| | ukierunkowanego wspierania cyfryzacji. | | |
| Wiedeńska Agencja Biznesowa / Wirtschafts-agentur Wien | Program finansowania "Wien Digital" wspiera przedsiębiorstwa oraz MŚP w realizacji działań związanych z cyfryzacją. | Wiedeńska Agencja Biznesowa oferuje osobiste doradztwo i dysponuje szeroką siecią małych i średnich przedsiębiorstw oraz (publicznych) partnerów do współpracy. W ważnych kwestiach wspierane są przedsiębiorstwa rozpoczynające działalność, osoby prowadzące jednoosobową działalność gospodarczą, krajowe i międzynarodowe małe i średnie przedsiębiorstwa oraz korporacje. | https://wirtschaftsagentur.at/ |
| Business Circle | Organizator szkolenia na certyfikowanego inspektora ochrony danych | Zdobyte na kursie kwalifikacje potwierdzane są certyfikatem Austriackich Norm zgodnie z kryteriami ISO/IEC 17024 po pozytywnie ocenionym egzaminie końcowym. | https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/ |
| 1a Beratung e.U. - Ing. Roland Fürbas | Prywatny dostawca szkoleń z zakresu GDPR i IS | Bezpieczeństwo danych i IT / DSGVO-DSB / Rozwój biznesu / Usługi online | http://www.1a-beratung.eu |
| 72solutions | Prywatny dostawca szkoleń z zakresu GDPR i IS | GDPR - Eksperci, którzy doradzają i opracowują dostosowane do potrzeb rozwiązania w zakresie ochrony danych. | https://www.72solutions.eu |
| TÜV Austria Akademie | Dostawca szkoleń z zakresu ochrony danych osobowych - ekspert GDPR | W ofercie znajduje się około 20 kursów, które są zorganizowane według sektorów. | https://www.tuv-akademie.at/kursprogramm?s=Datenschutz |

**Tabela 2: Interesariusze z Austrii**

Austria była jednym z pierwszych krajów europejskich, w których istniał organ zajmujący się ochroną danych - Komisja Ochrony Danych. Została ona utworzona wraz z pierwszą ustawą o ochronie danych, Federalny Dziennik Ustaw nr 565/1978. Unijna dyrektywa o ochronie danych 95/46/WE nadała nowe podstawy prawu o ochronie danych w całej Europie (EUR-LEX 1995).W Austrii dyrektywa ta została wdrożona ustawą o ochronie danych z 2000 r. (DSG 2000) (Rechtsinformationssystem des Bundes (RIS) 1999). Po 25 maja 2018 r. podstawowe rozporządzenie o ochronie danych (GDPR; DSGVO) postawiło prawo ochrony danych na nowych podstawach w całej Europie EUR-LEX (1995). W Austrii dyrektywa ta została wdrożona ustawą o ochronie danych z 2000 r. (DSG 2000) Rechtsinformationssystem des Bundes (RIS) (1999). Po 25 maja 2018 r. podstawowe rozporządzenie o ochronie danych (GDPR; DSGVO) (Federalne Ministerstwo Finansów (BMF)) oraz znowelizowana ustawa o ochronie danych (DSG) (Federalne Ministerstwo Finansów (BMF)) stanowią podstawę prawa o ochronie danych (zob. DSB 2019).

Zgodnie z austriackim kodeksem handlowym (UGB) i ustawą o spółkach z ograniczoną odpowiedzialnością (GmbHG) odpowiedzialność za ochronę danych i bezpieczeństwo IT spoczywa zawsze na kierownictwie. Nawet jeśli zadania IT związane z bezpieczeństwem zostaną przekazane pracownikom, kierownictwo firmy ponosi ostateczną odpowiedzialność za przestrzeganie przepisów prawnych. Dzięki dyrektywie NIS (UE) 2016/1148 (EUR-LEX), która została wdrożona w Austrii pod koniec 2018 r. przez ustawę o bezpieczeństwie sieci i systemów informatycznych (NISG), po raz pierwszy istnieją kompleksowe regulacje w zakresie cyberbezpieczeństwa dla strategicznie ważnych przedsiębiorstw, dostawców usług cyfrowych i organów na poziomie europejskim i krajowym. Przedsiębiorstwa muszą podjąć odpowiednie środki techniczne i organizacyjne (np. tworzenie kopii zapasowych danych, szyfrowanie, kontrola dostępu), aby chronić dane przed przypadkowym zniszczeniem, utratą danych lub bezprawnym wykorzystaniem przez osoby trzecie. Niedopełnienie tego obowiązku może skutkować wysokimi karami pieniężnymi.

Ogólne rozporządzenie UE o ochronie danych (GDPR) oraz austriacka ustawa o ochronie danych regulują postępowanie z danymi osobowymi (np. nazwisko, data urodzenia, adres e-mail, adres IP). Oznacza to, że wszyscy przedsiębiorcy w Austrii są związani przepisami prawnymi. Z reguły firmy, które osiągnęły pewien poziom cyfryzacji, dobrze je znają i są regularnie informowane, zwłaszcza przez Izbę Handlową. Więcej problemów mają mikroprzedsiębiorstwa, które ze względu na czas i koszty często kładą mniejszy nacisk na tematy bezpieczeństwa informacji i ochrony danych.

Szczególnie problematyczna wydaje się być kwestia obowiązku informowania zgodnie z GDPR, który według Conrada Lienhardta często nie jest stosowany w Austrii, zwłaszcza w małych firmach: "Zgodnie z ogólnym rozporządzeniem o ochronie danych (GDPR) prawa osób, których dane dotyczą, tj. osób, których dane osobowe są przetwarzane, obejmują obszerne prawo do informacji. Po stronie przedsiębiorstw i organizacji oznacza to rozległe obowiązki informacyjne. Są one uregulowane w art. 13 i 14 GDPR." Lienhardt ostrzega, aby nie lekceważyć obowiązku informacyjnego: "Istnieją firmy i organizacje, które pozyskują dane osobowe z publicznych baz danych, takich jak księgi wieczyste, spisy adresowe itp. a następnie je przetwarzają. Wiele osób sądzi, że nie podlegają one obowiązkowi informacyjnemu, zwłaszcza że "pozyskiwanie" danych z publicznych baz danych bardzo często wiąże się z dużą ilością danych osobowych. Należy się spodziewać skarg i prywatnych pozwów o odszkodowanie. Dlatego: Traktujcie obowiązek informowania poważnie." (Lienhardt 2020).

Dane pracowników zgodnie z ogólnym rozporządzeniem UE o ochronie danych osobowych: W Austrii obowiązują nie tylko przepisy o ochronie danych osobowych, ale także przepisy prawa pracy i prawa socjalnego, jak podkreśla WKO: "Należy tu sprawdzić, na jakiej podstawie dane są przetwarzane (obowiązek prawny, niezbędne do wykonania umowy o świadczenie usług, zgoda?). [...] Ponieważ księgowy ds. płac działa zazwyczaj na podstawie stosunku przetwarzania umowy z klientem (=

podmiotem odpowiedzialnym), a klient ma obowiązek również prawidłowo wypłacać wynagrodzenie na podstawie stosunku pracy, nie jest do tego potrzebna zgoda danego pracownika klienta. Należy jednak zawrzeć pisemną umowę o realizację zlecenia." (Wirtschaftskammer Österreich 2021b).

WKO (Wirtschaftskammer Österreich), Austriacka Izba Gospodarcza, oferuje również wsparcie w zakresie wdrażania GDPR za pomocą informacji branżowych, przewodników, przykładowych dokumentów i list kontrolnych. Przewodnik dotyczący środków technicznych i organizacyjnych w kontekście GDPR zawiera praktyczny przegląd tego, jakie techniczne środki bezpieczeństwa są konieczne i przydatne oraz jak można je wdrożyć w firmie. (c. f. Wirtschaftskammer Österreich (2020)) Wreszcie, "IT Safe" WKO (Wirtschaftskammer Österreich 2021a) jest dobrze znaną i ugruntowaną inicjatywą mającą na celu wspieranie MŚP we wdrażaniu środków bezpieczeństwa IT.

Firmy w Austrii mają do dyspozycji liczne źródła informacji na temat GDPR. Naturalne jest jednak, że tych bardzo obszernych tekstów prawnych nie da się ogarnąć jednym rzutem oka. W związku z tym należy zwrócić uwagę na usługi Austriackiej Federalnej Izby Gospodarczej, która jest ważnym punktem kontaktowym dla wszystkich - a zwłaszcza dla małych - przedsiębiorstw. W ramach projektu "IT Safe" opracowano obszerny przewodnik oraz organizowane są liczne bezpłatne imprezy informacyjne. Szczególnie ważną ofertą jest profesjonalna strona internetowa, która w zrozumiały sposób przedstawia najważniejsze podstawy GDPR (por. Wirtschaftskammer Österreich (2021b)).

Inną atrakcyjną ofertę ma KSV (Kreditschutzverband), który zapewnia firmom opłacalne wsparcie przy wprowadzaniu GDPR na kilku poziomach: doradztwo, szkolenia i aplikacja "Asystent DSVGO" (KSV1870).

Pomimo wszystkich wysiłków, ludzie w Austrii nadal lubią rozmawiać o "niekochanym GDPR"! Znaleźliśmy następującą - z naszego punktu widzenia - odpowiednią informację prasową:

**Otrzeźwiająca rzeczywistość w austriackich przedsiębiorstwach**

W tym komunikacie prasowym APA (Austriacka Agencja Prasowa) z maja 2020 r., Austriacka Agencja Prasowa (2020) informuje o wdrożeniu unijnego GDPR w Austrii pod tytułem: "Zrozumienie tak, wdrażanie powolne". (Austriacka Agencja Prasowa) komunikat prasowy z maja 2020 r., Austriacka Agencja Prasowa (2020) informuje o wdrożeniu EU GDPR w Austrii pod tytułem: "Understanding yes, implementation sluggish" (Zrozumienie tak, wdrożenie powolne).

> " Pomimo znacznie zwiększonej wrażliwości w kwestiach ochrony danych osobowych, od 2018 roku unijne rozporządzenie zostało w pełni wdrożone jedynie przez 30% krajowych przedsiębiorców."

W artykule podkreślono fakt, że dwa lata po wejściu w życie Ogólnego Rozporządzenia o Ochronie Danych Osobowych (EU GDPR) austriackie przedsiębiorstwa wykazują znacznie większe zrozumienie tematu ochrony danych. W ankiecie KSV1870, przeprowadzonej przed kryzysem Corona, w ramach Austrian Business Check w lutym 2020 r. z udziałem około 600 firm, 40% ankietowanych przedsiębiorstw stwierdziło, że w ciągu ostatnich trzech lat wzrosła ona "ogólnie". Badanie wyraźnie pokazało, że wciąż jest wiele do zrobienia, zanim EU GDPR zostanie w pełni wdrożone przez wszystkie firmy w Austrii, po tym jak tylko 30% respondentów w pełni zakotwiczyło je w swojej działalności do tej pory. Najczęściej wdrażanym środkiem mającym na celu zwiększenie ochrony danych było, zdaniem 46% uczestników badania, wprowadzenie lub dostosowanie środków ochrony danych i bezpieczeństwa IT. Pozytywnym akcentem jest fakt, że w ciągu ostatnich trzech lat w austriackich przedsiębiorstwach znacznie wzrosło zrozumienie dla opartego na zaufaniu i świadomego obchodzenia się z informacjami.

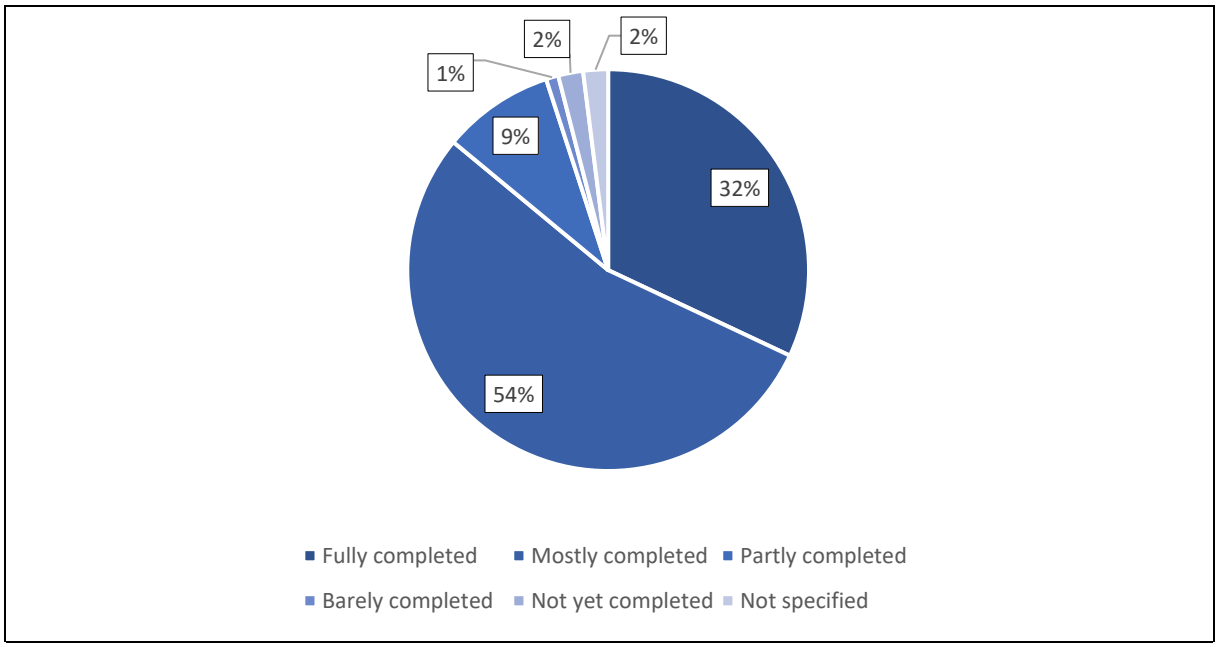
"I tak, 40 % krajowych przedsiębiorstw potwierdza, że rozwój ten nastąpił "w całej rozciągłości" - kolejne 32 % dostrzega wzrost przynajmniej w części obszarów. Podczas gdy dla 19% poprawa nie jest dostrzegalna, dla 2% nawet się zmniejszyła." 7% ankietowanych nie podało żadnych specyfikacji. ( Austriacka Agencja Prasowa , 2020). Często istnieje znaczna luka między zrozumieniem a faktycznym wdrożeniem niezbędnych środków ochrony danych. Zwłaszcza w czasach rosnącej cyfryzacji spowodowanej kryzysem Corona, szczególnie niepokojące jest to, że nawet jedna trzecia krajowych firm nie wdrożyła w pełni unijnego GDPR - wyjaśnia Ricardo-José Vybiral, MBA, CEO KSV1870 Holding AG. Dotyczy to m.in. wymaganego "rejestru operacji przetwarzania", który z powodzeniem wdrożyło do tej pory tylko 34% badanych firm. (Austriacka Agencja Prasowa 2020). Często istnieje znaczny rozdźwięk pomiędzy zrozumieniem a faktycznym wdrożeniem niezbędnych środków ochrony danych. Zwłaszcza w czasach rosnącej cyfryzacji spowodowanej kryzysem Corona, szczególnie niepokojące jest to, że nawet jedna trzecia krajowych firm nie wdrożyła w pełni unijnego GDPR" - wyjaśnia Ricardo-José Vybiral, MBA, CEO KSV1870 Holding AG. Dotyczy to m.in. wymaganego "rejestru operacji przetwarzania", który z powodzeniem wdrożyło do tej pory tylko 34% ankietowanych firm (Austriacka Agencja Prasowa 2020).

Firma Deloitte Services Wirtschaftsprüfungs GmbH (2020) opublikowała również badanie dotyczące stopnia wdrożenia GDPR w austriackich przedsiębiorstwach na początku 2020 r. 191 przedstawicieli firm na stanowiskach kierowniczych zostało przebadanych w ankiecie online: "Wynik: większość firm jest nadal zajęta wdrażaniem wymagań i postrzega ich długoterminową zgodność jako wyzwanie. Jednak znaczenie tego tematu zostało już dostrzeżone: Prawie wszyscy respondenci biorą obecnie pod uwagę wymogi ochrony danych przy podejmowaniu decyzji biznesowych."

Podobnie jak KSV, Deloitte również stwierdza, że poziom pełnego wdrożenia GDPR w austriackich firmach wynosi nieco poniżej jednej trzeciej: "Większość firm (54%), podobnie jak rok temu, jest nadal na etapie wdrażania unijnego GDPR. Podczas gdy prawie jedna trzecia (32 proc.) respondentów w pełni zakończyła już wdrażanie

dyrektywy, około 12 proc. nadal znajduje się w połowie procesu i ma palącą potrzebę nadrobienia zaległości." Deloitte stwierdza w raporcie, że nie powinno być już żadnych wymówek dla niewdrożenia dyrektywy. Pilnie zaleca się, aby zainteresowane firmy aktywnie zajęły się tą kwestią i w razie potrzeby zwróciły się o pomoc zewnętrzną w celu przyspieszenia wdrożenia.

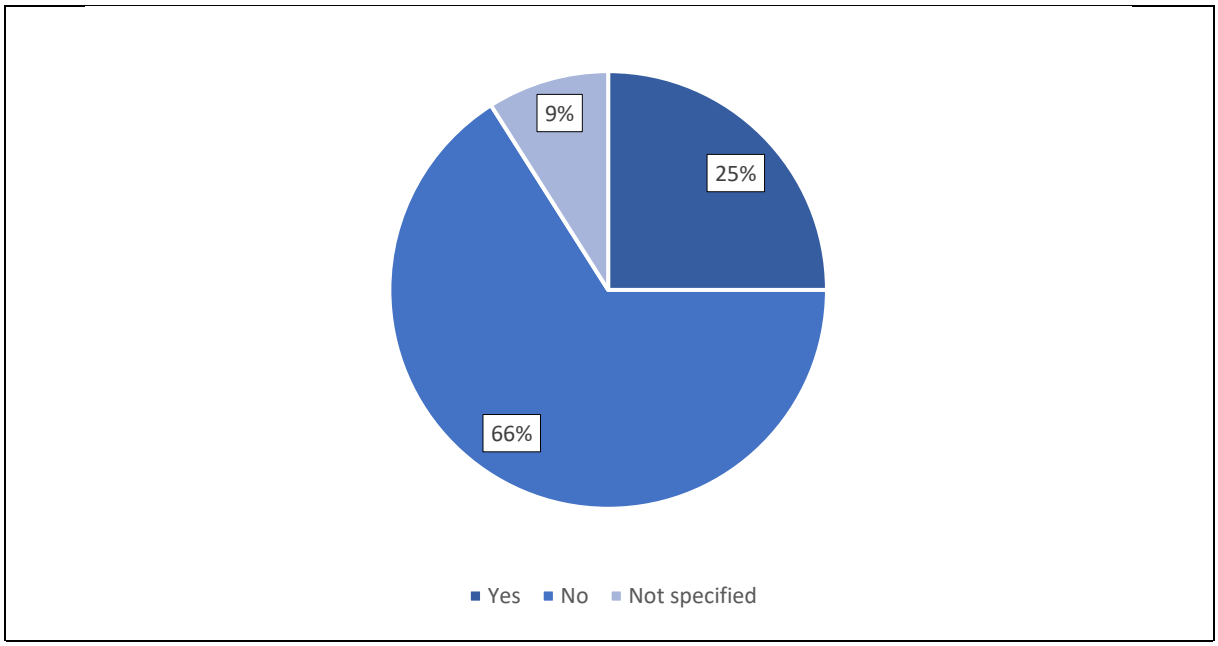
Zapytane o stan wdrożenia GDPR, firmy odpowiedziały w następujący sposób:




**Wykres 3: Wdrożenie GDPR w Austrii**

*Źródłó: Ilustracja własna. Dane pochodzą z Deloitte Services Wirtschaftsprüfungs GmbH (2020)*

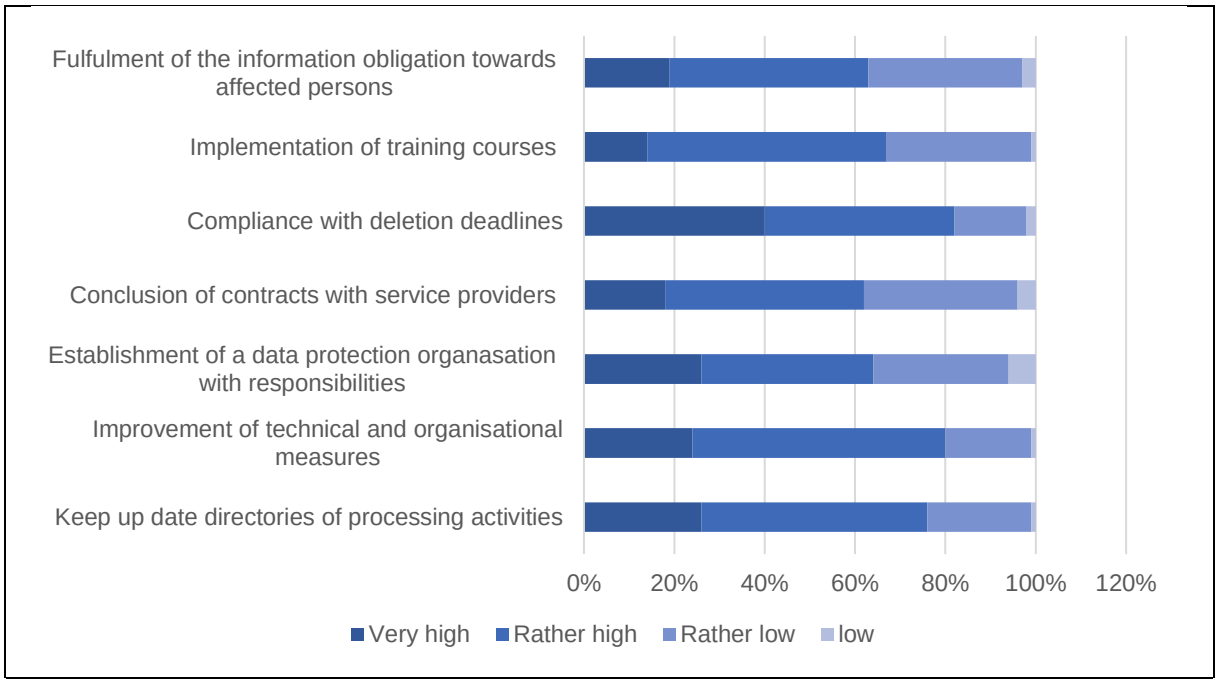
W 2020 roku, jak donosiły media, nastąpił wzrost kar za nieprzestrzeganie przepisów o ochronie danych osobowych. Deloitte zapytał więc firmy, jak te zawiadomienia wpłynęły na zachowania w firmie: "Tylko w jednej czwartej firm decyzje organu ochrony danych osobowych miały do tej pory wpływ na postępowanie z EU GDPR. Spośród nich większość wykorzystała ustalenia do oceny lub poprawy stanu we własnym przedsiębiorstwie." Pytanie zostało sformułowane w następujący sposób: Czy ostatnie decyzje austriackiego organu ochrony danych wpłynęły na twoje podejście do EU GDPR?




**Wykres 4: Wpływ austriackiego organu ochrony danych na podejście do unijnego GDPR**

*Źródło: Ilustracja własna. Dane pochodzą z Deloitte Services Wirtschaftsprüfungs GmbH (2020)*

Badanie Deloitte podkreśla, że w ostatnich latach wiele firm w Austrii niestety nie odrobiło pracy domowej. Często brakuje ustrukturyzowanej klasyfikacji danych, co znacznie zmniejszyłoby wysiłek. Interesująca jest następująca ocena kolejnego pytania: Jak duży wysiłek szacuje Pan/Pani, że w przyszłości trzeba będzie podjąć, aby spełnić wymogi unijnego GDPR?




**Wykres 5: Wysiłki potencjalnie poniesione w celu zapewnienia zgodności z wymogami unijnego GDPR**

*Źródło: Ilustracja własna. Dane pochodzą z Deloitte Services Wirtschaftsprüfungs GmbH (2020)*

Z raportu wynika, że dla większości firm długoterminowa zgodność z GDPR jest odczuwana jako wyzwanie. Respondenci dostrzegają największy wysiłek w rozważaniu terminów usuwania danych.

Innym interesującym pytaniem Deloitte jest to, czy istnieje wystarczająca liczba przeszkolonych pracowników do zadań związanych z ochroną danych: "Ponad jedna czwarta ankietowanych firm nie dysponuje zasobami ludzkimi, które pozwoliłyby na dostosowanie się do EU GDPR i wdrożenie związanych z tym prac. Tym ważniejsze jest inne wsparcie: dlatego też coraz więcej austriackich firm zwraca się o wsparcie technologiczne, aby móc spełnić wymogi EU GDPR. Podczas gdy w zeszłym roku 39% nie posiadało żadnego narzędzia, obecnie jest to około 30%."

Raport Deloitte konkluduje: "Po początkowej niepewności, austriackie firmy mają znacznie jaśniejszy obraz istniejącej potrzeby działania. Niektóre ze zidentyfikowanych kluczowych tematów wiążą się jednak z kompleksowymi zmianami. Ma to również wpływ na kulturę korporacyjną." Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Z punktu widzenia firmy Hafelekar możemy podsumować sytuację w Austrii w następujący sposób: Można powiedzieć, że w Austrii istnieją jasne przepisy dotyczące tematu wdrażania GDPR, choć nie zawsze są one sformułowane w sposób łatwy do zrozumienia. Istnieje kilka organów publicznych, przede wszystkim WKO, do których firmy mogą zwrócić się o wsparcie we wdrażaniu GDPR. W Austrii odpowiedzialność za wszelkie uchybienia w zakresie ochrony danych i bezpieczeństwa IT spoczywa na kierownictwie, nawet jeśli deleguje ono zadania na pracowników. Wdrożenie nadal nie przebiega w sposób zadowalający i jak już ustaliliśmy z naszą grupą ekspertów w Austrii, brak czasu w MŚP jest prawdopodobnie decydujący dla tego powolnego wdrażania. W każdym razie, według naszej Grupy Sterującej TeBeISi, w Austrii istnieje duże zainteresowanie przystępnymi cenowo szkoleniami w zakresie ochrony danych i bezpieczeństwa IT. Jest jeszcze wiele do zrobienia.

## 2.3 Niemcy

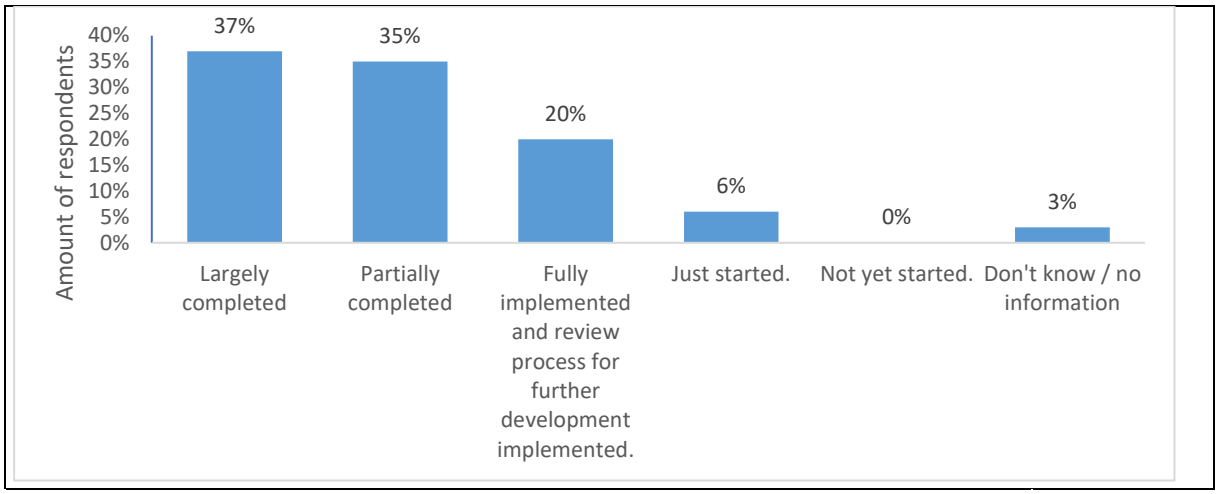
| Nazwa Instytucji | Krótki Opis | Główne cele | Strona internetowa |
|---|---|---|---|
| Deutsche Vereinigung für Datenschutz e.V. (DVD) | DVD jest odpowiedzialne za publikowanie komunikatów dotyczących ochrony danych (DANA). Do zadań należy również public relations i praca z mediami na aktualne tematy, konferencje prasowe i komunikaty prasowe. Poza tym organizowane są spotkania we współpracy z organizacjami partnerskimi i seminariami. DVD bierze również udział w corocznym konkursie Big Brother Awards. | DVD ma na celu doradzanie i informowanie społeczeństwa o zagrożeniach związanych z korzystaniem z elektronicznego przetwarzania danych i możliwym ograniczeniem prawa do informacyjnego samostanowienia. | https://www.datenschutzverein.de |
| Gesellschaft für Datenschutz und Datensicherheit (GDD) | Założone w 1977 roku GDD liczy dziś ponad 3.800 członków. Na terenie całego kraju działają 34 koła wymiany doświadczeń, w których uczestniczy ponad 3.500 osób, a w akademii GDD przeszkolono już ponad 10.000 inspektorów ochrony danych. | Ochrona danych, bezpieczeństwo danych i właściwe przetwarzanie danych mają na celu ochronę wszystkich zainteresowanych stron przed niebezpieczeństwem, przy jednoczesnym zapewnieniu wolności informacji i równowagi informacyjnej. Zobowiązania prawne dotyczą wszystkich przedsiębiorstw i jednostek administracyjnych, niezależnie od wielkości i branży. GDD chce wnieść do nich znaczący wkład. | https://www.gdd.de/ |
| Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfG) | W FIfG pracuje około 700 osób z obszaru nauki i praktyki, przede wszystkim profesjonaliści w dziedzinie informatyki i technologii informacyjnych. Celem jest umożliwienie wymiany pomiędzy wszystkimi osobami związanymi z informatyką i technologią informacyjną. FiFG jest | FiFG ostrzega opinię publiczną przed szkodliwym rozwojem w dziedzinie bezpieczeństwa informacji. Ponadto, stowarzyszenie walczy z wykorzystaniem technologii informatycznych do kontroli i inwigilacji.<br>FiFG wspiera również równouprawnienie osób niepełnosprawnych w projektowaniu i stosowaniu technologii informatycznych oraz działa na rzecz zwalczania dyskryminacji kobiet w dziedzinie informatyki. | https://www.fiff.de/ |

| | | | |
|---|---|---|---|
| | otwarte dla wszystkich, którzy chcieliby wziąć udział lub tylko zasięgnąć informacji. | | |
| Digitalcourage e.V. | Stowarzyszenie zostało założone w 1987 roku. Digitalcourage e.V. wspiera m.in. prawa fundacyjne i ochronę danych, prowadzi działalność edukacyjną poprzez public relations, np. poprzez kampanie i projekty, a także odpowiada za przyznawanie co roku nagrody BigBrotherAward. | Znaczna część pracy polega na organizowaniu projektów i kampanii, a także organizowaniu kongresów politycznych. Ponadto stowarzyszenie jest dostępne dla prasy i mediów jako prelegenci i eksperci w sprawach ochrony danych. Głównym celem jest zaangażowanie się w prawa podstawowe, ochronę danych i świat wart życia w epoce cyfrowej. | https://digitalcourage.de/ |
| Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDi) | Do głównych zadań instytucji założonej w 1978 roku należy monitorowanie i egzekwowanie GDPR, BDSG i innych przepisów dotyczących ochrony danych. Ponadto, chodzi o podnoszenie świadomości i public relations. | Głównym celem jest zabezpieczenie i rozwój ochrony danych. Od 2006 r. każdy, kto uważa, że jego prawo do dostępu do informacji zgodnie z ustawą o wolności informacji (IFG) zostało naruszone, może zwrócić się do pełnomocnika federalnego. Obecnie urząd ten sprawuje prof. Ulrich Kelber. | https://www.bfdi.bund.de/ |

**Tabela 3: interesariusze w Niemczech.**

Europejskie Ogólne Rozporządzenie o Ochronie Danych Osobowych (GDPR) weszło w życie 24 maja 2016 roku. Od 25 maja 2018 r. zawarte w nim wymogi dotyczące ochrony danych są obowiązkowe w poszczególnych krajach członkowskich również bez odrębnej transpozycji do prawa krajowego. Europejskie rozporządzenie o ochronie danych ma na celu przede wszystkim wzmocnienie praw konsumentów. Podmioty przetwarzające dane muszą liczyć się z zaostrzeniem przepisów. Nieprzestrzeganie GDPR może kosztować dane przedsiębiorstwo do 20 milionów euro grzywny lub do 4% jego globalnego obrotu (w zależności od tego, która wartość jest wyższa) (datenschutz 2021). Stan wdrożenia GDPR przez firmy w Niemczech przedstawia wykres 3. Statystyka ta została opublikowana jesienią ubiegłego roku. Jest to najbardziej aktualne dostępne badanie dotyczące wdrażania GDPR. W momencie przeprowadzania badania 37% respondentów wskazało, że wdrożyło już wytyczne GDPR. Ponad połowa uczestników stwierdziła, że wytyczne są częściowo wdrożone lub całkowicie wdrożone i ustalone do dalszego rozwoju (Statista 2020). [1]

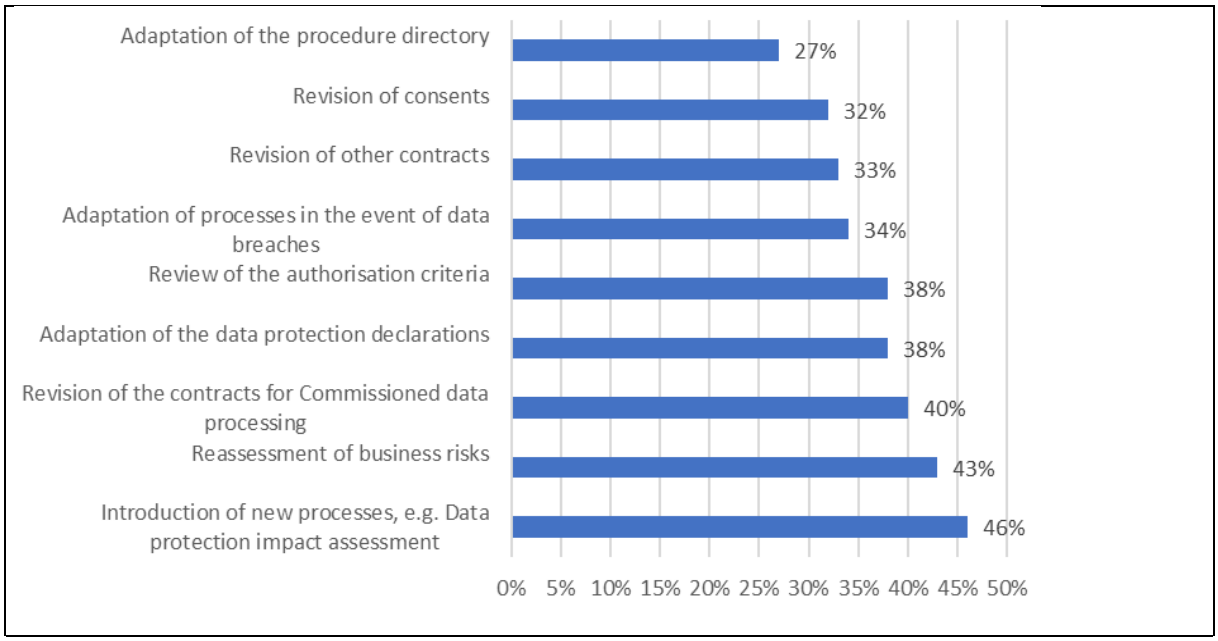
[1] Więcej informacji dotyczących badania: Data publikacji 09/2020, Niemcy, okres badania 09/2020, liczba respondentów: 504 firmy zatrudniające 20 lub więcej pracowników, ankieta telefoniczna.




**Wykres 6: Stan wdrożenia GDPR przez firmy w Niemczech (09/2020)**

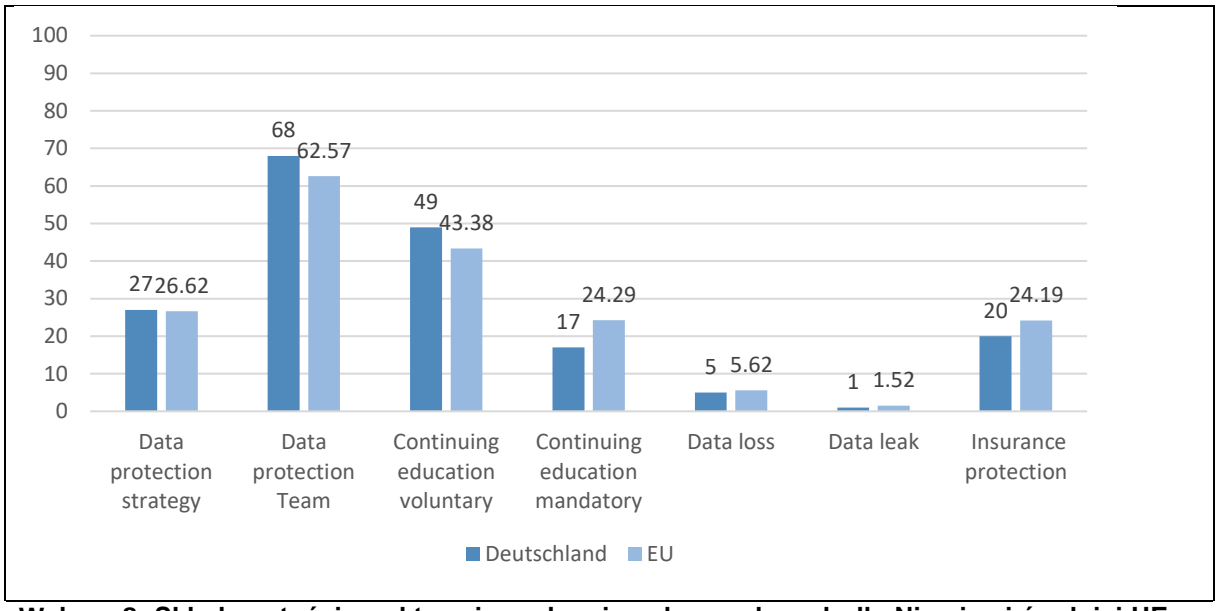
Biorąc pod uwagę upływ około 5 lat od publikacji i 3 lat od wejścia w życie, można wywnioskować, że poważne przeszkody uniemożliwiają firmom pełne wdrożenie GDPR. Konkretne konsekwencje zostały szczegółowo opisane w badaniu przeprowadzonym przez Bitkom e.V. (2020). Jednym z powodów, dla których firmy zmagają się z wdrożeniem, może być duża ilość niezbędnego wysiłku, począwszy od początkowych (i pojedynczych) dodatkowych wydatków (63%), oczekiwanie stałych dodatkowych wydatków (w porównaniu z poprzednim stanem prawnym, 29%) oraz potrzeba dodatkowego personelu (26%). Potrzeby kadrowe znajdują również odzwierciedlenie w decyzji firm o wykupieniu usługi ochrony danych od usługodawców, czy to w formie zewnętrznego doradztwa prawnego (40%), zewnętrznego doradztwa w zakresie ochrony danych (31%), czy też zewnętrznych przeglądów (28%). Niemniej jednak większość firm uważa, że GDPR ma pozytywny wpływ na funkcjonowanie i wyniki firmy biorąc pod uwagę wpływ na jednolite środowisko konkurencyjne w całej UE (57%).

W obliczu złożonych zmian regulacyjnych, kilka aspektów budzi jednak wątpliwości co do ich pozytywnego wpływu na działalność gospodarczą. Przeważają między innymi obawy dotyczące długoterminowej poprawy otoczenia prawnego (43%), hamowania innowacji (35%) i komplikowania procesów biznesowych (25%). Ryzyko związane z wdrożeniem GDPR znajduje również odzwierciedlenie w środkach, które są najpilniejsze, co widać na wykresie 4.




**Wykres 7: Które środki służące wdrożeniu GDPR będą przez Państwa wprowadzane w trybie pilnym?** Źródło: Bitkom e.V. (2020)

Badanie przeprowadzone w 2021 roku podkreśla ogólnie wysoki priorytet ochrony danych w Niemczech, plasując ten kraj na drugim miejscu wśród wszystkich państw europejskich pod względem ogólnego i właściwego traktowania ochrony danych (heyData 2021). Ze wszystkich rozpatrywanych kategorii warto zauważyć, że "przedsiębiorstwa" zajmują najniższą pozycję w porównaniu z "egzekwowaniem prawa", "kompetencjami w zakresie ochrony danych" i "odczuciami społecznymi", a "osoby prywatne" zajmują stosunkowo najwyższą pozycję. Każdą kategorię można rozłożyć na kilka kryteriów, które rzucają światło na konkretne mocne i słabe strony. Patrząc na sytuację firm, jak można zobaczyć na wykresie 5, staje się oczywiste, że tylko 17% firm ma wdrożone obowiązkowe dalsze szkolenia w porównaniu ze średnią UE wynoszącą 24,29%. Drugim istotnym niedociągnięciem w porównaniu z pozostałymi krajami UE jest ochrona ubezpieczeniowa, w przypadku której Niemcy osiągają wynik o 4 punkty procentowe niższy niż średnia UE.




**Wykres 8: Skład wartości punktowej w zakresie ochrony danych dla Niemiec i średniej UE w %.**

Źródło: heyData (2021). Ilustracja własna.

W związku z naruszeniami prywatności danych, w Niemczech nakładane są surowe kary. Około 69 milionów euro grzywien w 2020 roku oznacza, że naruszenia danych są surowo karane. Stwierdzenie to idzie w parze z faktem, że w Niemczech odnotowano największą łączną liczbę naruszeń ochrony danych. Szczególnie w czasach pandemii i home-office odnotowano wzrost liczby naruszeń o około 76% w porównaniu z rokiem poprzednim. Konsekwencje tego odkrycia są wyjaśnione w następujący sposób: "W porównaniu z resztą Europy, firmy w Niemczech w większości zachowują się w sposób bardzo wzorcowy. Jest to jednak również konieczne. Prawo w Niemczech jest ściśle przestrzegane" (Milos Djurdjevic, CEO heyData, (maj 2021)).

Biorąc pod uwagę te dane, nic dziwnego, że powstało kilka stowarzyszeń, które zajmują się właśnie właściwym wdrażaniem ochrony danych w sferze publicznej i korporacyjnej. Prawo do informacyjnego samostanowienia" (BVerfG 15.12.1983) i ochrona praw osobistych przed rosnącym naciskiem na interesy bezpieczeństwa jest elementarną częścią pracy tych stowarzyszeń. Zagrożenie dla ochrony danych i bezpieczeństwa informacji nie jest zatem postrzegane wyłącznie jako utrzymujące się wśród przestępców i wrogich podmiotów, ale także ze strony rządu federalnego i jego interesów bezpieczeństwa.

## 2.4 Włochy

| Nazwa Instytucji | Krótki Opis | Główne cele | Strona internetowa |
|---|---|---|---|
| Apindustria Vicenza - Stowarzyszenie MŚP w Vicenzie | Około 1,000 członków (większość z nich to mikro/małe firmy, zatrudniające mniej niż 20 pracowników). Oferują usługi takie jak: kontakty z władzami lokalnymi i regionalnymi (Departament Regionalny, Izby, polityki regionalne); usługi fiskalne i prawne dla członków; kursy szkoleniowe; specyficzne usługi (np. w zakresie eksportu, sieci, suistanibility, kwestie prawne, projekty UE, certyfikaty, itp.) Osoba kontaktowa: Pan Manuel Maraschin (Dyrektor; mail: m.maraschin@apindustria.vi.it) | Niektóre firmy (stowarzyszone z Apindustria Vicenza) posiadają już wewnętrznego kierownika ds. informatyki i zarządzania zasobami ludzkimi. W takim przypadku moglibyśmy zweryfikować i pilotować (częściowy) proces certyfikacji z udziałem tych menedżerów, sprawdzając ścieżki szkoleniowe poprzez zawartość IO3 (kwestionariusz on-line). I odwrotnie, w przypadku ekspertów zewnętrznych (konsultantów, dostawców IT, prawników, itp.), którzy wspierają MŚP, moglibyśmy sprawdzić, czy certyfikacja pasuje do ich codziennej pracy. Apindustria Vicenza jest w stanie zorganizować kilka spotkań z lokalnymi MŚP i w tym samym czasie zaproponować kierownikom IT i DP przeprowadzenie wywiadów, które mogą być przydatne dla OI projektu.<br>Apindustria nie jest organem publicznym, ale swego rodzaju organizacją "pośrednią", która reprezentuje również lokalne / regionalne interesy zbiorowe. Apindustria Vicenza, jako stowarzyszenie branżowe, bierze udział w niektórych regionalnych spotkaniach roboczych i technicznych. Spotkania te koncentrują się również na profilu zawodowym, określeniu konkretnych kompetencji, procesach (częściowej) certyfikacji itp. Tak więc Apindustria może wspierać wdrażanie nowego profilu, również dlatego, że reprezentuje kilka lokalnych MŚP. Dzięki niektórym kursom EFS - Europejskiego Funduszu Społecznego, Apindustria mogłaby wdrożyć, pod koniec projektu, również konkretne ścieżki szkoleniowe, które mogłyby być (częściowo) certyfikowane przez nasze regionalne biuro szkoleniowe.<br>Harmonogram: nowy plan UE na lata 2021-2027 jest nadal przedmiotem dyskusji. W tej chwili odbywa się kilka spotkań technicznych na poziomie regionalnym (główny cel strategii szkoleniowej, nowe treści, harmonizacja profili zawodowych na poziomie krajowym i europejskim, priorytety ESCO, itp.) ). Apindustria może również informować władze regionalne o zawartości projektu. Dzięki temu, niektóre wyniki projektu mogły zostać wdrożone do nowych programów. | WWW. apindustria.vi.it |
| CPV – CentroProduttivitàVeneto | Jest to jeden z największych dostawców szkoleń w regionie Veneto, z prawie 70-letnim doświadczeniem. CPV oferuje szeroki zakres kursów szkoleniowych, dla MŚP, pracowników, menedżerów, konsultantów i osób bezrobotnych. W ciągu ostatnich 2-3 lat zorganizowało również kilka kursów szkoleniowych w tematach związanych z projektem. Osoba kontaktowa: Pan Enrico Bressan, (dyrektor działu szkoleń i projektów UE; mail: bressan@cpv.org). Jest on również zewnętrznym ekspertem dla agencji | Pan Bressan posiada szerokie doświadczenie (dzięki kilku regionalnym, krajowym i ponadnarodowym projektom) w zakresie platformy ESCO, ram Ecvet, systemów EQF, itp. Mógłby on wspierać projekt, wymieniając się swoim doświadczeniem. Ponadto, CPV jest w stanie zaangażować kilka lokalnych małych przedsiębiorstw. Jako dostawca szkoleń, CPV zbudował silną sieć regionalną w dziedzinie VET i edukacji dorosłych. Posiada również wielu ekspertów (np. konsultantów i trenerów), którzy mogliby sprawdzić i zatwierdzić listę kompetencji. CPV jest w stanie zaangażować lokalny mały biznes, organizując na przykład rozmowy z potencjalnymi kandydatami i spotkania (warsztaty) z firmami. CPV prowadzi również "grupę studyjną" (od 1985 roku) skoncentrowaną na IT, informatyce, ochronie danych, digitalizacji, itp. Wyniki pośrednie i końcowe projektu mogłyby być im przedstawione. Jako instytucja "publiczno-prywatna", CPV zasiada w kilku technicznych grupach na poziomie regionalnym (np. w komitecie grupy ekspertów ds. uznawania i oceny kompetencji i profili zawodowych). Mógłby on dokonać przeglądu naszego regionalnego planu adaptacji, a następnie podjąć pewne działania lobbingowe z władzami regionalnymi. | www.cpv.org |

| | | | |
|---|---|---|---|
| | Long Life Learning w Rzymie. | | |
| Cesar srl | Jest to centrum szkoleniowe w Vicenzy dla lokalnego stowarzyszenia rzemiosła (zrzeszającego ponad 20 000 mikro i małych przedsiębiorstw). Oferuje szeroki zakres usług szkoleniowych, w tym kursy z zakresu bezpieczeństwa IT, ochrony danych, GDPR, itp. Osoba do kontaktu: Pani Daniela Bucci, (wicedyrektor działu szkoleń; mail: d.bucci@confartigianatovicenza.it). | Cesar pracuje tylko z mikro i małymi firmami (poniżej 10 pracowników). Zazwyczaj firmy te nie posiadają wewnętrznego eksperta, takiego jak kierownik ds. bezpieczeństwa IT i ochrony danych lub osoba odpowiedzialna za te kwestie. Dzięki kursom szkoleniowym (finansowanym lub nie) Cesar jest w stanie wspierać proces certyfikacji (częściowej). Cesar może być zaangażowany w kilku fazach, takich jak: zaangażowanie małych firm, analiza potrzeb, definicja kluczowych kompetencji, pilotaż i szkolenia. W przyszłości, Cesar mógłby również oferować lokalnym firmom kursy certyfikowane przez TEBEISI, wraz ze wszystkimi rezultatami projektu. Cesar jest częścią regionalnej sieci ośrodków szkoleniowych, dla mikro i małych przedsiębiorstw, składającej się z 7 prowincji (łącznie 75 000 członków). Cesar jest bardzo często zaangażowany w kilka regionalnych grup technicznych i roboczych zajmujących się profilami zawodowymi i procesem certyfikacji. Może być świadomy naszego regionalnego autorytetu w zakresie celów i rezultatów projektu, przede wszystkim dla mikroprzedsiębiorstw. | www.confartigianatovicenza.it |
| Vicenza Izba Handlowa | Jest to instytucja publiczna we Włoszech, która oferuje obowiązkowe usługi dla wszystkich firm. Na przykład, każda lokalna firma musi być zarejestrowana w lokalnej bazie danych (dla wszystkich etapów działalności, od rozpoczęcia do zakończenia działalności). Izba Vicenzy reprezentuje ponad 90.000 firm, z których większość to mikro lub małe przedsiębiorstwa. Osoba do kontaktu: Pan Diego Rebesco (szef departamentu statystyki i promocji; mail: diego.rebesco@vi.camcom.it). | Izba oferuje szeroki zakres usług, które obejmują mniej więcej wszystkie potrzeby firmy (obowiązki administracyjne, szkolenia, eksport, certyfikaty, patenty, itp.) Izba jest również aktywna w dziedzinie uznawania profili zawodowych, na przykład za pośrednictwem Ministerstwa Edukacji i Pracy w Rzymie. Prowadzi również staże dla młodych ludzi (ze szkół średnich), którzy uczestniczą w krótkich doświadczeniach w firmie, poprzez certyfikowane praktyki, które na koniec są oceniane. Mogłaby być zaangażowana nie tylko w promocję i rozpowszechnianie projektu (np. biuletyn lub lokalne warsztaty), ale także w proces certyfikacji, dzięki powiązaniu z naszym krajowym Ministerstwem. Mogłaby być przynajmniej informowana o postępach w realizacji projektu. Mogłaby również utworzyć lokalną (prowincja Vicenza) grupę roboczą. Grupa ta mogłaby, na zakończenie projektu, przedstawić proces certyfikacji końcowej (częściowej) TEBEISI naszym władzom regionalnym, w celu uzyskania pełnego uznania. Mógłby to być nasz organ publiczny, który weryfikowałby i certyfikował cały regionalny plan adaptacji, jako część jego funkcjonalności i celu. Bardziej szczegółowo, może sprawdzić harmonogram, role poszczególnych uczestników i, przede wszystkim, zatwierdzić główną treść planu, także pod kątem przyszłego specyficznego prawodawstwa w temacie projektu lub specyficznych potrzeb, które można uwzględnić w regionalnych programach szkoleniowych. | www.vi.camcom.it |
| Proservizi srl | Jest to regionalne centrum szkoleniowe ConfProfessioni Veneto (zrzeszające ponad 45.000 członków, takich jak prawnicy, eksperci podatkowi, notariusze, konsultanci, itp.) Oferuje szeroki zakres usług szkoleniowych, w tym kursy z zakresu bezpieczeństwa IT, ochrony danych, GDPR, itp. Osoba kontaktowa: Pani Greta Cosentino, (dyrektor działu szkoleń; mail: greta.cosentino@proservizi.it). | Proservii ma jako klientów tylko konsultantów (nie firmy). Dzięki temu jest w stanie zaangażować dużą liczbę prawników specjalizujących się w bezpieczeństwie IT i ochronie danych osobowych. Ponadto, bardzo często oferują szkolenia (podstawowe i zaawansowane) z zakresu GPPR i kodeksu prywatności. Tak więc, są w stanie sprawdzić i porównać ścieżki projektu (na przykład w zakresie listy konkretnych kompetencji) z tym, czego potrzebuje rynek (firmy). Proservizi był już zaangażowany w działania projektowe. Na przykład, niektórzy członkowie (np. prawnicy) przeprowadzali wywiady projektowe. Oferują również finansowane kursy szkoleniowe (dzięki ESF - Europejski Fundusz Społeczny, i/lub specjalne dotacje z ich systemu szkoleniowego, zwanego "Fondo ConfProfessioni"). Tak więc, są w stanie sfinansować kurs profilowy TEBEISI w najbliższej przyszłości. Proservizi mogłoby wesprzeć przede wszystkim fazy pilotażowe, angażując np. kilku lokalnych prawników i kilka małych firm (ich klientów) tylko po to, aby sprawdzić zawartość projektu. Ale również w celu zdobycia | www.proservizi.it |

| | | | |
|---|---|---|---|
| | | nowych kompetencji w dziedzinie bezpieczeństwa IT i ochrony danych. Mogliby również zorganizować specjalną ścieżkę szkoleniową dla członków, która obejmowałaby wszystkie wyniki i rezultaty projektu TEBEISI. Proservi jest bardzo często zaangażowane w prace kilku regionalnych grup roboczych, w zakresie potrzeb szkoleniowych i uznawania kompetencji. Może więc zasugerować naszym regionalnym władzom szkoleniowym na przykład nowe materiały do następnego programu EFS (który będzie obejmował lata 2021-2027). | |
| SATEF srl | Jest to regionalne centrum szkoleniowe. Oferuje szeroki zakres usług szkoleniowych, w tym kursy z zakresu bezpieczeństwa IT, ochrony danych, GDPR, itp. Specjalizuje się również w sektorze zdrowia i bezpieczeństwa, w tym w ośrodkach opieki nad osobami starszymi. Osoba kontaktowa: Pan Paolo Pedron, (założyciel i dyrektor działu szkoleń; mail: pedron@satef.com). | Pan Pedron, dyrektor, jest ekspertem ESCCO / Ecvet, na poziomie regionalnym i krajowym. Stworzył on specjalną platformę szkoleniową do uznawania kompetencji i (częściowej) certyfikacji. Obecnie prowadzi ją w dwóch sektorach: zdrowia i bezpieczeństwa oraz turystyki. Moglibyśmy więc przetestować i pilotować zawartość naszego projektu w jego platformie. Ten test mógłby również obejmować małe firmy i niektórych konsultantów/ekspertów. Satef mógłby przetestować zawartość projektu, na przykład w dziedzinie turystyki. W rzeczywistości, dzięki wcześniejszym doświadczeniom, platforma już istnieje, również w zakresie ścieżek szkoleniowych. Można więc przetestować treści szkoleniowe TEBEISI, ale także przeprowadzić (częściowy) proces certyfikacji, także na poziomie regionalnym. Pan Pedron bierze udział w niektórych regionalnych grupach roboczych, zajmujących się "certyfikacją i oceną profili zawodowych". Jest on więc w stanie mocno wspierać naszą fazę wdrażania. Ze względu na rolę Pedrona na poziomie regionalnym, jest on w stanie promować wśród naszych władz publicznych zawartość projektu i jego rezultaty (włączając w to fazy testowe). Mógł również, nieformalnie, zatwierdzić nasz "regionalny plan adaptacji", tuż przed wysłaniem go (do ostatecznej dyskusji) do naszego regionalnego wydziału szkoleń i pracy w Wenecji. | www.satef.com |
| ENGIM Veneto | Jest to największy dostawca usług szkoleniowych w regionie Veneto, z prawie 90-letnim doświadczeniem. ENGIM oferuje szeroki zakres szkoleń dla MŚP, pracowników, menedżerów, konsultantów i osób bezrobotnych. W ciągu ostatnich 2-3 lat ENGIM zorganizował również kilka kursów szkoleniowych z zakresu tematyki projektu. Osoba kontaktowa: Pan Manuel Fochesato, (dyrektor działu szkoleń i projektów UE; mail: manuel.fochesato@engimvi.it). | Pan Fochesato posiada szerokie doświadczenie (dzięki kilku regionalnym, krajowym i ponadnarodowym projektom) w zakresie platformy ESCO, ram Ecvet, systemów EQF, itp. Mógłby on wspierać projekt, wymieniając się swoim doświadczeniem. Ponadto, ENGIM jest w stanie zaangażować kilka lokalnych małych firm, ale także konsultantów, trenerów i ekspertów. Engim działa również jako VETs; więc część kursów szkoleniowych skupia się na młodzieży, dorosłych, którzy potrzebują dodatkowego szkolenia, a przede wszystkim na osobach bezrobotnych. Engim prowadzi już (i planuje) kilka platform szkoleniowych, które obejmują nie tylko materiały szkoleniowe (tj. kursy on-line dla szerokiego zakresu potrzeb edukacyjnych), ale także systemy informatyczne, które rozpoznają, częściowo, określone kompetencje. Engim może zdecydowanie wspierać wdrażanie profili zawodowych na kilka sposobów: znaleźć użytkowników końcowych (małe firmy i/lub konsultantów/ekspertów); zaangażować stażystów (młodych i/lub dorosłych), którzy szukają nowej specjalizacji zawodowej i wreszcie, co nie mniej ważne, dyskutować i wymieniać się z lokalnymi (regionalnymi) władzami szkoleniowymi. Dzięki roli i doświadczeniu Fochesato, na poziomie regionalnym, jest on w stanie promować wśród naszych władz publicznych zawartość projektu i wyniki (w tym fazy testowania). Engim może również podzielić się regionalnym planem adaptacji z kilkoma interesariuszami publicznymi. Mógłby również wprowadzić nowe treści do swoich internetowych platform szkoleniowych, w tym treści TEBEISI. | www.engimvi.it |
| Veneto lavoro | Jest to publiczna agencja regionalna, która prowadzi wszystkie treści dotyczące rynku pracy (kursy, certyfikaty, lokalne centra | Region Veneto, poprzez Veneto Lavoro, prowadzi "Departament Pracy i Szkoleń"; jest to więc organ publiczny, który zarządza wszystkimi funduszami (tj. EFS - Europejski Fundusz Społeczny) dla pracowników, firm, menedżerów i konsultantów/szkoleniowców. Veneto Lavoro prowadzi | www.venetolavoro.it |

| | | | |
|---|---|---|---|
| | pracy dla bezrobotnych, itp.) Osoba kontaktowa: Pan Mirco Casteller, (odpowiedzialny za dział opieki społecznej i projekty UE; mail: mirco.casteller@venetolavoro.it). | również "RRSP - Repertorio Regionale Standard Professionali" (regionalną bazę danych / repertorium standardów i kwalifikacji zawodowych). Jako instytucja publiczna, Veneto Lavoro jest najważniejszym interesariuszem na poziomie regionalnym, przede wszystkim dlatego, że prowadzi RRSP. A pan Casteller jest naszym głównym kontaktem w tej strategicznej wymianie i dyskusji. Veneto Lavoro odgrywa kluczową rolę we wdrażaniu profilu TEBEISI, przede wszystkim w ostatnich fazach projektu (gdzie włoski partner powinien rozpowszechniać pewne wytyczne i zalecenia). Jako niezależne i publiczne biuro, Veneto Lavoro nie może być bezpośrednio zaangażowane w ten proces, ale może działać jako "doradca publiczny". Veneto Lavoro może zatwierdzić nasz "regionalny plan adaptacji" krok po kroku. Oznacza to, że moglibyśmy od początku informować Veneto Lavoro o postępach projektu, a na koniec zaproponować nowy profil zawodowy, który mógłby być (częściowo) certyfikowany i umieszczony w regionalnej bazie danych standardów zawodowych (RRSP). | |
| INAPP - Ministerstwo Pracy | Jest to nowa agencja na poziomie krajowym, która prowadzi i sprawdza wszystkie krajowe (i europejskie) projekty związane z oceną kompetencji i certyfikacją. Kontakty: urp@inapp.org (lub niektóre konkretne działy, jak atlante_lq@inapp.org) | Podobnie jak poprzedni wspomniany interesariusz (Veneto Lavoro) INAPP mógłby mocno wesprzeć nasz projekt, w zakresie wymiany i sugestii dotyczących całego procesu certyfikacji. W szczególności, INAPP prowadzi nowy "Atlante del lavoro e delle qualificazioni" (Atlas zawodów i kwalifikacji). Atlas jest ogólną (krajową) bazą danych / repertorium dla standardów zawodowych i kwalifikacji. Zawiera również profile dla studentów (szkoły średnie i uniwersytety) oraz linie przewodnie dla VET i centrów szkoleniowych. Ostatnio INAPP uruchomił również "Atlas dla profesjonalistów" (takich jak konsultanci, trenerzy, prawnicy, itp.) i mogą oni sprawdzić postępy projektu w zakresie nowych profili "TEBEISI IT secury i menedżerów DP". W perspektywie średnioterminowej, wprowadzić i promować również ten nowy profil. INAPP mógłby również sprawdzić zawartość projektu pod kątem przyszłych EFS - Europejskich Funduszy Społecznych - nowych kursów szkoleniowych (program: 2021 _ 2027) opartych na wynikach TEBEISI. INAPP mógłby być informowany o postępach, na poziomie regionalnym. I sprawdzić, dając pewne uwagi/sugestie w zakresie spójności i trwałości projektu w perspektywie średnioterminowej. Mogłaby również ocenić materiały szkoleniowe, w tym przede wszystkim proces certyfikacji (częściowej) kompetencji, przynajmniej na poziomie krajowym. NAPP prowadzi dziesiątki grup roboczych na poziomie krajowym. Wielokrotnie grupy te działają również na poziomie regionalnym. Moglibyśmy więc spotkać się i przedyskutować z niektórymi członkami grup, proponując im regionalny plan adaptacji, przed zamknięciem projektu. | www.inapp.org |
| AIPSI | Associazione italiana dei professionisti sicurezza informatica (włoskie stowarzyszenie specjalistów i ekspertów ds. bezpieczeństwa IT). Jest to włoski oddział ISSA, międzynarodowej organizacji non-profit zrzeszającej profesjonalistów i doświadczonych praktyków. Dzięki aktywnemu udziałowi poszczególnych członków i ich oddziałów na całym świecie, AIPSI, jako oddział ISSA, jest częścią największego | AIPSI jest jednym z najważniejszych włoskich stowarzyszeń zrzeszających ekspertów ds. bezpieczeństwa IT. Współpracuje ono jednak również z menedżerami ochrony danych. Oferuje szeroki zakres usług, przydatnych dla projektu TEBEISI, takich jak: ankiety i badania, raporty, szkolenia i konsultacje oraz, oczywiście, (częściowo) działania związane z oceną i certyfikacją profili zawodowych. Większość ich kursów (bezpłatnych lub płatnych) uzyskała już certyfikację krajowej lub regionalnej instytucji. Jest to również część szerszej międzynarodowej sieci, więc może dać nam szerszą wizję i dalsze informacje. AIPSI może sprawdzić zawartość projektu i fazy oceny. W szczególności, mogłoby zaakceptować i zweryfikować niektóre nowe materiały szkoleniowe, na przykład niektóre specyficzne kompetencje (takie jak umiejętności miękkie lub osobiste). AIPSI ma kilku członków pochodzących również z regionu Veneto (istnieje również lokalne biuro w Wenecji; większość lokalnych członków to inżynierowie informatyki). Z nimi moglibyśmy wymienić się niektórymi treściami, a przede wszystkim | www.aipsi.org |

| | | | |
|---|---|---|---|
| | stowarzyszenia non-profit zrzeszającego specjalistów ds. bezpieczeństwa, liczącego ponad 13.000 osób na całym świecie. Osoba kontaktowa: Pani Yvette Agostini (Dyrektor, info@aipsi.org) | sprawdzić wersje końcowe. Ponadto, nasz projekt mógłby połączyć członków Clusit (którzy są profesjonalistami) z MŚP. AIPSI bierze już udział w kilku technicznych grupach roboczych, na poziomie krajowym (w szczególności Ministerstwo Innowacji i Edukacji) oraz w kilku regionalnych grupach zadaniowych. W szczególności, ich raporty i publikacje stanowią podstawę naukową dla dalszych ulepszeń legislacyjnych w dziedzinie rozpoznawania (nowych) profili zawodowych. W naszym regionie, lokalny prezydent lub dyrektor AIPSI mógłby reprezentować ekspertów naukowych i technicznych. | |
| CLUSIT | Associazione Italiana per la sicurezza informatica (włoskie stowarzyszenie na rzecz bezpieczeństwa informatycznego). CLUSIT Italy powstało na bazie doświadczeń innych europejskich stowarzyszeń bezpieczeństwa informatycznego, takich jak CLUSIB (Belgia), CLUSIF (Francja), CLUSIS (Szwajcaria) CLUSIL (Luksemburg), które od ponad 20 lat stanowią punkt odniesienia dla bezpieczeństwa informatycznego w swoich krajach. Główny cel: Rozpowszechnianie kultury bezpieczeństwa informacji wśród firm, administracji publicznej i obywateli.<br>Osoba kontaktowa: Pan Gabriele Faggioli (Prezes; president@clusit.it) | Clusit jest jednym z najważniejszych włoskich stowarzyszeń zrzeszających ekspertów ds. bezpieczeństwa IT. Współpracuje jednak również z menedżerami ochrony danych. Oferuje szeroki zakres usług, przydatnych dla projektu TEBEISI, takich jak: ankiety i badania, raporty, szkolenia i konsultacje oraz, oczywiście, (częściowo) działania związane z oceną i certyfikacją profili zawodowych. Większość ich kursów (bezpłatnych lub odpłatnych) uzyskała już certyfikację krajowej lub regionalnej instytucji. Clusit mógł sprawdzić zawartość projektu i etapy oceny. W szczególności, mógłby zaakceptować i zweryfikować niektóre nowe materiały szkoleniowe, na przykład niektóre specyficzne kompetencje (jak umiejętności miękkie lub osobiste). Clusit ma kilku członków, którzy pochodzą również z regionu Veneto (większość z nich to inżynierowie informatyki). Z nimi moglibyśmy wymieniać się treściami, a przede wszystkim sprawdzać wersje końcowe. Ponadto, nasz projekt mógłby połączyć członków Clusit (którzy są profesjonalistami) z MŚP. Clusit już bierze udział w kilku technicznych grupach roboczych, na poziomie krajowym (Ministerstwo Innowacji i Edukacji w szczególności) oraz w kilku regionalnych grupach zadaniowych. W szczególności, ich raporty i publikacje stanowią podstawę naukową dla dalszych ulepszeń legislacyjnych w dziedzinie rozpoznawania (nowych) profili zawodowych. | www.clusit.it |
| Padua University – wydział informatyki i inżynierii komputerowej" . | W ostatnich latach przeprowadzili kilka ankiet dotyczących tematyki projektu.Osoba kontaktowa: Prof. Antonio Scipioni (scipioni@unipd.it). | Padua University already organizes second level masters on project topics (data protection manager, IT security expert, etc.) and also training courses. Their training contents and paths could be useful for the competenteces and job profiles selection. They could involve managers, experts and SMEs, for example for making inteviews, workshops, etc. As University, they could “guarantee” a scientific approach and the right methodologies. As athenaeum they could involve also several departments (economy, law, IT - informatics, management, etc.). The university is a public body, that takes part into several regional steering committee and working groups, including also expert groups on project topics. So, if they are aware on project progress they could support the certification process at regional level. | www.unipd.it |
| APCO – Włoskie stowarzyszenie konsultantów zarządzania | Jest to włoskie stowarzyszenie konsultantów zarządzania, założone w 1968 roku; obecnie liczy ponad 400 członków. APCO oferuje kilka usług dla członków, takich jak: szkolenia, inicjatywy sieciowe, lobby z instytucjami, itp. Osoba do kontaktu: Pani Cesara Pasini (Prezes; mail: presidenza@apcoitalia.it) | APCO posiada kilka "społeczności praktyki", które koncentrują się na różnych tematach. W szczególności dwie z nich (transformacja cyfrowa / menedżer innowacji i zgodność / normy ISO) mogą nam pomóc w certyfikacji częściowej.<br>APCO promowało specjalną ustawę krajową (nr 4, rok 2013), która uznała również konsultantów, którzy nie są zarejestrowani w organizacji zawodowej (zgodnie z prawem), ale posiadają profesję certyfikacyjną i ciągłe szkolenia. APCO jest dostępne do organizowania spotkań (również on-line), z niektórymi członkami, którzy pracują nad tematami projektów. APCO nie jest organem publicznym, ale czymś w rodzaju organizacji "pośredniej", która reprezentuje również lokalne/regionalne interesy zbiorowe. Na przykład, istnieje delegacja "Północny Wschód" (region Veneto, Trentino Alto | www.apcoitalia.it |

| | | | |
|---|---|---|---|
| | | Adige i Friuli Venezia Giulia), która może być zaangażowana w niektóre działania projektowe. Delegacja lokalna (region Veneto, Pan Paolo Ferrarese jako koordynator) mogłaby prowadzić lobbying z naszymi władzami lokalnymi (Region, departament pracy i szkoleń). | |

*Tabela 4: Interesariusze z Włoch*

GDPR we Włoszech oficjalnie obowiązuje już od jakiegoś czasu, dokładnie od 25 maja 2018 roku. Następnie, 19 września 2018 roku, wszedł w życie tekst dostosowujący włoskie przepisy do ogólnego rozporządzenia o ochronie danych, czyli dekret 101/2018.

**Włoskie GDPR: jak wygląda sytuacja po trzech latach?**

W czerwcu 2021 r. "Urząd ds. nadzoru nad prywatnością" opublikował sprawozdanie ze swojej działalności w ciągu trzech lat egzekwowania rozporządzenia i okazało się, że nastąpił wzrost świadomości osób, których dane dotyczą, w odniesieniu do ich praw, z około 27 192 skargami i zgłoszeniami naruszeń do Garante. (GDPD 2020) Wysoka liczba zgłoszeń, około 24 dziennie, 365 dni w roku przez trzy lata, pokazuje, że przyjęcie GDPR z pewnością zwiększyło świadomość osób, których dane dotyczą, w zakresie istnienia ich praw i żądania ich ochrony.

Liczba powiadomień wzrosła do 2839 w kwartale między 1 stycznia a 31 marca 2021 r., co świadczy o tym, że rok pandemii wraz z cyfryzacją wielu działań doprowadził również do zwrócenia większej uwagi użytkowników na kwestię ochrony danych osobowych.

Podobnie było z 3 873 powiadomieniami o naruszeniu danych (ok. 3,5 dziennie), co stanowi niewiele w porównaniu ze statystykami dotyczącymi cyberataków, niemniej jednak wskazuje na znaczenie przyjęcia polityk i narzędzi bezpieczeństwa, które pomogą im zapobiec. W każdym razie podstawowym aspektem jest szkolenie pracowników i podnoszenie ich świadomości w zakresie bezpieczeństwa i postępowania w przypadku wniosków niezgodnych z procedurami przedsiębiorstwa.

Podano nazwiska 59 838 inspektorów ochrony danych (zwanych również DPO), i nie wszyscy z nich zostali podani przez administracje publiczne, które na mocy rozporządzenia są zobowiązane do powołania DPO. Pokazuje to, że potrzeba posiadania osoby koordynującej, nadzorującej i kontaktującej się między organem nadzorczym, podmiotami danych i administratorem danych jest postrzegana jako ważny wymóg.

Jeśli chodzi o sankcje, w Europie przeprowadzono 654 postępowania na łączną kwotę 283 757 083 EUR (źródło). Patrząc na statystyki w podziale na kraje, Włochy zajmują pierwsze miejsce pod względem łącznej kwoty nałożonych sankcji w wysokości 76 298 601 EUR w 79 przypadkach, co potwierdza aktywność włoskiej Garante i uwagę, z jaką rozpatrywane są skargi i zgłoszenia. Liczba ta uwzględnia oczywiście tylko sankcje nałożone na mocy art. 83 GDPR i nie bierze pod uwagę żadnych odszkodowań lub rekompensat wypłaconych osobom, których dane dotyczą, a których prawa zostały naruszone. Jak stwierdzili członkowie organu nadzorczego w rocznicę wydania rozporządzenia UE, przed nami jeszcze długa droga do połączenia cyfryzacji

państw członkowskich z bezpiecznym zarządzaniem infrastrukturą. Wzrost wrażliwości firm, spowodowany mniej lub bardziej wymuszonym przyjęciem rozwiązań pracy zdalnej, wymaga od właścicieli przemyślenia na nowo przepływu danych i procedur bezpieczeństwa w swoich organizacjach.

Ale co to oznacza dla przedsiębiorców w naszym kraju? Na szczęście tendencja wydaje się pozytywna. Prawie dwa lata po pełnym wprowadzeniu rozporządzenia w życie, we Włoszech dokonuje się znaczny postęp w zakresie zgodności z rozporządzeniem, przy jednoczesnym zwiększeniu budżetu dostępnego dla organizacji i wzroście dojrzałości, jeśli chodzi o konkretność projektów i ukierunkowanych zmian organizacyjnych.

Złożoność i znaczenie tego zagadnienia wymagają jednak od przedsiębiorstw nieustannych wysiłków na rzecz dostosowania się do zasad narzuconych przez przepisy o ochronie danych oraz reagowania na wnioski władz. W tym względzie w kilku krajach europejskich nałożono pierwsze grzywny za naruszenie przepisów rozporządzenia. We Włoszech natomiast postawa organu nadzorczego była początkowo przychylna, również ze względu na opóźnienia w wyborze nowego kolegium organu nadzorczego. Jednak w ostatnim okresie zaobserwowano nasilenie kontroli i inspekcji oraz zastosowanie pierwszych sankcji przewidzianych przez lokalne i ponadnarodowe przepisy dotyczące ochrony danych.Dzięki badaniom przeprowadzonym przez Cyber Security & Data Protection Observatory możemy zobaczyć, jak te przepisy zmieniają włoski rynek.

**Stan zgodności z włoskim GDPR**

W celu zbadania zmian zachodzących we włoskich przedsiębiorstwach w zakresie ochrony danych, Protection Observatory przeanalizowało cztery aspekty:

- status projektów zgodności
- dedykowany budżet
- wdrożone działania
- napotkane problemy krytyczne

Z badania wynika, że prawie wszystkie włoskie firmy wdrożyły lub udoskonaliły projekty dotyczące zgodności z GDPR. Ponad połowa organizacji stwierdziła, że spełniła wymagania przepisów, a jednocześnie zmniejszyła się liczba firm, które stwierdziły, że nie są świadome konsekwencji GDPR.

W tej ostatniej kwestii należy jednak zaznaczyć, że są to firmy, w których kwestia ochrony danych nie dotarła jeszcze na szczyt, ale jest znana specjalistycznym działom, takim jak bezpieczeństwo IT, dział prawny i dział zgodności. Innym pozytywnym znakiem dojrzałości i świadomości GDPR we Włoszech jest niski odsetek firm (5%), które nadal są na etapie analizy wymogów i definiowania planów zgodności, podczas gdy dwa lata temu odsetek ten wynosił 34%. Obraz jest również pozytywny, jeśli chodzi o budżet przeznaczony na środki zgodności z GDPR: 45% włoskich firm zwiększyło swój dedykowany budżet. Chociaż liczba ta jest pozytywna, prawdą jest

również, że należy jeszcze przesunąć punkt ciężkości na konkretne działania, takie jak okresowe audyty, aktualizacja procedur oraz technologie bezpieczeństwa i ochrony danych. (Andrea Antonelli 2020)

### Działania DPR w zakresie zgodności

Konkretnie, co robią włoskie firmy, aby dostosować się do GDPR? Należy pamiętać, że proces zgodności musi koniecznie składać się z kilku etapów, które obecnie mają różne poziomy przyjęcia:

- Utworzenie rejestru przetwarzania danych (85%): obowiązkowe utworzenie rejestru, w którym należy odnotowywać wszystkie przeprowadzone operacje przetwarzania danych;
- Określenie ról i obowiązków (81 %): określenie i zawarcie umów ze wszystkimi osobami odpowiedzialnymi za przetwarzanie danych;
- Modyfikacja formularzy (76%): aktualizacja formularzy zgodnie z wymogami GDPR;
- Procedura powiadamiania o naruszeniu danych (68%): proces powiadamiania organu nadzorczego o naruszeniu poufnych danych;
- określenie polityki bezpieczeństwa i ocena ryzyka (66%): przyjęcie środków w celu zapewnienia zgodności przetwarzania z rozporządzeniem;
- ocena skutków w zakresie ochrony danych (56%): obowiązkowa ocena skutków w zakresie ochrony danych (DPIA), gdy przetwarzanie może wiązać się z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą;
- wdrożenie procesów służących wykonywaniu praw osób, których dane dotyczą (54%): działania mające na celu egzekwowanie praw przyznanych osobom, których dane dotyczą w wyniku przetwarzania. (Andrea Antonelli 2020)

Oprócz tych działań, należy również rozważyć wprowadzenie w firmach funkcji Inspektora Ochrony Danych (IOD). Osoba ta, której powołanie jest w wielu przypadkach przewidziane przez GDPR, jest obecna w 65% organizacji. Liczba ta jest z pewnością pozytywna, ponieważ ujawnia wzrost liczby firm, które wprowadziły tę funkcję.

### Jakie krytyczne kwestie wiążą się z GDPR dla włoskich firm?

Jeśli prawdą jest, że obraz stanu zgodności z włoskim GDPR jest ogólnie pozytywny, prawdą jest również, że organizacje napotkały pewne trudności. W rzeczywistości wiele firm nadal doświadcza trudności z organizacyjnego punktu widzenia, na przykład w zakresie identyfikacji ról i obowiązków w firmie, podczas gdy inne zgłaszają znaczne spowolnienie w codziennej działalności.

Jednak te negatywne elementy nie mają większego znaczenia w porównaniu z dojrzałym scenariuszem, w którym włoskie firmy okazują się nie tylko zorientowane na wyzwania związane z ochroną danych, ale także świadome całego zagadnienia.

## 2.5 Litwa

| Nazwa Instytucji | Krótki Opis | Główne cele | Strona internetowa |
|---|---|---|---|
| Alytus Centrum Doradztwa Biznesowego (AVKC) | Alytus Business Consulting Center (AVKC) jest pierwszym centrum doradztwa biznesowego na Litwie, zarejestrowanym 13 maja 1993 r. jako organizacja non-profit, która następnie została ponownie zarejestrowana jako instytucja publiczna. Alytus Business Consulting Centre - Alytus Regional Development Strategy uczestnikiem międzynarodowej współpracy w zakresie rozwoju regionalnego z szwedzkim Jonkompingo County, Polską, Danią, Węgrami, Włochami, władzami regionalnymi, Ministerstwem istniejących agencji rozwoju biznesu, gminami powiatu Alytus i powiązanymi strukturami inicjatora. | Misja Alytus Business Consulting Center - promowanie i rozwój małych i średnich przedsiębiorstw, zapewnienie szkoleń biznesowych, doradztwo, informacje, nowe inicjatywy rozwoju biznesu w rozwoju i realizacji rozwoju sieci w regionie Alytus. | https://www.avkc.lt/lt/ |
| Stowarzyszenie Kierowników Gminnych Ośrodków Pomocy Społecznej | Stowarzyszenie Kierowników Gminnych Ośrodków Pomocy Społecznej - niezależna, dobrowolna organizacja non-profit, skupiająca 30 gminnych ośrodków pomocy społecznej | Cel Stowarzyszenia - pomoc w rozwiązywaniu problemów osób korzystających z opieki społecznej wszystkich grup społecznych poprzez poprawę ich jakości życia i integracji ze społeczeństwem. | http://ssgivasociacija.blogspot.com/ |
| Kancelaria prawna ALIANT Tarvainyte Vilys Bitinas | Zespół ALIANT® na Litwie świadczy zintegrowane usługi prawne we wszystkich procesach zarządzania i rozwoju biznesu oraz w sporach biznesowych w krajowych i międzynarodowych instytucjach sądowych. Pracują również w dziedzinie ochrony danych osobowych. | Zespół ALIANT® na Litwie świadczy zintegrowane usługi prawne we wszystkich procesach zarządzania i rozwoju biznesu oraz w sporach biznesowych w krajowych i międzynarodowych instytucjach sądowych. | www.aliantlaw.lt |
| LDAPA - Litewskie Stowarzyszenie | Priorytetem członków LDAPA jest stworzenie innowacyjnej, niekomercyjnej platformy nowej generacji dla profesjonalistów z zakresu ochrony | Priorytetem członków LDAPA jest stworzenie innowacyjnej, | https://ldapa.lt/ |

| | | | |
|---|---|---|---|
| Inspektoró w Ochrony Danych. | danych osobowych, umożliwiającej dzielenie się specjalistyczną wiedzą prawną, dobrymi praktykami, praktycznymi i nowymi rozwiązaniami. | niekomercyjnej platformy nowej generacji dla profesjonalistów z zakresu ochrony danych osobowych, umożliwiającej dzielenie się specjalistyczną wiedzą prawną, dobrymi praktykami, praktycznymi i nowymi rozwiązaniami. | |
| Centrum Bezpiec-zeństwa In-formacji | W celu osiągnięcia celów operacyjnych Centrum, administratorzy danych i podmioty przetwarzające dane są konsultowani w zakresie wdrażania odpowiednich środków technicznych i organizacyjnych służących ochronie danych. Osoby, których dane dotyczą, są konsultowane w zakresie realizacji praw człowieka w dziedzinie ochrony danych. | Celem Centrum Bezpieczeństwa Informacji jest podnoszenie świadomości społecznej w zakresie bezpiecznego przetwarzania danych osobowych, ochrony informacji oraz cyberbezpieczeństw a. | https://in-fosec.mobi/ |

**Tabela 5: Interesariusze z Litwy**

Ustawa o rozwoju małego i średniego biznesu Republiki Litewskiej (2017) określa, że małe i średnie podmioty gospodarcze to średnie, małe i bardzo małe przedsiębiorstwa, które spełniają określone wymagania (liczba pracowników, dochód, niezależność) oraz osoby fizyczne uprawnione do samozatrudnienia, działań handlowych i innych podobnych. W ciągu 2019 r. liczba małych i średnich przedsiębiorstw wzrosła o 0,4 proc. (zarejestrowanych 11153). Największy udział - 83% - wśród MŚP stanowiły przedsiębiorstwa bardzo małe (0-9 pracowników). Małe przedsiębiorstwa stanowiły 14% (10-49 pracowników), średnie (50-249 pracowników) - 3% w 2019 r. W ciągu roku liczba pracujących w MŚP wzrosła o 2,2%.

Pomimo postępów w sektorze małych i średnich przedsiębiorstw, poprawy ogólnego otoczenia biznesu i zmniejszenia barier utrudniających wejście na rynek, dynamika przedsiębiorczości na Litwie jest nadal słaba. Procedury administracyjne dotyczące zakładania nowych przedsiębiorstw są skomplikowane, a przedsiębiorcom brakuje kapitału początkowego, umiejętności w zakresie zarządzania i finansów, umiejętności marketingowych i eksportowych oraz informacji. Decyzje mające na celu przezwyciężenie kryzysu pandemicznego, pobudzenie gospodarki i poprawę otoczenia biznesowego są trudne do wdrożenia i nie przynoszą oczekiwanych rezultatów..

Badania w ramach projektu TebeISi na Litwie pokazują, że zbyt mało uwagi poświęca się tej kwestii. Niewystarczająca uwaga poświęcana jest sektorowi publicznemu oraz małym i średnim przedsiębiorstwom. Brak uwagi związany jest z brakiem funduszy. Większą uwagę w kwestii bezpieczeństwa informacji poświęca się tej części społeczeństwa, która w taki czy inny sposób jest bardziej narażona. Zdaniem ekspertów, dużo uwagi poświęca się instytucjom państwowym. Jeśli chodzi o biznes - nacisk jest znacznie mniejszy, ponieważ niewiele osób w pełni rozumie to zagadnienie. Uwaga opinii publicznej w odniesieniu do bezpieczeństwa informacji wzrasta również po incydentach związanych z bezpieczeństwem publicznym. Badania pokazują, że MŚP nie poświęcają wystarczającej uwagi szkoleniom wewnętrznym. Zwykle zależy to od inicjatywy samych pracowników w poszukiwaniu i uczestniczeniu w szkoleniu. Ostatnio eksperci powiązali również brak szkoleń z trudną sytuacją pandemii COVID-19, kiedy wiele firm zostało zawieszonych i skupiło się na przetrwaniu.

Badanie ilościowe przeprowadzone przez M. Lipinskienesa (Austriacka Agencja Prasowa 2020) (2019) dotyczące wdrożenia Ogólnego Rozporządzenia o Ochronie Danych w litewskich przedsiębiorstwach wykazało, że przedsiębiorstwa biorące udział w badaniu na Litwie, które samodzielnie przetwarzają dane osobowe oraz powierzyły przetwarzanie danych podmiotowi przetwarzającemu dane, w wystarczającym stopniu przestrzegają GDPR. Podczas badania ankietowego respondenci odpowiadali na stwierdzenie: "firma, którą reprezentuję, skutecznie wdrożyła wymagania GDPR " od 1 "zdecydowanie się nie zgadzam" do 100 "zdecydowanie się zgadzam". Odpowiedzi zostały zakodowane w programie SPSS na skali interwałowej i obliczono średnią ocenę respondentów. Łącznie 77 respondentów udzieliło odpowiedzi na to stwierdzenie, najniższa ocena wynosiła 0, najwyższa 100, a średnia ocena wyniosła 77 na skali 100-punktowej, co oznacza "zgadzam się". Najczęściej respondenci oceniali swoje firmy na 100 punktów - 23 respondentów, 8 respondentów - na 95 punktów, 6 - na 90 punktów, 7 - na 85 punktów, 6 - na 80 punktów. Do wyniku 80 punktów odpowiedzi oceniane są jako "zdecydowanie zgadzam się", co oznacza pełną zgodność z GDPR. Takich firm było 50 na 77 respondentów, co stanowi 65%. Ponad połowa przedstawicieli firm zgadza się ze stwierdzeniem, że firma przestrzega standardu GDPR jako "całkowicie się zgadzam".

Badanie wykazało, że w opinii respondentów rozporządzenie jest dość abstrakcyjne, lakoniczne, trudne do przeczytania i trudne do zrozumienia dla osób niezwiązanych zawodowo z prawem. Firmom, które same przetwarzają dane, brakuje wiedzy i zrozumienia GDPR, co prowadzi do niewiedzy i niezdecydowania. Szkolenia wewnętrzne są jednak ważne i istotne dla każdego pracownika firmy oraz dla samej firmy. Aby zachować zgodność z GDPR, administrator danych musi dowiedzieć się, jakie dane osobowe są przechowywane, gdzie, w jakim celu, jak długo, w jaki sposób są one przetwarzane i przechowywane. Tylko dzięki zrozumieniu tego, co się posiada, administrator danych będzie wiedział, jak się zachowywać i zarządzać. Zostało to potwierdzone przez projekt TebeISi desk reseach (IO1), przetwarzanie danych i oceny ochrony danych osobowych jako okazja do zidentyfikowania zbędnych informacji i przeglądu procesów biznesowych. W ten sposób w firmach zostaną rozpoznane efektywne procesy biznesowe, a nieefektywne i zbędne etapy procesów zostaną

zredukowane lub wyeliminowane. Pomogłoby to firmom zapewnić bezpieczeństwo informacji i ochronę danych osobowych.

### Sytuacja szkoleniowa

Na Litwie istnieje szeroki zakres szkoleń (od 1,5 godziny do kilku dni) w zakresie bezpieczeństwa danych i informacji. Najczęściej szkolenia prowadzone są przez instytucje prywatne, na przykład: Cyber Security Academy założona przez UAB "Hermitage Solutions", której celem jest szkolenie informatyków, którzy są w stanie rozwiązać skomplikowane problemy związane z cyberbezpieczeństwem w sposób terminowy i skuteczny oraz ocenić podatność infrastruktury informatycznej swojej organizacji. UAB "Atea", która jest wiodącym bałtyckim dostawcą rozwiązań i usług IT oraz wspiera klientów specjalistycznymi kompetencjami, produktami, usługami i rozwiązaniami w zakresie infrastruktury IT, rozwoju oprogramowania i bezpieczeństwa. NRD Cyber Security, która jest firmą doradczą w zakresie technologii cyberbezpieczeństwa, reagowania na incydenty oraz badań stosowanych. Firma koncentruje się na usługach dla wyspecjalizowanych dostawców usług publicznych (organy ścigania, krajowe CERT, telekomunikacja, krajowe organy regulacyjne komunikacji, krajowa infrastruktura krytyczna), branży finansowej i korporacji o wysokiej wrażliwości danych. UAB "Competence Development", które oferują kursy szkoleniowe przygotowujące do najbardziej popularnych certyfikatów, które są podstawą do pracy z urządzeniami innych producentów, więc te certyfikaty są często preferowane przez pracodawców nie tylko na Litwie, ale także za granicą.

Szkolenia z zakresu bezpieczeństwa informacji organizowane są dla różnych grup docelowych: zarówno dla początkujących, jak i zaawansowanych użytkowników IT oraz profesjonalistów IT. Głównymi tematami szkoleń informacyjnych są: "Szkolenia z zakresu bezpieczeństwa informacji"; "Szkolenia z zakresu cyberbezpieczeństwa"; "Szkolenia z zakresu bezpieczeństwa informacji dla nieprofesjonalistów". Osobną grupę szkoleń z zakresu bezpieczeństwa informacji stanowią szkolenia dla profesjonalistów IT. Są oni szkoleni w takich tematach jak: "Podstawy cyberbezpieczeństwa"; "Hack IT to Defend IT"; "Praktyk etycznego hakera"; "Bezpieczne programowanie"; "Praktyk bezpieczeństwa IT"; "Zarządzanie incydentami cyberbezpieczeństwa" oraz "Szkolenie świadomości bezpieczeństwa IT".

Profesjonalne szkolenia na różnych poziomach zaawansowania z tematyki ochrony danych osobowych przeznaczone są głównie dla specjalistów IT. Główne tematy takich szkoleń związane są z Ochroną danych osobowych w kontekście szkoleń dotyczących wymogów GDPR. Szkolenia z zakresu bezpieczeństwa danych organizowane są również dla prawników korporacyjnych, administratorów, kierowników, osób zarządzających pracownikami. Na takich szkoleniach zapoznawani są z GDPR; "Ochrona danych osobowych i odpowiedzialność za naruszenia GDPR"; "Ochrona danych osobowych i naruszenia przepisów o danych osobowych w 2018 roku".

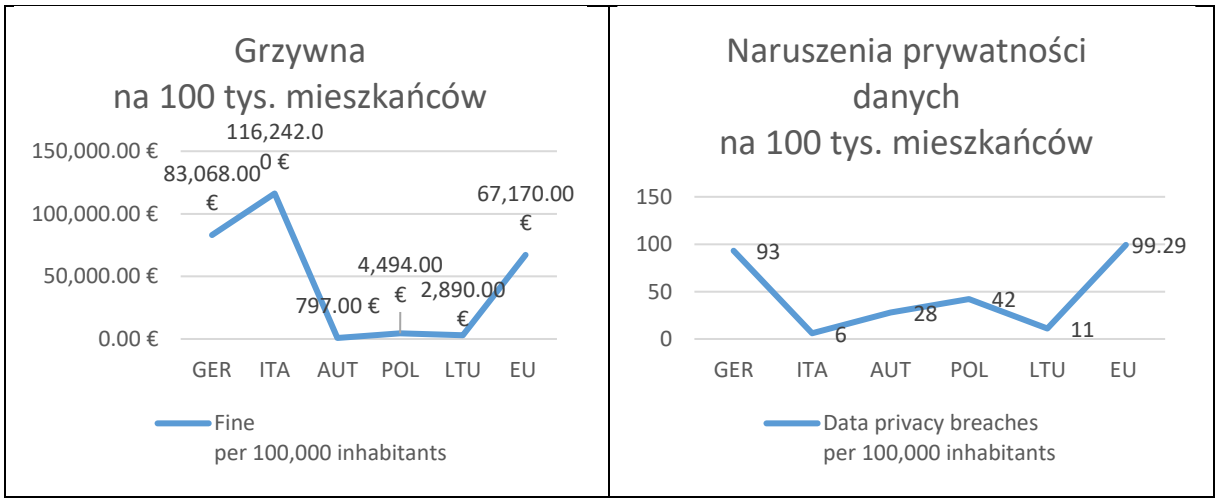
## 2.6 GDPR a działalność gospodarcza

Wraz z zainicjowaniem GDPR w 2018 roku Komisja Europejska wyznaczyła spójne szlaki ochronne zapewniające podstawowe prawo do ochrony danych i dające podstawy do realizacji Karty Praw Podstawowych Unii Europejskiej. GDPR pobudziło wiele innych krajów na całym świecie do aktywności w zakresie ich regulacji ochrony danych i podążania ścieżką UE oraz wpływania na stanowisko i zachowanie wszystkich interesariuszy z korzyścią dla obywateli Europy.

Niemniej jednak przyjęcie europejskiej strategii w zakresie danych (Komisja Europejska 2020a) napotyka na kilka przeszkód, o których Komisja Europejska poinformowała w komunikacie dotyczącym wdrażania GDPR (Komisja Europejska 2020b). W międzyczasie wśród obywateli wzrosła ogólna świadomość wartości danych osobowych, a prawa proceduralne zwiększyły możliwość zgłaszania przypadków uchybień, zwłaszcza w przypadku transgranicznego wykorzystywania danych. W związku z tym należy zbadać prawo do przenoszenia danych między usługami z korzyścią dla wykorzystania dóbr publicznych oraz ujawnić czynniki ograniczające. (Komisja Europejska 02.06.2020).

Jeśli chodzi o potrzeby MŚP, GDPR zwiększyło możliwości swobodnego przepływu danych w obrębie UE i usprawniło przepływ danych z firmami spoza UE, a tym samym wsparło innowacje i działalność gospodarczą. MŚP muszą jednak poradzić sobie ze stosunkowo wymagającym wdrożeniem GDPR, aby móc skorzystać z tych nowych możliwości, ponieważ ryzyko naruszenia danych nie zmniejsza się wraz z wielkością operacji. Należy zatem zwiększyć wysiłki na rzecz zapewnienia praktycznych i łatwych w użyciu narzędzi dla MŚP. Komisja zamierza wesprzeć zwłaszcza MŚP, dostarczając wzory umów i klauzul zgodnych z GDPR.

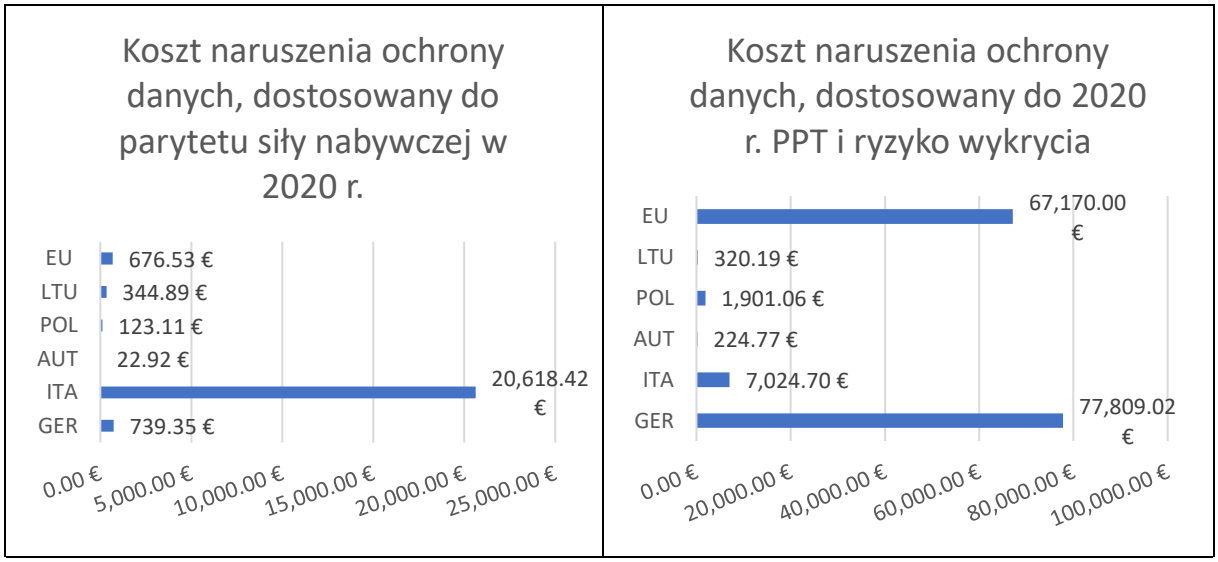
Ostatecznie udane wdrożenie odzwierciedla się w skutecznym egzekwowaniu przepisów przez krajowe organy ochrony danych. Jak widać na wykresie 6, w poszczególnych państwach członkowskich widoczne są duże różnice.




**Wykres 9: Egzekwowanie prawa ochrony danych w krajach członkowskich. Wartości netto na 100.000 mieszkańców.**

Dane: heyData (2021). Ilustracja własna.

W międzyczasie wszystkie kraje pozostają poniżej średniej UE w zakresie łącznej liczby naruszeń ochrony danych na 100 000 mieszkańców, która jest zdominowana przez duże liczby zgłoszone w Irlandii (245), Danii (325) i Holandii (382), można zauważyć znaczny wzrost w przypadku zapłaconych grzywien. Aby lepiej zrozumieć związek między kwotą zapłaconych grzywien a liczbą naruszeń, wartości netto zostały dostosowane do parytetu siły nabywczej, aby zapewnić porównywalność między krajami. Wyniki pokazują, że Niemcy są bliskie średniego wskaźnika wykrywalności w UE, natomiast Włochy, Austria, Polska i Litwa plasują się znacznie poniżej tego wskaźnika. Podobne ustalenia można zaobserwować w odniesieniu do płaconych grzywien, z wyraźnym wyjątkiem w przypadku Włoch, gdzie płacone grzywny niemal podwajają średnią europejską i przewyższają te w Niemczech o około 40%. Rysunek 7 (po lewej) oraz ponownie dla ryzyka wykrycia, podczas gdy średni poziom ryzyka obliczono poprzez ustalenie średniej wartości dla UE na poziomie 1.




**Wykres 10: Koszty naruszeń ochrony danych skorygowane o parytet siły nabywczej i ryzyko wykrycia**

Dane: heyData (2021). Ilustracja własna.

Tymczasem z obserwacji korekt ppt jasno wynika, że w każdym zgłoszonym przypadku we Włoszech obserwuje się skrajny wzrost, natomiast korekta ryzyka jasno pokazuje, że są to bardzo nieliczne przypadki, w których nałożono wysokie grzywny. Niemniej jednak można zauważyć, że istnieją duże rozbieżności w obliczaniu kosztów ryzyka związanego z naruszeniami ochrony danych, przy czym w Austrii, na Litwie i w Polsce kary są znikome, a w Niemczech - surowe. Można zatem stwierdzić, że egzekwowanie prawa ma jeszcze przed sobą długą drogę, by stać się równie skuteczne we wszystkich państwach członkowskich.

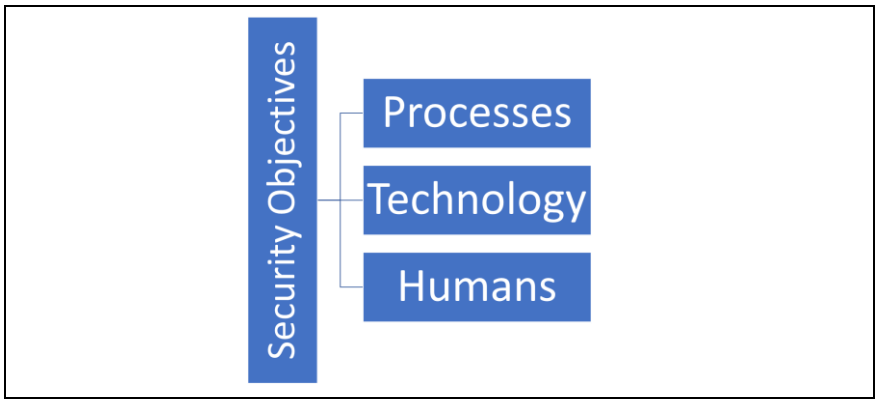
Biorąc pod uwagę indywidualne sytuacje w krajach partnerskich, szczególnie dla MŚP, wyzwania w procesie wdrażania stają się oczywiste. W szczególności brak czasu i zasobów został zidentyfikowany jako główne przyczyny powolnego wdrażania. Zwłaszcza dostosowanie procesów i kontrola informacji istotnych z punktu widzenia GDPR w firmie to obszary, w których we wszystkich krajach MŚP mają możliwość wprowadzenia usprawnień. Ostatecznie kwestia właściwego wdrożenia jest ściśle

związana z dostępnością personelu i zapotrzebowaniem na szkolenia zorientowane na praktykę. Silny popyt na kursy dokształcające (zarówno dobrowolne, jak i obowiązkowe) ilustruje lukę rynkową w zakresie zwięzłych, uniwersalnych i przejrzystych kursów, zgodnie z sugestiami zawartymi w programie badań TeBelSi.

## 2.7 Najsłabsze ogniwo - rola pracowników i rachunek prywatności

W świetle wysiłków podejmowanych przez firmy, organizacje pozarządowe i władze publiczne w celu wprowadzenia GDPR w życie, udane wdrożenie napotyka na te same ograniczenia, co wdrożenie bezpieczeństwa informacji: czynnik ludzki. Jak wykazano w rozdziale 2.6, istnieje duże zapotrzebowanie na personel, a zwłaszcza na kursy dokształcające. Pracownicy, będący główną przyczyną utraty informacji i naruszeń ochrony danych, odgrywają kluczową rolę w prowadzeniu i przestrzeganiu zasad ochrony danych i bezpieczeństwa informacji.

Firmy mają wiele możliwości zapewnienia ochrony swoich danych, zarówno na poziomie organizacyjnym, jak i technicznym. Z organizacyjnego punktu widzenia, mogą one wdrożyć procesy, które zapewnią, że gromadzona jest jedynie marginalna ilość danych, że fizyczne i cyfrowe magazyny są zabezpieczone, że dostęp do danych jest ograniczony do odpowiedniego personelu itp. Analiza i wdrożenie tych środków leżą w gestii urzędnika ds. bezpieczeństwa informacji we współpracy z kierownictwem firmy i przy jego wsparciu.




**Wykres 11: Wymiary ryzyka dla celów bezpieczeństwa**

Na poziomie technicznym, można zaprojektować programy i aplikacje, które zapewniają zgodność z prawem ochrony danych i specyficznymi regulacjami firmy, tj. privacy by design. Dostawcy usług zaczęli tworzyć model biznesowy z platform typu Software as a Service (SaaS), wdrażając Privacy as a Service (PaaS). W ten sposób, za zgodą użytkownika, przechowywanie i przetwarzanie informacji jest skoncentrowane na właściwym postępowaniu zgodnie z indywidualnymi wymaganiami. Ponadto, znaczenie bezpiecznego oprogramowania potwierdza silny wzrost w ciągu ostatnich lat, kiedy wycieki stają się bardziej znane opinii publicznej i szkodzą reputacji firm. W związku z tym, firmy zainteresowały się projektowaniem bezpiecznego oprogramowania i budowaniem zaufania wśród użytkowników, co daje im przewagę konkurencyjną na rynku.

Wreszcie, firmy muszą szanować wymiar ludzki w kontekście ochrony ich know-how i danych krytycznych. Są to użytkownicy i podmioty działające w firmie, obsługujący maszyny i technologie, wykonujący zadania i nadzorujący procesy. Podczas gdy zarówno technologia, jak i procesy cechują się bardzo wysoką niezawodnością, pracownicy mają tendencję do popełniania błędów, ponieważ podlegają "ograniczonej

racjonalności" (Simon 1990). W rzeczywistości, około 88% przypadków naruszenia danych lub utraty informacji można przypisać błędom ludzkim, co czyni ten wymiar najważniejszym wymiarem w celu zapewnienia bezpieczeństwa danych w firmie. (Tessian 2021)

W skrócie, koncepcja ograniczonej racjonalności odrzuca założenie, że ludzkie myślenie, zachowanie i działanie jest kierowane przez pełną racjonalność, ponieważ wymagałoby to nieograniczonych zdolności poznawczych do natychmiastowego przetwarzania każdej dostępnej informacji i podejmowania w pełni świadomych decyzji. Zamiast tego zakłada się, że ludzie maksymalizują swoją indywidualną użyteczność, czyli wybierają działanie, które najbardziej zaspokaja ich własną, odczuwaną potrzebę (tzw. "Satisficing"). Wreszcie, osoba może również dojść do wniosku, że brakuje jej informacji do podjęcia decyzji, ale poszukiwanie tych informacji pochłonęłoby znaczną ilość czasu i energii. W związku z tym osoba decyduje się na podjęcie działania z niepełną informacją, ponieważ koszty alternatywne (czas i energia) przewyższają użyteczność posiadania tej konkretnej informacji..

Wśród tych działań, ustawianie łatwych haseł (lub zapisywanie ich na karteczkach post-it), opóźnianie aktualizacji zabezpieczeń, przechowywanie poufnych informacji w szafkach, używanie pendrive'a znalezionego w windzie, to tylko niektóre z nierozważnych konsekwencji. Brak pełnej informacji i postrzegane wysokie koszty alternatywne w chwilach pośpiechu i presji są coraz częściej wykorzystywane przez ataki socjotechniczne, w których intruz tworzy scenariusz za pośrednictwem poczty lub telefonu, który wywołuje pilną potrzebę podjęcia działania w nadziei, że pracownik pominie protokoły bezpieczeństwa, dobrowolnie udostępniając krytyczne informacje (np. hasła, informacje finansowe itp.).

Niestety, przestrzeganie zasad właściwego postępowania w codziennym życiu zawodowym wymaga dodatkowej energii - która często jest zasobem deficytowym w produktywnym lub gorączkowym środowisku pracy. Na tle utartych schematów pracy zmiana postaw, przekonań i wreszcie zachowań stanowi duże wyzwanie zarówno dla firmy, jak i dla jej pracowników. Jak dotąd, nauczanie, szkolenie i uwrażliwianie pracowników w celu podniesienia świadomości na ciągłe zagrożenie dla najcenniejszych aktywów firmy - jej know-how i danych - jest ważniejsze niż kiedykolwiek wcześniej. A wraz z coraz mniejszymi trudnościami w przeprowadzeniu jakiegokolwiek ataku, coraz więcej MŚP musi zmierzyć się z nową rzeczywistością: już są, lub najprawdopodobniej będą, przedmiotem ataków ukierunkowanych. Co zatem można zrobić?

# 3 Strategia TeBeISi

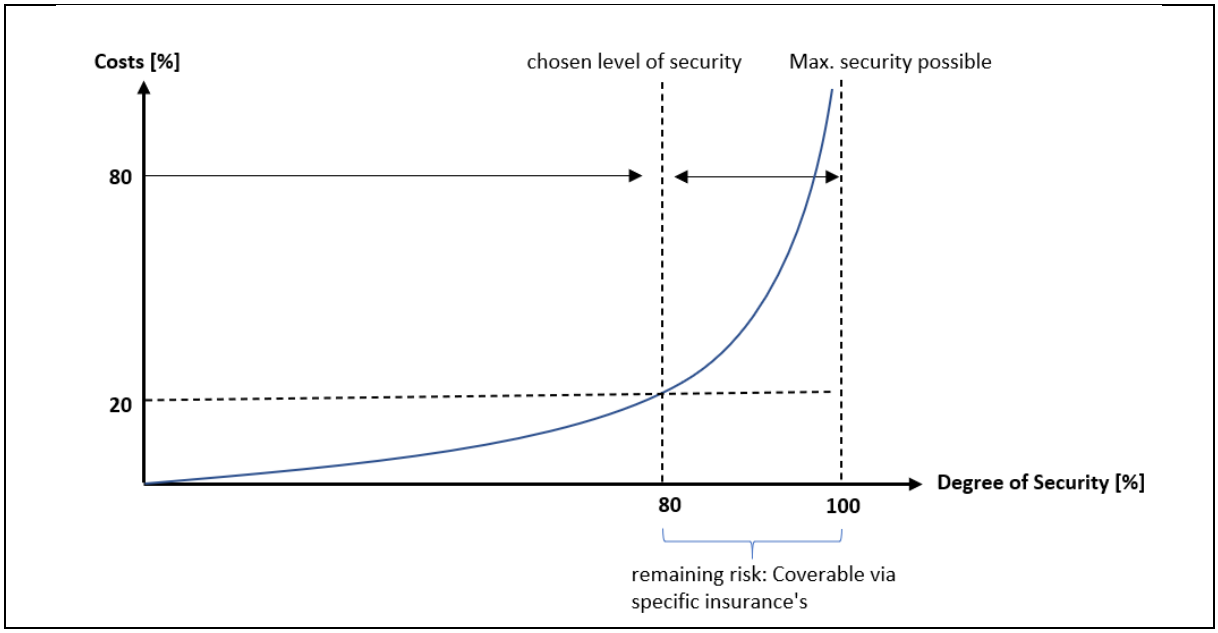
W ramach projektu TeBeISi przeanalizowano sytuację bezpieczeństwa informacji, również pod kątem implementacji GDPR, na poziomie firm w partnerskich krajach członkowskich. Po dokonaniu przeglądu obecnie istniejących profili zawodowych, formalnych kwalifikacji i certyfikatów przeprowadzono porównanie obecnie istniejących, możliwych do przekazania kompetencji z wymaganiami wygenerowanymi na podstawie analizy ilościowej i jakościowej.

## 3.1 Łączenie szkolnictwa wyższego ze szkoleniem zawodowym

Po przeanalizowaniu wszystkich informacji zebranych za pomocą badań ilościowych i jakościowych, partnerstwo doszło do wniosku, że bezpieczeństwo informacji powinno stanowić połączenie szkolenia zawodowego i kształcenia wyższego. Istnieją trzy powody, które wpłynęły na ten koncept:

1. Działania operacyjne: Większość zadań, które muszą być wykonywane w MŚP ma raczej rutynowy charakter. Stopień transferu wiedzy i rekontekstualizacji pozostaje niski, ponieważ technologia i procesy pozostają na standardowym poziomie, a firmy korzystają ze standardowego oprogramowania EDP i kanałów komunikacji. Większość MŚP może osiągnąć znaczący wzrost poziomu bezpieczeństwa poprzez trzymanie się zasady 20:80 (lub podobnej) - osiągają 80% bezpieczeństwa poprzez wykonanie 20% pracy niezbędnej do osiągnięcia 100%. Oczywiście, nie jest to możliwe biorąc pod uwagę ochronę danych, która jest obowiązkowa z mocy prawa i dla której firmy są zobowiązane do spełnienia wymagań GDPR. Konsekwencje tego stwierdzenia są wielorakie: firmy muszą wziąć pod uwagę, czy chcą sięgnąć po konkretną certyfikację (ze względu na charakter ich produktu, wymagania rynku itp.), czy posiadają zasoby, które wymagają więcej niż rutynowych środków ochronnych itp. Tak więc, MŚP często znajdują się w sytuacji, w której strukturalne przestrzeganie podstawowych środków bezpieczeństwa zapewnia znaczny wzrost ogólnego poziomu bezpieczeństwa i znaczne zmniejszenie narażenia na ryzyko w opłacalnym kompromisie.
2. Obowiązki prawne: Pomimo możliwości wykonywania zrutynizowanych zadań w ustrukturyzowanym środowisku pracy, niektóre aspekty bezpieczeństwa informacji dotykają również aspektów prawnych, w szczególności dotyczących wdrożenia prawidłowego przetwarzania danych zgodnie z GDPR. Ze względu na złożoność postępowania z przepisami krajowymi, od odpowiedzialnego personelu wymaga się posiadania kompetencji w zakresie postępowania z przepisami i ich prawidłowej implementacji. Odpowiedzialność ta wiąże się z wysokim stopniem zdolności do rekontekstualizacji i przekazywania abstrakcyjnej wiedzy w środowisku pracy. Podczas gdy stopień złożoności pozostaje do ogarnięcia w odniesieniu do technicznego aspektu

bezpieczeństwa informacji opisanego w punkcie (1), aspekt prawny wymaga starannego szkolenia i wykonania w celu zapewnienia zgodności z odpowiednimi przepisami.




*Wykres 12: Zależność między kosztami a bezpieczeństwem inwestycji w bezpieczeństwo informacji*

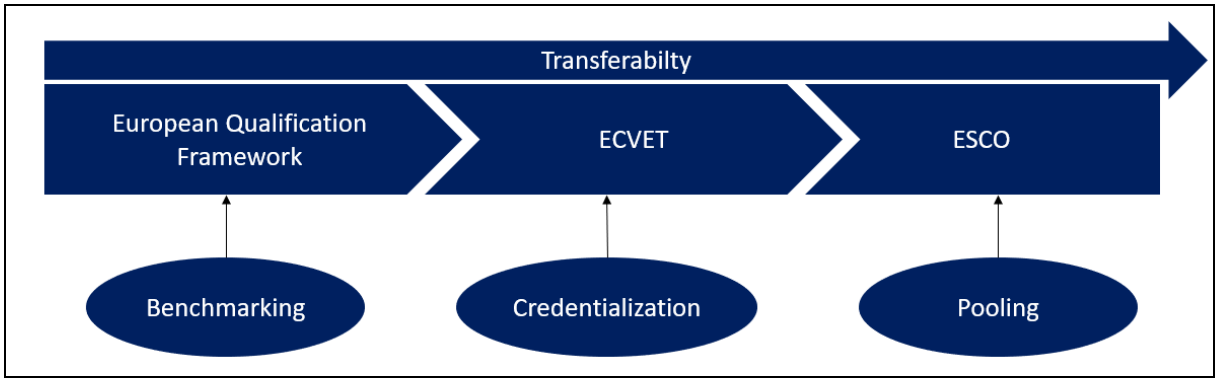
3. Praca osób odpowiedzialnych za bezpieczeństwo informacji wymaga różnorodnych umiejętności społecznych. Jak opisano w punkcie 2.3, największym zagrożeniem dla bezpieczeństwa firmy są jej pracownicy. Zmiana postawy współpracowników, wpływanie na ich sposób pracy i tworzenie kultury bezpieczeństwa informacji w firmie stanowi, prawdopodobnie, największe wyzwanie przy wdrażaniu systemu bezpieczeństwa informacji. Od osoby odpowiedzialnej wymaga się aktywizacji, współpracy, przewodnictwa, mentoringu i pogodzenia pracowników, menedżerów i bezpieczeństwa informacji. Nie jest zaskoczeniem, że firmy doceniają profesjonalistów z doświadczeniem w pracy - i cenią praktyczne doświadczenie wyżej niż jakiekolwiek formalne kwalifikacje (por. badanie "Edukacja w zakresie bezpieczeństwa informacji dla MŚP"). Otrzymanie praktycznego wykształcenia uczy pułapek w codziennej współpracy ze współpracownikami oraz umiejętności produktywnego współdziałania z interesariuszami w firmie.

Edukacja w zakresie bezpieczeństwa informacji, jeśli istnieje, skupia się obecnie w dużym stopniu na nauczaniu i szkoleniu kompetencji technicznych, czy to w dziedzinie informatyki, czy prawa. Zdobywanie praktycznego doświadczenia, a zwłaszcza efektywnych strategii komunikacyjnych, rzadko znajduje miejsce w programach nauczania. TeBeISi proponuje zatem połączenie tego, co najlepsze z obu światów, i zapewnienie edukacji za pomocą kształcenia i szkolenia zawodowego oraz szkolnictwa wyższego.

## 3.2 Wykorzystanie instrumentów europejskich

Połączenie kształcenia i szkolenia zawodowego ze szkolnictwem wyższym zostało określone przez Komisję Europejską jako możliwe do zrealizowania w ramach Europejskich Ram Kwalifikacji (EQF). Ponadto, w celu zapewnienia przejrzystości i porównywalności w kształceniu i szkoleniu zawodowym, należy wdrożyć europejski system transferu osiągnięć w kształceniu i szkoleniu zawodowym (ECVET). Wreszcie, odnosząc się do europejskich ram umiejętności/kompetencji, kwalifikacji i zawodów (ESCO), pojedyncze kompetencje mogą być sformułowane w sposób umożliwiający ich ponowne wykorzystanie i rozpoznawalność w różnych kontekstach zawodowych.

Wykorzystanie instrumentów europejskich odróżnia przejrzysty proces certyfikacji od już istniejącego, zdezorganizowanego rynku certyfikatów wydawanych przez prywatnych dostawców. Należy powtórzyć, że istnieje wiele różnych certyfikatów, również w domenie MŚP, jednakże pozostaje niejasne, w jakim stopniu stosowane są wspólne standardy jakości i zapewnienia jakości, co skutkuje brakiem przejrzystości i możliwości przenoszenia w różnych krajach. Zaległości w zakresie ogólnoeuropejskich systemów akredytacji, zapewnienia jakości i standardów kompetencji pozwalają na szerokie i przejrzyste rozpowszechnianie certyfikatów w ramach systemów edukacyjnych i zinstytucjonalizowanych krajobrazów certyfikacji.




**Wykres 13: Instrumenty przejrzystości w kształceniu i szkoleniu zawodowym w UE**

Krótko mówiąc, instrumenty te wspierają upowszechnianie kompetencji i kwalifikacji w całej UE. EQF jako system odniesienia kategoryzuje kwalifikacje zgodnie z ich podstawowymi umiejętnościami, kompetencjami i autonomią oraz zapewnia możliwość dopasowania każdej kwalifikacji z różnych systemów edukacyjnych do jednego schematu odniesienia, co sprawia, że różne kwalifikacje są porównywalne w różnych kontekstach edukacyjnych. Z kolei ECVET zapewnia podstawę do łączenia efektów uczenia się w punkty edukacyjne, dając wgląd w zakres i głębokość uczenia się stojącego za daną kwalifikacją. Ponadto wspiera on zapewnianie jakości, stwarza możliwości kształcenia ustawicznego w kontekstach specyficznych dla danego regionu oraz wspiera uznawanie kwalifikacji zawodowych w ramach różnych systemowych lub krajowych ścieżek edukacyjnych. Wreszcie, ESCO stanowi ujednolicającą bazę danych, która łączy istniejące kwalifikacje i kompetencje z całej UE. Powracając do tej bazy danych podczas tworzenia nowych programów nauczania, można zapewnić, że kompetencje są zrozumiałe w różnych kontekstach nauczania.

### 3.2.1 Europejskie Ramy Kwalifikacji

Europejskie Ramy Kwalifikacji określają systematyzację formalnych kwalifikacji w systemach edukacyjnych w Unii Europejskiej. Celem tych ram jest uczynienie kwalifikacji porównywalnymi pomiędzy krajami, a w konsekwencji zwiększenie zrozumienia wartości kwalifikacji za granicą. Ponieważ systemy edukacyjne w państwach członkowskich UE znacznie się różnią, EQF mogą być stosowane jako punkt odniesienia w celu zapewnienia równoważności nauczanych kompetencji. W kontekście TeBelSi poziom 5 EQF został uznany za zapewniający cenne możliwości dla firm i osób uczących się.

| Efekty uczenia się odnoszące się do poziomu 5 są następujące | | |
|---|---|---|
| Wiedza | Umiejętności | Kompetencje |
| wszechstronna, specjalistyczna, rzeczowa i teoretyczna wiedza w - dziedzinie pracy lub nauki oraz świadomość granic tej wiedzy | wszechstronny zakres umiejętności poznawczych i praktycznych wymaganych do opracowania twórczych rozwiązań abstrakcyjnych problemów | zarządzanie i nadzór w kontekście pracy lub nauki działania, w których występują nieprzewidywalne zmiany, przegląd i rozwój wydajności własnej i innych |

**Tabela 6: Poziom 5 EQF - efekty uczenia się - wiedza - umiejętności - kompetencje**

Źródło: Komisja Europejska (2008)

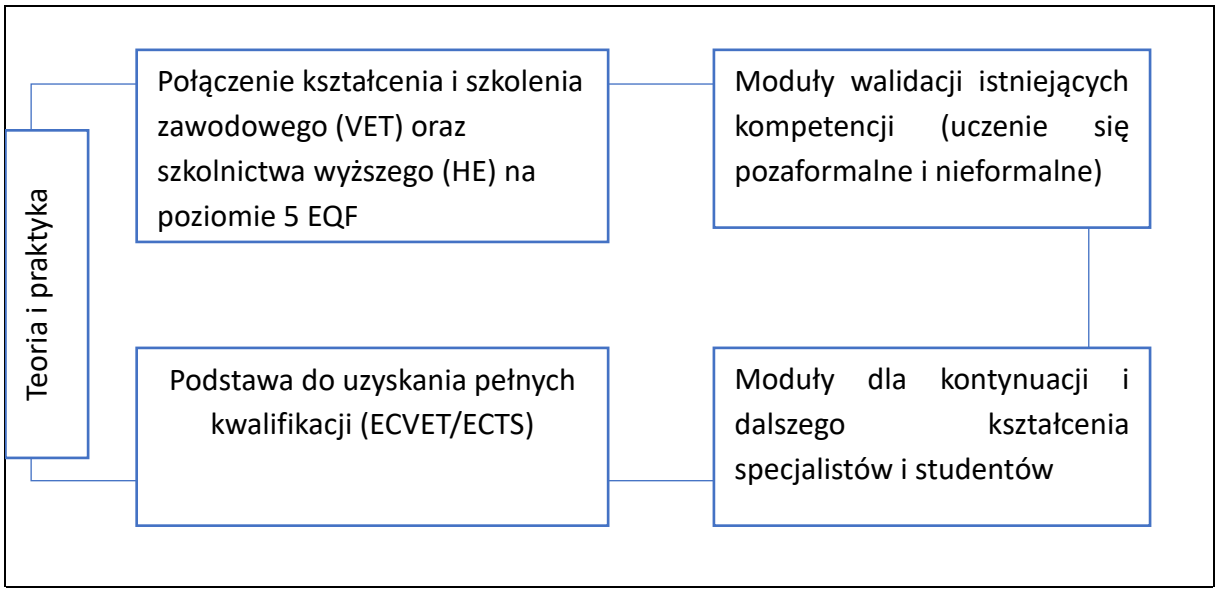
Biorąc pod uwagę kluczowe założenie projektu, że większość dostępnego personelu prawdopodobnie posiada zbyt wysokie kwalifikacje w stosunku do potrzeb MŚP (co jest również odzwierciedlone w istniejących profilach zawodowych w ESCO), należy znaleźć odpowiednie środki w celu dostosowania nieodłącznej złożoności zadań związanych z bezpieczeństwem informacji (tj. know-how w zakresie IT i wiedzy prawnej) oraz minimalnych wymagań MŚP w celu zwrócenia się do nowych osób uczących się w tej dziedzinie. Można stwierdzić, że ze względu na charakter niektórych zadań, szczególnie tych związanych z niestandardowymi działaniami lub wymagających kompetencji prawnych, niektóre elementy edukacji w zakresie bezpieczeństwa informacji dla MŚP muszą być zakorzenione w szkolnictwie wyższym, co umożliwia uczącym się działanie w mniej ustrukturyzowanym i bardziej niezależnym środowisku. W szczególności, do tej kategorii należą kompetencje związane z prawem, tj. głównie GDPR.

Zastosowanie EQF 5 zapewnia kilka korzyści, które można wykorzystać. Po pierwsze, stanowi podstawę dla wielu pracowników posiadających kwalifikacje EQF 4, aby znaleźć wejście do kształcenia ustawicznego. W konsekwencji, częściowa walidacja na tym poziomie może być ułatwiona poprzez uznanie wcześniejszego doświadczenia zawodowego, uczenia się pozaformalnego i nieformalnego. Połączenie z EQF 6 wypełnia lukę i daje możliwość adaptacji instytucjom szkolnictwa wyższego, które chcą zapewnić swoim studentom albo pełne kwalifikacje w kontekście bezpieczeństwa informacji, albo dodatkowe kwalifikacje.

### 3.2.2 ECVET

Z perspektywy funkcjonalnej, zorientowana na efekty uczenia się operacjonalizacja kompetencji oznacza zmianę perspektywy z "Czego chcę nauczyć?" na "Czego powinni nauczyć się uczący się?". Wynik procesu uczenia się stanowi punkt ciężkości procesu uczenia się i daje uczącym się jaśniejszy obraz ich własnych postępów w nauce. Dzięki zastosowaniu przejrzystego systemu punktów można osiągnąć kilka pozytywnych efektów zewnętrznych, które odróżniają modułową ścieżkę edukacyjną od istniejących systemów certyfikacji.

Rozproszenie profilu kompetencji TeBeISi oficera bezpieczeństwa informacji i ochrony danych w MŚP na podzielone na moduły obszary uczenia się (por. "Curriculum") ułatwia modularyzację obszarów kształcenia i stosowanie systemów transferu punktów, takich jak ECTS lub ECVET. ECVET. Modularyzacja (mikrokredytowanie) zapewnia kilka korzyści, zilustrowanych na Rysunku 11, prowadzących do zwiększenia przejrzystości, mobilności i wiarygodności kwalifikacji cząstkowych. Moduły mogą być wykorzystywane zarówno do celów szkoleniowych i edukacyjnych dla pracowników lub studentów, jak i jako środek częściowej walidacji poprzez udostępnienie procesu certyfikacji osobom wchodzącym później na rynek pracy w obszarze bezpieczeństwa informacji..




**Wykres 14: Zalety kwalifikacji modułowych**

Biorąc pod uwagę istniejące systemy walidacji, wiarygodność odgrywa kluczową rolę w akceptacji procesu certyfikacji przez pracodawców i organizatorów szkoleń. W tym przypadku, oprócz istniejących standardów zapewniania jakości (np. EQAVET), należy wziąć pod uwagę konkretne szczegóły dotyczące oceny kompetencji w celu zapewnienia jak największej wiarygodności procedury walidacji.

### 3.3 Pomiar efektów uczenia się

Pomiar efektów uczenia się pozostaje kwestią dyskusyjną, tymczasem istnieją najlepsze praktyki w tym zakresie, jak np. VALIKOM lub MySkills z Niemiec, ale szerokie przyjęcie tych metod nie może stanowić odpowiedzi na wszystkie zastrzeżenia zgłaszane przez firmy i praktyków zajmujących się oceną. W szczególności, wśród dostawców usług edukacyjnych pozostaje pytanie, czy krótkoterminowe badania są odpowiednią formą zastąpienia całego programu nauczania. Aby zwiększyć ważność procesu pomiaru, należy wziąć pod uwagę kilka kwestii:

1. Przejrzyste procesy. Kluczowe znaczenie ma przejrzystość całego procesu uznawania kwalifikacji. Rozmowa wstępna, przydzielenie specjalnego mentora i właściwe przygotowanie do oceny muszą być częścią całościowo przemyślanego, zaplanowanego krok po kroku procesu uznawania kwalifikacji.

2. Samo rozpoznanie musi uwzględniać kilka środków w celu zapewnienia jak największej ważności oceny. Ogólnie rzecz biorąc, konkretne formy oceny są bardziej odpowiednie do oceny konkretnych form kompetencji. Podczas gdy testy pisemne, czy to z otwartymi odpowiedziami, czy wielokrotnego wyboru, są odpowiednie do oceny wiedzy, odgrywanie ról, ćwiczenia typu post box lub gry prezentacyjne są nastawione na testowanie kompetencji komunikacyjnych i społecznych, takich jak rozmowa, retoryka, argumentacja, empatia, asertywność, perswazyjność, wrażliwość (obserwacja zachowań). Są one również przydatne do oceny gotowości operacyjnej, orientacji na cel, tolerancji na frustrację, wytrwałości, umiejętności rozwiązywania problemów, umiejętności analitycznych, umiejętności podejmowania decyzji itp. Metody biograficzne, takie jak rozmowa oparta na kryteriach, przegląd ustrukturyzowanego portfolio i dyskusje techniczne, pozwalają kandydatom uzyskać wszechstronny wgląd we własne osiągnięcia i nauczyć się oceniać siebie i swoje cechy. Wreszcie, obserwacje na miejscu i w symulowanym środowisku pozwalają na zaobserwowanie reakcji w rzeczywistych scenariuszach, samokontroli i podejścia do spontanicznych wydarzeń. Dlatego też, poprzez połączenie metod oceny, można dokonać triangulacji kompetencji cząstkowych i wiarygodnie określić dyspozycję.

3. Aby móc przeprowadzać obiektywne oceny, osoby oceniające muszą zostać przeszkolone w zakresie sprawiedliwego, przejrzystego i obiektywnego postępowania z różnymi metodami oceny, różnymi błędami w ocenie i różnymi kandydatami. Osoby oceniające muszą być świadome różnych ścieżek uczenia się i różnych celów kandydatów oraz rozumieć cały proces walidacji i uznawania.

4. Samoocena jako krok w kierunku oceny jest zalecana, ale samoocena jako źródło oceny nie jest zalecana. Samoocena w formie oceny technicznej ("kandydat X wie..." "tak", "nie") lub w formie testów osobowościowych może

przynieść orientacyjne wyniki, jednak należy zakwestionować wiarygodność i obiektywność tych wyników.

Dlatego też należy wprowadzić szczegółową strukturę i system zapewnienia jakości, aby zagwarantować rzetelną, obiektywną i przejrzystą ocenę oraz wzbudzić zaufanie wśród instytucji edukacyjnych i pracodawców.

# 4 Perspektywy i zalecenia

Niedobór wykwalifikowanej siły roboczej w sektorze bezpieczeństwa informacji utrzymuje się w całej UE. Kompetencje techniczne wśród specjalistów stają się coraz mniej istotne w porównaniu z kompetencjami społecznymi i osobistymi. Inwestycje w kapitał ludzki, tj. odpowiednie kształcenie pracowników, są coraz bardziej opłacalne w obliczu rozproszonych sytuacji ryzyka, takich jak wielowymiarowe wektory ataków w przestrzeni fizycznej i cyfrowej. Bezpieczeństwo firmowego know-how i gotowość do świadczenia usług wewnętrznych i zewnętrznych jest coraz częściej łączona z nowymi możliwościami wykorzystania. Jednak w ostatecznym rozrachunku, wszystkie nowe technologie i wytyczne wprowadzone w celu ograniczenia ryzyka wrogich naruszeń są niweczone, jeśli pracownicy firmy nie akceptują i nie stosują aktywnie kultury bezpieczeństwa firmy.

Świadomość ryzyka i przestrzeganie zasad są punktem wyjścia do zmniejszenia ryzyka wszelkiego rodzaju ataków. Aby to osiągnąć, należy zmienić wartości, przekonania i ostatecznie zachowania ludzi w firmie, w celu ustanowienia kultury ryzyka. Przesunięcie uwagi z technicznego aspektu problemu na czynnik ludzki sprawia, że edukacja i szkolenia muszą być przemyślane również pod tym kątem.

Nasilenie działalności przestępczej w odniesieniu do informacji prywatnych i poufnych w erze cyfrowej stawia pod znakiem zapytania nie tylko kształtowanie zdolności w środowiskach zawodowych i sferze pracy, ale także sferę prywatną obywateli europejskich. Chociaż ataki na korporacje powodują znaczne szkody dla gospodarki europejskiej, ważne jest, aby podkreślić konsekwencje wzmożonej działalności przestępczej w kontekście informacji poufnych: jej celem są osoby fizyczne, a nie firmy. W związku z tym budowanie zdolności wśród obywateli poprzez kształcenie podstawowe i szkolenia przyniosłoby pozytywne efekty zewnętrzne dla przedsiębiorstw i społeczeństwa. Budowanie potencjału nie powinno być zatem traktowane wyłącznie jako interes poszczególnych firm - ale całego społeczeństwa. Wprowadzenie w szkołach, instytucjach kształcenia zawodowego i wyższego szkoleń z zakresu świadomości, postępowania z informacjami wrażliwymi i zrozumienia własnej ekspozycji na wrogie ataki. W 2018 roku Rada Unii Europejskiej na nowo zdefiniowała "Kompetencje Obywatelskie" jako

“umiejętność działania jako odpowiedzialny obywatel i pełnego uczestnictwa w życiu obywatelskim i społecznym, w oparciu o zrozumienie pojęć i struktur społecznych, gospodarczych, prawnych i politycznych, jak również globalnych zmian i zrównoważonego rozwoju".

Uczestnictwo dojrzałych obywateli w dzisiejszym i przyszłym świecie jest ściśle związane z umiejętnością oddzielenia intencjonalnych szkód od codziennych incydentów. Wykrywanie dezinformacji, manipulacji, dbałość o prywatność i bezpieczeństwo cyfrowe są kwestią odporności obywatelskiej - i nie powinny być ograniczane do kwestii opłacalnych wydatków w prywatnych korporacjach. W ostatecznym rozrachunku leży to w najlepszym interesie Unii Europejskiej i jej państw

członkowskich - a zatem jest to pytanie, na które powinny odpowiedzieć ministerstwa edukacji, a nie tylko wydziały informatyki.

W związku z tym zaleca się następujące środki w celu budowania potencjału wśród obywateli europejskich:

1. Założenie europejskiej organizacji na rzecz ochrony prywatnych informacji i danych. Wdrożenie punktu kontaktowego, areny dla wspólnych przekonań w krytycznej sprawie oraz platformy wymiany wiedzy i kampanii na rzecz interesów stanowi kluczowy element kierowania interesami obywatelskimi, publicznymi i korporacyjnymi. Główny cel, promowanie pozostałych zaleceń wymienionych poniżej, leży u podstaw wspólnej organizacji.

2. Wprowadzenie "bezpieczeństwa informacji" do programów praktyk zawodowych ceteris paribus "bezpieczeństwo i higiena pracy". Zmiana ludzkich wartości, przekonań i działań jest niewykonalna z ekonomicznego punktu widzenia. Dlatego ważne jest, aby angażować się w proces formacji i uczyć jednostki znaczenia świadomości wobec rozproszonych scenariuszy zagrożeń, w tym ukierunkowanej manipulacji i dezinformacji w erze cyfrowej.

3. Wprowadzenie mikrokredytów i częściowych systemów certyfikacji w zakresie bezpieczeństwa informacji dla odbiorców prywatnych i zawodowych. Obecna sytuacja w kształceniu ustawicznym i szkoleniach pozostaje nieprzejrzysta i brakuje jej ustrukturyzowanej wizji na przyszłość. Obok istniejących systemów certyfikacji, pełnoprawne programy nauczania, zbudowane z pojedynczych i możliwych do szkolenia modułów, zapewniają różnorodne możliwości wykorzystania i powielania. Mogą one być zintegrowane ze szkoleniem VET (EQF 4) i szkolnictwem wyższym (EQF 6-7) w zależności od przedmiotu, połączone w jedną ścieżkę szkoleniową, która łączy szkolenie w miejscu pracy i szkolnictwo wyższe (EQF 5) lub oferowane pracownikom jako możliwości kształcenia ustawicznego. Modułowość pozwala na ukierunkowane, mniej złożone i wymagające mniejszej ilości zasobów wzorce szkoleniowe, przynosząc niższe koszty i większe możliwości dla MŚP.

4. Zwiększenie wykorzystania europejskich narzędzi przejrzystości w celu wspierania elastyczności na rynku pracy i przyciągania nowych talentów.

# 5 Bibliografia

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.

# Raport Strategiczny

**Podziękowania dla współautorów z:**

BF/M-Bayreuth

Mykolas Romeris University

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Finansowane przez program Erasmus+ Unii Europejskiej

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