Strateginė ataskaita

Europos piliečių ir darbuotojų informacijos saugumo gebėjimų ugdymas

Bendrai finansuojama pagal Europos Sąjungos programą „Erasmus+“

TeBeISi

Bendrai finansuojama pagal
Europos Sąjungos programą
„Erasmus+“

Šis dokumentas parengtas įgyvendinant ERASMUS+ projektą "Dalinis sertifikavimas informacinės saugos profesinėje srityje – TeBeiSi", projekto ID: 2018-1-EN02-KA202-005218

Turinys

Paveikslų sąrašas

Lentelių sąrašas

1 Įvadas

2018 m. įsigaliojęs BDAR paskatino vartotojus, įmones ir visą visuomenę keisti asmens duomenų suvokimą ir vertę. Įvedus privalomus ir sankcionuotus standartus ir įstatymus, susijusius su asmens duomenų rinkimu, saugojimu ir tvarkymu, buvo tikimasi sustiprinti vartotojų teises, nustatyti duomenų naudojimo ir rinkimo ribas ir, galiausiai, padidinti bei užtikrinti teisę į privatumą ir asmens laisvę skaitmeniniame amžiuje.

Nuo tada, po daugybės viešų diskusijų apie prasmę ir beprasmybę, apie tai, ką daryti ir ko nedaryti, pirmosios kliūtys buvo įveiktos ir didelio susidomėjimo banga nuslūgo. Duomenų apsauga tapo neatsiejama kiekvienos organizacijos darbo dalimi. Įmonės privalo ne tik paskirstyti atsakomybę už tinkamą duomenų apsaugos vykdymą įmonėje, bet ir kiekvienas darbuotojas turi žinoti apie galimus duomenų apsaugos pažeidimus savo veiklos praktikoje ir laikytis nustatytų procedūrų. Galiausiai, patys darbuotojai, pradėdami darbo santykius, yra suinteresuoti savo duomenų apsauga, kuri priskiriama darbuotojų duomenų apsaugai. Darbuotojams, kurie yra silpniausia įmonės informacijos saugumo strategijos grandis, turi būti skiriamas ypatingas dėmesys. Didelės korporacijos pradėjo sėkmingai įgyvendinti įvairias švietimo programas, skirtas darbuotojų sąmoningumui ugdyti, tuo tarpu MVĮ prioritetai, susiję su informacijos saugumo ir duomenų apsaugos gebėjimais, išlieka nedideli.

Informacijos saugumas, kuris, priešingai nei duomenų apsauga, nėra privalomas ar teisiškai įpareigojantis organizacijų veiklą. Tačiau ji susijusi su daugeliu duomenų tvarkymo, rinkimo ir saugojimo aspektų, todėl atsakingiems darbuotojams reikalingas platus išsilavinimas ir mokymas. Švietimas ir mokymas, ypač susijęs su įmonės *know-how* apsauga, išlieka pagrindiniu ES MVĮ saugumo didinimo aspektu. Šioje ataskaitoje siekiame išdėstyti ES informacijos saugumo ir duomenų apsaugos kompetencijų ugdymo ir mokymo prielaidas bei perspektyvas ir pateikti rekomendacijas dėl tolesnės plėtros, ypač MVĮ aplinkoje.

2 Duomenų apsauga šalyse partnerėse

2.1 Lenkija

Institucijos pavadinimas	Trumpas aprašymas	Tinklapis
Asmens duomenų apsaugos tarnyba (UODO)	UODO yra pagrindinė valstybės institucija, atsakinga už asmens duomenų apsaugą. Vykdydamas užduotis, numatytas CK 6.2 str. 57 BDAR, ši institucija: stebi ir užtikrina BDAR taikymą; skleidžia žinias apie su duomenų tvarkymu susijusią riziką, taisykles, apsaugos priemones ir teises visuomenėje, taip pat šių reiškinių supratimą; konsultuoja nacionalinį parlamentą, vyriausybę ir kitas institucijas bei įstaigas duomenų apsaugos klausimais, nagrinėja duomenų subjekto arba subjekto, organizacijos ar asociacijos pateiktus skundus; veda bylas dėl BDAR taikymo, priima sprendimus ir, jei tai proporcinga, - nustato administracinių baudų už BDAR pažeidimus dydį ir jas skiria.	https://uodo.gov.pl/
GovTech centras	„GovTech“ centras perėmė dalį pareigų iš Skaitmeninimo ministerijos, kuri buvo likviduota 2020 m. rudenį. Tiesioginiai „GovTech“ paslaugų gavėjai yra plačiai apibrėžtos vietos ir centrinės administracijos, taip pat kitos viešąsias užduotis atliekančios įstaigos, pavyzdžiui, ligoninės, mokyklos ar transporto įmonės. GovTech paslaugų gavėjai yra ne tik viešasis sektorius, bet ir įmonės.	https://www.gov.pl/web/govtech
"Panoptykon" fondas	Fondas „Panoptykon“ vykdo priežiūros funkcijas. Jame nagrinėjami galiojantys teisės aktai, teisėkūros tendencijos, valdžios institucijų ir privačių bendrovių veiksmai. Fondas stebi žiniasklaidos ir piliečių pranešimus, analizuoja surinktą informaciją, diagnozuoja problemas ir reaguoja. Pateikia savo nuomonę apie pasiūlymus dėl naujų teisės aktų, prieštarauja galiojantiems įstatymams ir teikia savo pasiūlymus dėl pakeitimų. Fondas atkreipia dėmesį į piktnaudžiavimą ir aplaidumą.	www.panoptykon.org
Nacionalinis mokslinių tyrimų institutas (NASK)	NASK – valstybinis mokslinių tyrimų institutas, prižiūrimas Ministro Pirmininko kanceliarijos. Jo misija – ieškoti ir įgyvendinti sprendimus, padedančius plėtoti IKT tinklus Lenkijoje, didinti jų efektyvumą ir saugumą. Institutas vykdo mokslinius tyrimus, plėtros darbus ir operatyvinę veiklą Lenkijos civilinės kibernetinės erdvės saugumo labui. Kitas svarbus NASK veiklos elementas yra vartotojų švietimas ir informacinės visuomenės koncepcijos propagavimas, visų pirma, siekiant apsaugoti vaikus ir jaunimą nuo grėsmių, susijusių su naujų technologijų naudojimu.	www.nask.pl

Asmens duomenų apsaugos bendrovių sąjunga ZFODO	Asmens duomenų apsaugos įmonių asociacijoje susivienijusios įmonės turi ilgametę verslo konsultacijų asmens duomenų apsaugos srityje patirtį. Jie teikia aukščiausio lygio profesionalias paslaugas didžiausioms privataus sektoriaus bendrovėms, taip pat vietos ir centrinės valdžios institucijoms. Asociacija turi patirties įvairiuose sektoriuose ir pramonės šakose, todėl gali pasiūlyti klientams individualius, jų poreikius atitinkančius sprendimus. Asociacija turi daug verslo partnerių - advokatų kontorų, IT ir rinkodaros konsultacijų bendrovių. Tai leidžia jiems visapusiškai konsultuoti savo klientus ne tik duomenų apsaugos, bet ir viso klientų verslo klausimais.	www.zfodo.org.pl
Fondas „Žinios tai saugumas”	Fondas populiarina žinias informacijos saugumo srityje: rengia mokslines konferencijas, padeda spręsti problemas, su kuriomis žmonės susiduria kasdieniame gyvenime tiek privačiame, tiek verslo sektoriuje. Fondas rengia socialines kampanijas, kad padidintų visuomenės informuotumą, siekiant parodyti, kokie pavojai gresia dėl neteisėto asmens duomenų naudojimo.	https://wtb.org.pl/

Lentelė 1: Lenkijos socialiniai partneriai

Tarp dažniausių klaidų, susijusių su RODO (BDAR atitikmuo Lenkijoje) įgyvendinimu Lenkijos įmonėse, ataskaitoje „10 didžiausių klaidų užtikrinant atitiktį BDAR“ ZFODO nurodomos:

- Neteisingas BDAR idėjos supratimas, t. y. jos įgyvendinimas tik "ant popieriaus". Todėl niekas nežino jos procedūrų ir jų nesilaiko. Neįgyvendinus šio reikalavimo, priežiūros institucija gali taikyti sankcijas.
- Nepakankamas informuotumas apie informacijos saugumą. Rizikos analizę atlieka nekvalifikuoti arba per mažai patirties turintys darbuotojai, todėl analizė neatliekama arba atliekama neteisingai. Rezultatas – neidentifikuotos grėsmės, galimybė prarasti duomenis, saugumo trūkumas.
- Netinkama IT sritis, nenustatyta duomenų saugojimo politika arba saugojimo taisyklės neįgyvendintos IKT sistemose. Dėl to gali būti prarasti duomenys arba nesankcionuota prieiga prie duomenų, taip pat negalėjimas pasinaudoti teisėmis, su kuriomis susiję duomenys.

Be to, buvo paminėta, kad netinkamai atliktas poveikio duomenų apsaugai vertinimas, nereglamentuoti subjektų tarpusavio duomenų patikėjimo santykiai, supainiotos duomenų valdytojo ir duomenų tvarkytojo sąvokos, neįgyvendinta įpareigojimo teikti informaciją procedūra, trūksta procedūrų įgyvendinimo koordinatoriaus, trūksta darbuotojų informuotumo, trūksta holistinio požiūrio į įgyvendinimą.

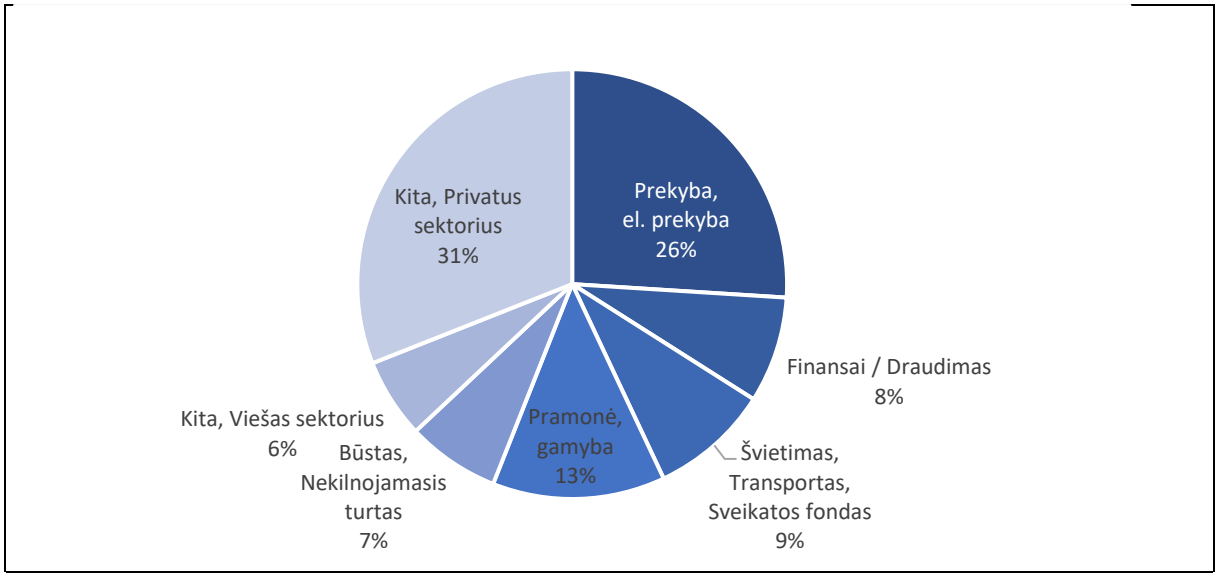
Minėtos sritys yra „pagrindinės nuodėmės“, tačiau yra ir kitų naujų reglamentų įgyvendinimo aspektų, dėl kurių kilo problemų.

Pavyzdžiui, dažniausiai nepakankamai įvertinamas duomenų apsaugos pareigūno vaidmuo, o jo padėtis organizacijoje yra žema. Dažnai duomenų apsaugos pareigūnas yra „ranka parinktas“ asmuo. Duomenų apsaugos pareigūnas dažnai yra įdarbinamas, neturi tinkamos kvalifikacijos ir turi mažai įtakos aukščiausiosios vadovybės priimamiems sprendimams, jo balsas traktuojamas tik kaip patariamasis. Ataskaitą lenkų kalba paskelbė (ZFODO 2020) ZFODO (2020).

Informacija apie tai, kaip BDAR įgyvendinamas praktikoje, ir apie pažeidimų bei incidentų, susijusių su asmens duomenų apsauga Lenkijos įmonėse ir įstaigose, mastą, be kita ko, pateikiama Duomenų apsaugos įmonių asociacijos parengtoje ataskaitoje. (ZFODO, 2020).

Ataskaita apėmė 454 organizacijas, kurias 2019 m. gegužės mėn. – 2020 m. gegužės mėn. aptarnavo su ZFODO susijusios įmonės. Tarp apklaustųjų buvo tiek privataus, tiek viešojo sektoriaus organizacijos ir įmonės. Statistiniai duomenys rodo, kad incidentas (duomenų apsaugos incidentas) vidutiniam duomenų valdytojui statistiškai įvyksta 0,65 karto per metus. To nepakanka, kad būtų galima įgyti reikiamos praktikos, kaip išvengti tokių incidentų arba juos valdyti, o klaida tvarkant net vieną incidentą gali turėti pražūtingų pasekmių įmonei.

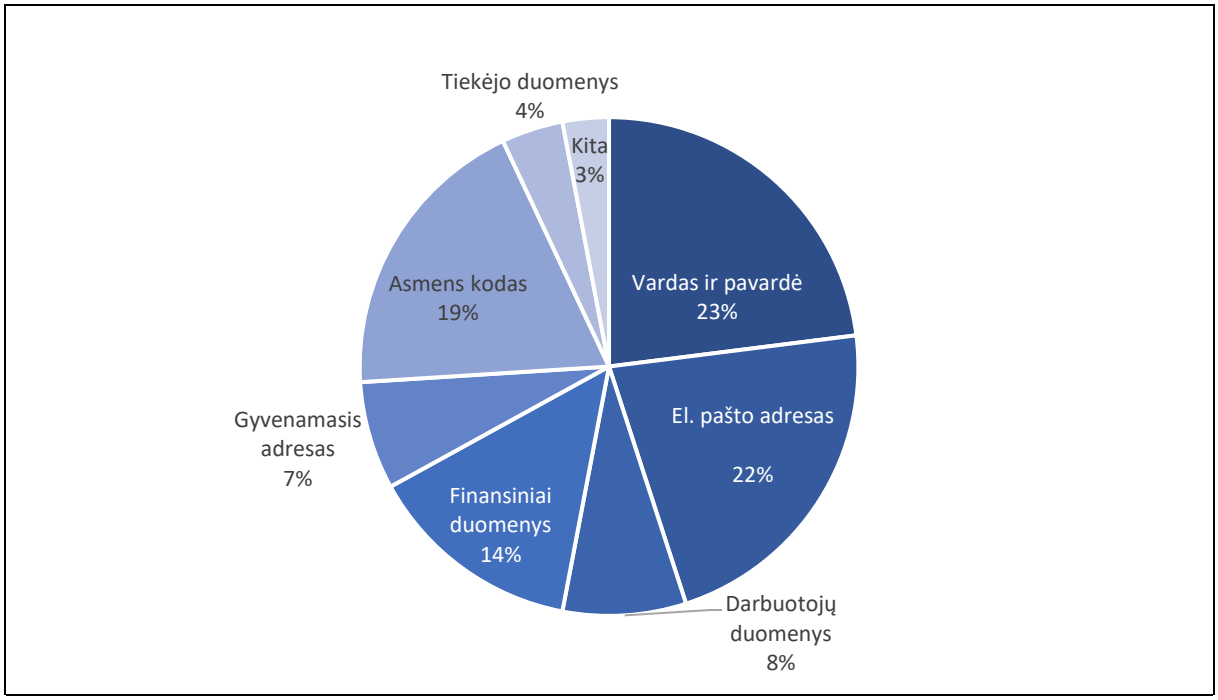
Ataskaitoje nurodoma, kad apie beveik 70 proc. incidentų nebuvo pranešta priežiūros institucijai. Pagal BDAR 33 straipsnio 1 dalį galima nepranešti apie incidentą priežiūros institucijai, jei "mažai tikėtina, kad dėl pažeidimo kils fizinių asmenų teisių ar laisvių pažeidimo pavojus". 70 proc. atvejų asmenys, kuriems šie incidentai turėjo įtakos, nebuvo informuoti. Nepriklausomai nuo to, ar apie incidentą pranešama priežiūros institucijai, pagal BDAR 34 straipsnį "Jei dėl asmens duomenų saugumo pažeidimo gali kilti didelis pavojus, kad bus pažeistos asmenų teisės ar laisvės", būtina informuoti ir pačius nukentėjusius asmenis.



Pav. 1: Pramonės šakos ir (arba) sektoriai, kuriems gresia didžiausia asmens duomenų saugumo pažeidimų rizika
Šaltinis: ZFODO (2021),sudaryta autoriaus.

Asmens duomenų saugumo pažeidimų šaltiniai buvo tiek įmonės (įstaigos) viduje (68 proc.), tiek už jos ribų (20 proc.), tiek iš vadinamojo duomenų tvarkytojo, t. y. subjekto, tvarkančio duomenis duomenų valdytojo vardu (12 proc.). Prie išorinių priskiriami, pavyzdžiui, buvę darbuotojai arba įsilaužėliai, o prie vidinių – organizacijos darbuotojai.

92 proc. atvejų tai buvo netyčiniai atvejai (neteisingai adresuoti el. laiškai, paslėptos kopijos nebuvimas, neteisingo turinio tradicinės korespondencijos siuntimas). Tyčiniai incidentai: nešiojamųjų kompiuterių ar kitų duomenų laikmenų vagystė, sukčiavimas, dalijimasis duomenimis su neįgaliotais asmenimis. Beveik 96 proc. incidentų įvyko dėl asmeninių priežasčių. Tarp jų buvo ir žmogiškojo veiksnio poveikis. Neasmeninės priežastys – tai situacijos, kai pažeidimas įvyko dėl netinkamo technologijų veikimo, nuo žmogaus valios nepriklausančių aplinkybių.



Pav. 2: Dažniausiai pažeidžiamų duomenų kategorijos.
Šaltinis:.(ZFODO 2021), sudaryta autoriaus

Kalbant apie darbuotojų asmens duomenų apsaugą, deja, nepavyko rasti ataskaitos, kurioje būtų išanalizuotas šio klausimo mastas ir dažniausiai pasitaikančios situacijos Lenkijoje. Siekdama palengvinti įdarbinimo procesą ir padėti lengviau orientuotis teisės aktuose, UODO (Asmens duomenų apsaugos tarnyba) išleido leidinį "Asmens duomenų apsauga darbo vietoje. Vadovas darbdaviams“ (Asmens duomenų apsaugos tarnyba, 2018 m.).

2.2 Austrija

Įstaigos pavadinimas	Trumpas aprašymas	Pagrindinis tikslas	Tinklapis
WKO – Austrijos prekybos rūmai / WKO Wirtschafts-kammer	WKO skatina įmones parengti tinkamą saugumo strategiją, apsaugančią nuo galimų grėsmių.	Darbuotojų sąmoningumo didinimas yra svarbus saugumo veiksnys. Įsteigtas atskiras IT saugumo ir duomenų saugumo skyrius. MVĮ remiamos pasitelkiant įvairias iniciatyvas.	https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
Austrijos duomenų apsaugos tarnyba/ Österreichische Datenschutzbehörde (DSB)	Austrijos duomenų apsaugos tarnyba yra nacionalinė Austrijos Respublikos duomenų apsaugos priežiūros institucija.	Austrijos Respublikos teisinės informacijos sistemoje (www.ris.bka.gv.at) pateikiami dabartiniai Austrijos teisės aktai (federaliniai ir valstybiniai), teisės leidiniai (federaliniai ir valstybiniai) ir teismų praktika.	www.dsb.gv.at
BFI Wien Duomenų apsaugos mokymai ir informacinės sistemos (IS)	Duomenų apsaugos ir informacinių sistemų (IS) mokymų teikėjas	BFI, kaip valstybės pripažinta tęstinio mokymo institucija, turi teisę išduoti atestatus ir pateikti neformaliojo mokymo kursų pripažinimo procedūras NKS (Nacionalinės kvalifikacijos sistemos) koordinavimo įstaigai (NKS) arba per jos aptarnavimo tarnybas.	https://www.bfi.wien/edv-und-informationstechnologien/datenschutz-und-informationssicherheit/
KMU platforma	Šis verslo ir technologijų ekspertų tinklas buvo įkurtas siekiant remti Austrijos MVĮ ir padėti įmonėms prisitaikyti prie skaitmeninių pokyčių.	Be daugelio kitų paslaugų, siūlomi seminarai įvairiomis temomis. Šūkis „Bendras pagrindas pakeičia dydį“ aiškiai parodo, kad daugiausia dėmesio skiriama mažų įmonių bendradarbiavimui, o tai savo ruožtu joms pačioms sukuria konkurencinį pranašumą.	https://www.kmu-plattform.eu/
Skaitmeninimo agentūra / Digitalisierungs-agentur	FFG, Mokslinių tyrimų skatinimo agentūroje, buvo įsteigta „Skaitmeninimo agentūra“, skirta dotacijoms Austrijos MVĮ (mažoms ir vidutinėms įmonėms)	Tam, kad Austrijos mažosios ir vidutinės įmonės (MVĮ) galėtų kuo geriau išnaudoti savo skaitmeninimo galimybes, „KMU SKAITMENINĖ Iniciatyva“ teikia numatytą pagalbą. Įmonės gauna subsidijas konsultacijoms, kvalifikacijai, žinių perdavimui ir tolesniam mokymui.	https://www.ffg.at/dia

	skirti, siekiant tikslingai skatinti skaitmeninimą.		
Vienos verslo agentūra / Wirtschafts-agentur Wien	„Wien Digital“ finansavimo programa remia MVĮ įgyvendinant skaitmeninimo priemones.	Vienos verslo agentūra siūlo asmenines konsultacijas ir turi platų MVĮ ir (viešojo) bendradarbiavimo partnerių tinklą. Pradedantiesiems, individualiems verslininkams, vietinėms ir tarptautinėms mažoms ir vidutinėms įmonėms ar korporacijoms teikiama pagalba svarbiais klausimais.	https://wirtschaftsagentur.at/
Verslo ratas	Sertifikuotų duomenų apsaugos pareigūno mokymo kursų teikėjas	Kursų metu įgyta kvalifikacija patvirtinama Austrijos standartų sertifikatu atitinkančiu ISO/IEC 17024 kriterijus, prieš tai gavus teigiamą galutinio egzamino įvertinimą.	https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/
1a Beratung e.U. - Ing. Roland Fürbas	Privatus BDAR ir informacinių sistemų (IS) mokymo kursų tiekėjas	Duomenys ir IT sauga / DSGVO-DSB / Verslo plėtra / Internetinės paslaugos	http://www.1a-beratung.eu
72solutions	Privatus BDAR ir informacinių sistemų (IS) mokymo kursų tiekėjas	BDAR - ekspertai, kurie pataria ir kuria individualius duomenų apsaugos priemonių sprendimus.	https://www.72solutions.eu
TÜV Austria Akademie	Mokymų apie duomenų apsaugą tiekėjas - BDAR ekspertas	Siūloma apie 20 kursų, suskirstytų pagal sektorius.	https://www.tuv-akademie.at/kursprogramm?s=Datenschutz

Lentelė 2: Austrijos socialiniai partneriai

Austrija buvo viena pirmųjų Europos šalių, turinčių reguliuojančią duomenų apsaugos instituciją – Duomenų apsaugos komisiją. Ji buvo įkurta remiantis pirmuoju duomenų apsaugos įstatymu (Federal Law Gazette No. 565/1978). ES duomenų apsaugos direktyva 95/46/EC perkėlė duomenų apsaugos teisinį reguliavimą į naują lygmenį (EUR-LEX 1995). Austrijoje ši direktyva buvo įgyvendinta Duomenų apsaugos įstatymu 2000 (DSG 2000) (Rechtsinformationssystem des Bundes (RIS) 1999). Po 2018 gegužės 25-osios Bendrasis duomenų apsaugos reglamentas (GDPR; DSGVO) ir atnaujintas Duomenų apsaugos įstatymas (DSG) (Federalinė finansų ministerija (BMF)) sudarė asmens duomenų apsaugos teisinio reguliavimo pagrindą (žr. DSB 2019). Remiantis Austrijos komerciniu kodeksu (UGB) ir Ribotos atsakomybės kompanijų įstatymu (GmbHG), atsakomybė už duomenų apsaugą ir IT sistemų saugumą tenka organizacijų vadybos lygmeniui. Net ir perleidus duomenų apsaugos funkcijų užtikrinimą kitam personalui, galutinė atsakomybė užtikrinti teisės aktų reikalavimų vykdymą tenka organizacijos vadovybei. Duomenų apsaugos reguliavimo teisės aktai, drauge su direktyvą (EU) 2016/1148 realizuojančiu Tinklų ir informacinių

sistemų saugumo įstatymu (NISG), sukūrė vientisą reguliavimo mechanizmą strateginės svarbos įmonėms, skaitmeninių paslaugų teikėjams bei valstybinėms institucijoms nacionaliniu bei europiniu lygiu kibernetinio saugumo srityje. Remiantis šiais dokumentais įmonės privalo užtikrinti tinkamas technines bei organizacines priemones (pvz.: rezervinių kopijų darymą, duomenų šifravimą, prieigos kontrolę), siekiant išvengti atsitiktinio duomenų sunaikinimo arba nutekinimo trečiosioms šalims. Neužtikrinant šių reikalavimų įmonėms taikomos ženklios finansinės nuobaudos. ES Bendrasis duomenų apsaugos reglamentas drauge su Austrijos Duomenų apsaugos įstatymu reguliuoja asmens duomenų tvarkymą (pvz.: vardo bei pavardės, gimimo datos, elektroninio pašto, IP adreso įrašus). Tai suvienodina reguliavimo apimtį visoms verslo organizacijoms Austrijoje. Įmonėms pasiekus tam tikrą duomenų įrašų skaitmenizacijos lygį šie reikalavimai paprastai būna žinomi. Be to, Austrijos prekybos rūmai nuolat informuoja įmones apie teisinius reikalavimus asmens duomenų tvarkymui. Mažosios įmonės, kurios kreipia mažiau dėmesio į informacinių sistemų bei duomenų apsaugos teisinį reguliavimą, susiduria su rimtesniais iššūkiais užtikrinant teisės aktų reikalavimus.

Pareiga informuoti duomenų subjektus remiantis BDAR yra viena sunkiausiai įgyvendinamų ir, remiantis Conrad Lienhardt, Austrijoje yra dažnai netaikoma, ypač mažesnėse įmonėse: „Remiantis Bendruoju asmens duomenų apsaugos reglamentu, duomenų subjektų teisės apima ir teisinę prieigą prie informacijos“. Iš dalies tai reiškia padidintus įsipareigojimus tvarkyti įrašus iš įmonių pusės. Šie reikalavimai nurodomi 13-tame bei 14-tame BDAR straipsniuose. Lienhardt perspėja, kad pareiga informuoti apie duomenų naudojimą neturėtų būti nuvertinama: „Esama įmonių, kurios renka asmens duomenis iš viešai prieinamų duomenų bazių, tokių kaip žemės registrų duomenų bazės, adresų katalogai ir t.t. Vėliau šie duomenys yra apdorojami. Dažnai manoma, kad tokiu būdu įgyti duomenys nesukuria pareigos informuoti apie jų naudojimą, ypač kai išgaunami dideli asmens duomenų masyvai. Tačiau toks teisės aktų reikalavimų traktavimas gali sukelti nuostolių įmonėms, privatiems asmenims pradėjus ginti savo teises instituciniame lygmenyje. Dėl šios priežasties pareiga informuoti turėtų būti vertinama rimtai“ (Lienhardt 2020).

Darbuotojų duomenų naudojimas remiantis BDAR: Austrijoje asmens duomenų naudojimas papildomai reguliuojamas darbo bei socialinės teisės normų. Austrijos prekybos rūmai (WKO) pažymi: „Turėtų būti tikrinama, kokiais pagrindais duomenys yra apdorojami (pvz.: teisinių prievolių, būtinų paslaugos suteikimui, sutikimo gavimui). [...] Atvejais, kuomet apskaitininkas veikia kaip sutarties su klientu šalis, vykdanti įsipareigojimus organizacijai, papildomų sutikimų tvarkyti duomenis nereikia, tačiau tai turi būti raštiškai apibrėžta sutartyje (Wirtschaftskammer Österreich 2021b).

Austrijos prekybos rūmai (Wirtschaftskammer Österreich) taip pat siūlo paramą įgyvendinant BDAR, suteikiant informaciją apie reikalavimų užtikrinimą specifinėse veiklos srityse, veiksmų vadovus, pavyzdinius dokumentų šablonus bei atliktinų veiksmų sąrašus. Techninių ir organizacinių priemonių vadovas įgyvendinant BDAR suteikia praktinių įžvalgų apie technines duomenų saugos priemones bei jų įgyvendinimą (c. f. Wirtschaftskammer Österreich, 2020). Galiausiai, WKO iniciatyva

„IT Safe“ (c. f. Wirtschaftskammer Österreich, 2020) yra gerai žinoma užtikrinant IT saugos sprendimų paramą smulkioms ir vidutinėms organizacijoms.

Įmonės Austrijoje turi prieigą prie reikšmingo informacijos kiekio, susieto su BDAR įgyvendinimu. Svarbu ir tai, kad išsamūs teisiniai tekstai negali būti įsisąmoninami greitai. Dėl šios priežasties svarbu akcentuoti Austrijos federalinės ekonomikos rūmų veiklą. Ši organizacija yra svarbus kontaktinis taškas mažoms įmonėms ieškant atsakymų apie BDAR taikymo niuansus. Įgyvendinant „IT Safe“ buvo parengtas išsamus BDAR taikymo vadovas bei suorganizuoti nemokami informaciniai renginiai. Vienas iš itin reikšmingų paramos įrankių – interneto svetainė, kurioje pateikiami BDAR pagrindai suprantamu būdu (c.f. Wirtschaftskammer Österreich, 2021b).

Kitas patrauklus instrumentas yra pasiūlytas Kredito apsaugos asociacijos (Kreditschutzverband), teikiančios optimalią (kainos prasme) paramą, supažindinant su BDAR pagrindais keliais lygmenimis: patarimų, mokymų bei aplikacijos "DSVGO Assistant" (KSV1870) formomis.

Nepaisant visų šių pastangų žmonės Austrijoje vis dar kalba apie „nemylimą BDAR“. Šį teiginį iliustruoja Austrijos spaudos agentūros pranešimas spaudai:

Išblaivinanti Austrijos įmonių realybė

Šiame Austrijos spaudos agentūros pranešime (2020, gegužė) raportuojama apie BDAR įgyvendinimą Austrijoje, pradedant antrašte “Suprantama taip, įgyvendinama lėtai“.

„Nepaisant reikšmingai išaugusio jautrumo asmens duomenų apsaugos klausimams, ES reguliavimas buvo adaptuotas 30-yje procentų nacionalinių verslų nuo 2018-ųjų.“

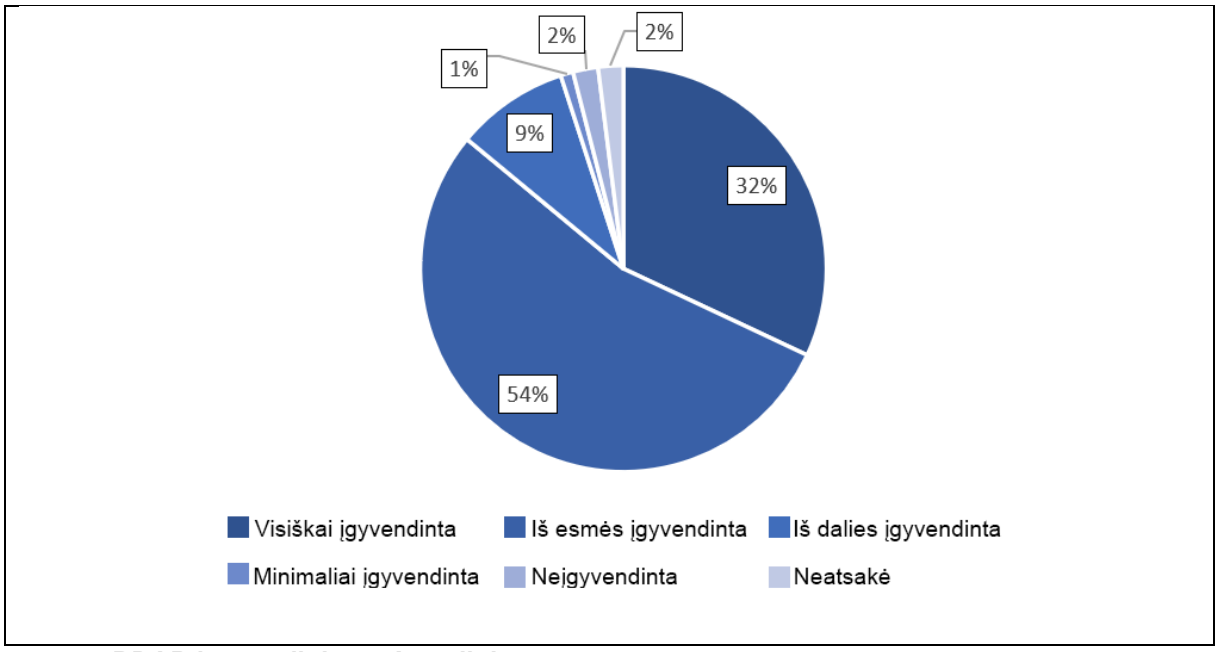
Straipsnyje akcentuojama, kad praėjus dvejiems metams nuo BDAR įsigaliojimo Austrijos įmonės demonstruoja gilesnį suvokimą asmens duomenų apsaugos tematikoje. Remiantis KSV1870 apklausa, vykdyta iki ištinkant COVID-19 pandemijai, kurioje dalyvavo apie 600 įmonių, 40 procentų įmonių teigė, kad suvokimas apie asmens duomenų apsaugą išaugo „visame sektoriuje“ per pastaruosius trejus metus. Apklausa parodė, kad dar reikia nemažai nuveikti siekiant geresnio BDAR reikalavimų įgyvendinimo, nes tik 30 procentų įmonių pripažino visa apimtimi perkėlusios šiuos reikalavimus į savo veiklos procesus. IT saugos priemonių integravimas buvo paminėtas 46 procentų įmonių, kaip viena iš dažniausių priemonių, padedančių užtikrinti geresnę duomenų apsaugą. Teigiamu aspektu laikytina tai, kad sąmoningumas apie informacijos asmens duomenų apsaugos svarbą yra reikšmingai išaugęs per pastaruosius trejus metus tarp Austrijos įmonių (Austrijos spaudos agentūra, 2020).

„Nepaisant to, kad 40 procentų įmonių patvirtina, jog asmens duomenų apsaugos svarbos suvokimas padidėjo „visame sektoriuje“ - kiti 32 procentai įmonių teigia įžvelgiančios pokyčius atskirose veiklos sferose. 19 procentų įmonių teigė, kad suvokimo lygis nepakito, o 2 procentai – kad sumažėjo“. 7 procentai respondentų atsakymų nepateikė. Austrijos spaudos agentūra, 2020). Dažnu atveju esama reikšmingos spragos tarp suvokimo ir realaus reikalingų duomenų apsaugos priemonių

įgyvendinimo. Anot Ricardo-José Vybiral, KSV1870 Holding AG vadovo, esant padidėjusiems skaitmenizacijos mastams dėl COVID-19 pandemijos nuogąstaujama, kad net trečdalis iš vietinių įmonių neįgyvendino BDAR reikalavimų visa apimtimi. Tarp visų reikalavimų nemažiau svarbus „duomenų apdorojimo operacijų registravimas“, kurį realizavo vos 34 procentai apklausoje dalyvavusių įmonių (Austrijos spaudos agentūra, 2020).

Deloitte Services Wirtschaftsprüfungs GmbH (2020) taip pat publikavo studiją, apžvelgiančią BDAR įgyvendinimo laipsnį tarp Austrijos įmonių 2020-ųjų pradžioje. Šioje internetinėje apklausoje dalyvavo 191 kompanijos atstovas, užimantis vadovaujančias pareigas. Studijos rezultatai atskleidė, kad „didžioji dalis įmonių vis dar dirba ties BDAR reikalavimų įgyvendinimu ir regi ilgalaikį reikalavimų vykdymą kaip iššūkį.“ Tuo pat metu temos svarbumas yra suprantamas tarp įmonių ir beveik visi respondentai teigė atkreipiantys dėmesį į asmens duomenų apsaugos reikalavimus priimant verslo sprendimus.

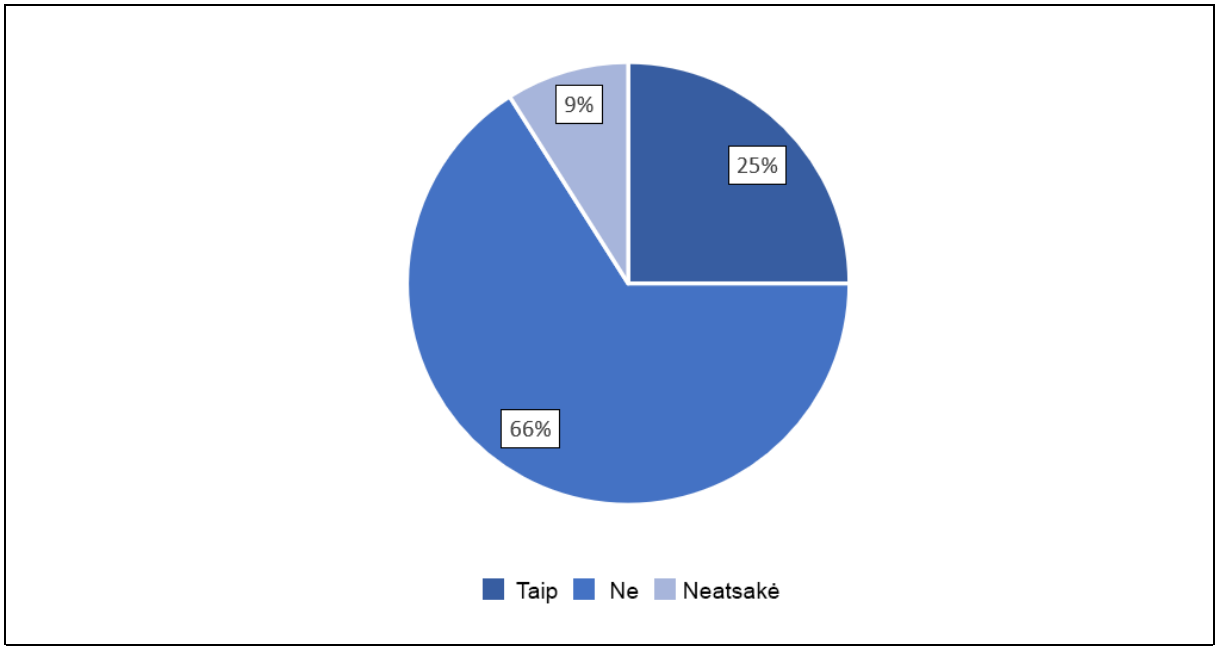
Panašiai kaip ir KSV1870 apklausos atveju, Deloitte prieina išvados, kad mažiau nei trečdalis Austrijos įmonių yra visiškai įgyvendinusios BDAR reikalavimus: „Didžioji dalis kompanijų (54%) vis dar yra paskutiniame BDAR reikalavimų įgyvendinimo etape – ten pat, kur ir buvo prieš metus. Nepaisant to, kad beveik trečdalis respondentų (32%) teigė visiškai įgyvendinę BDAR reikalavimus, 12 procentų įmonių procesą tėra įpusėję ir joms būtina pasitempti.“ Deloitte ataskaitoje teigiama, kad daugiau neturėtų būti pasiteisinimų direktyvos reikalavimų įgyvendinime. Dėl šios priežasties skubiai rekomenduojama imtis veiksmų tvarkant šią situaciją ir, esant reikalui, kreiptis išorinės pagalbos siekiant reikalavimų įgyvendinimą paspartinti. Respondentų atsakymai apie BDAR įgyvendinimo lygį įmonėse pasiskirsto taip:



Pav. 3: BDAR įgyvendinimas Austrijoje

Šaltinis: Sudaryta autorių naudojant Deloitte Services Wirtschaftsprüfungs GmbH (2020) duomenis

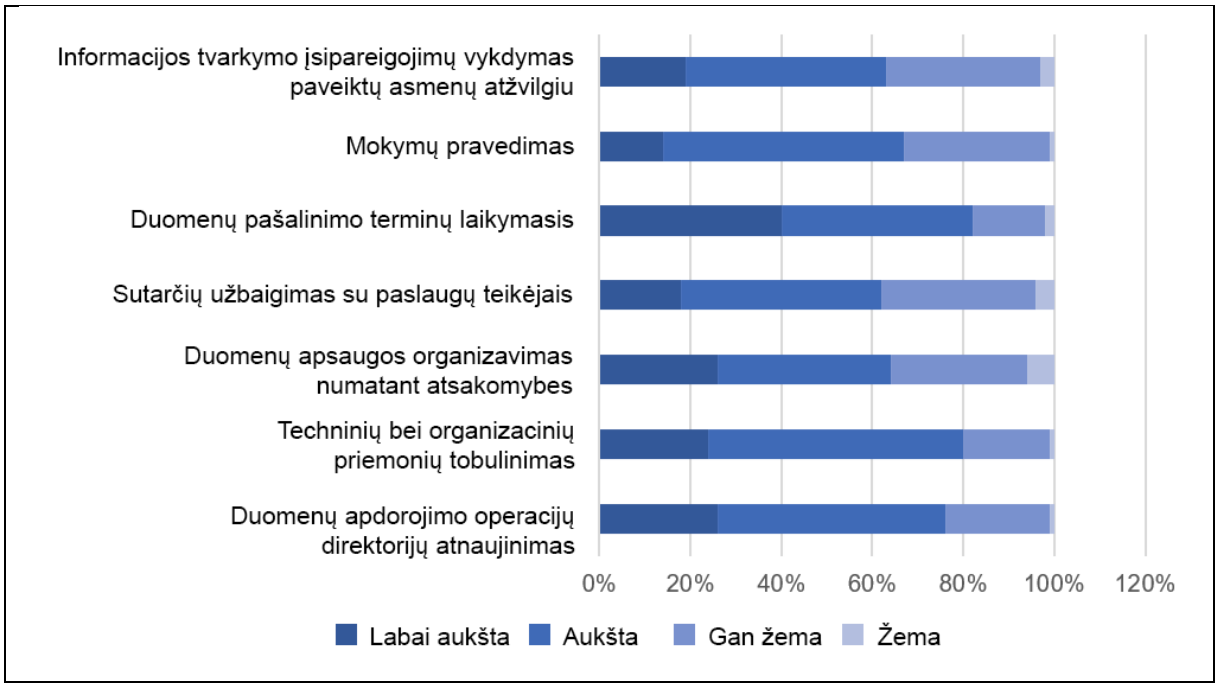
2020-aisiais žiniasklaida pranešė, kad baudų lygis už neįvykdytus BDAR reikalavimus išaugo. Deloitte taip pat klausė įmonių, kaip šie pranešimai paveikė jų elgseną: „Tik ketvirtyje įmonių duomenų apsaugos instancijų sprendimai paveikė jų procesus įgyvendinant BDAR. Iš šių įmonių didžioji dalis panaudojo išskirtus neatitikimus įvertinant arba tobulinant savo įmonės atitikties statusą. Klausimas buvo formuluojamas taip: „Ar pastarieji Austrijos duomenų apsaugos vadovybės sprendimai paveikė jūsų požiūrį į BDAR?



Pav. 4: Austrijos duomenų apsaugos vadovybės poveikis požiūriui į BDAR

Šaltinis: Duomenys panaudoti iš Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Deloitte studijoje pažymima, kad daugybė kompanijų Austrijoje nesugebėjo atlikti savo namų darbų per pastaruosius metus. Neretai stokojama struktūruotos duomenų klasifikacijos, kuri reikšmingai sumažintų pastangas reikalavimų užtikrinimui. Kitas klausimas pateikia įdomių įžvalgų apie susidariusią situaciją: Kiek pastangų prireiks norint atitikti BDAR reikalavimus ateityje?



Pav. 5: Potencialios pastangos siekiant įgyvendinti BDAR reikalavimus

Šaltinis: Sudaryta autorių remiantis Deloitte Services Wirtschaftsprüfungs GmbH (2020)

Ataskaita rodo, kad didžiosios dalies kompanijų ilgalaikis procesų suderinamumas su BDAR yra vertintinas kaip keliantis iššūkių. Respondentai labiausiai akcentavo pastangas, kurių reikia siekiant laiku pašalinti duomenų įrašus.

Kitas klausimas, kurį analizavo Deloitte, buvo susietas su personalo kiekiu, reikalingu duomenų apsaugos užtikrinimui: „Daugiau nei ketvirtis apklausoje dalyvavusių įmonių akcentavo žmogiškųjų išteklių trūkumą siekiant atliekant BDAR įgyvendinimo darbus. Dėl to kitų formų parama tarpa itin aktualia. Dėl šios priežasties vis daugiau Austrijos įmonių atsigręžia į technologinius sprendimus siekiant atitikties BDAR. Nepaisant to, kad praėjusiais metais priemonių stokojo 39 procentai įmonių, šiuo metu tokių organizacijų yra apie 30 procentų.“

Deloitte ataskaitoje prieinama išvados, kad: „po pirminio netikrumo laikotarpio Austrijos kompanijos gerokai aiškiau suvokia esamą veiksmų poreikį. Visgi, kai kurios nurodytos temos reikalauja esminių pokyčių. Tai paliečia į įmonės kultūrą.“ (Deloitte Services Wirtschaftsprüfungs GmbH 2020)

Hafelekar teigimu, Austrijos situaciją įgyvendinant BDAR galima apibendrinti taip: “Galima teigti, kad įstatymų bazė numatanti BDAR įgyvendinimo priemones yra aiški. Nepaisant to, teisės aktai ne visais atvejais yra formuluojami suprantamai. Esama keletas viešųjų institucijų (pirmiausiai – WKO), į kurias įmonės gali kreiptis siekiant paramos BDAR įgyvendinime. Austrijoje atsakomybė už asmens duomenų apsaugos pažeidimus tenka organizacijos vadovybei net jei atsakomybės ir yra deleguojamos kitiems darbuotojams. Įgyvendinimas vis dar nėra patenkinamas ir remiantis mūsų apklaustos fokus grupės Austrijoje duomenimis, laiko trūkumas mažose bei vidutinėse įmonėse yra svarbiausias faktorius trukdantis BDAR įgyvendinimui. Galiausiai, TeBelsi

iniciatyvinė grupė įžvelgia ženklų interesą turėti prieigą prie prieinamų tolimesnių mokymų asmens duomenų apsaugos ir IT saugumo srityje.

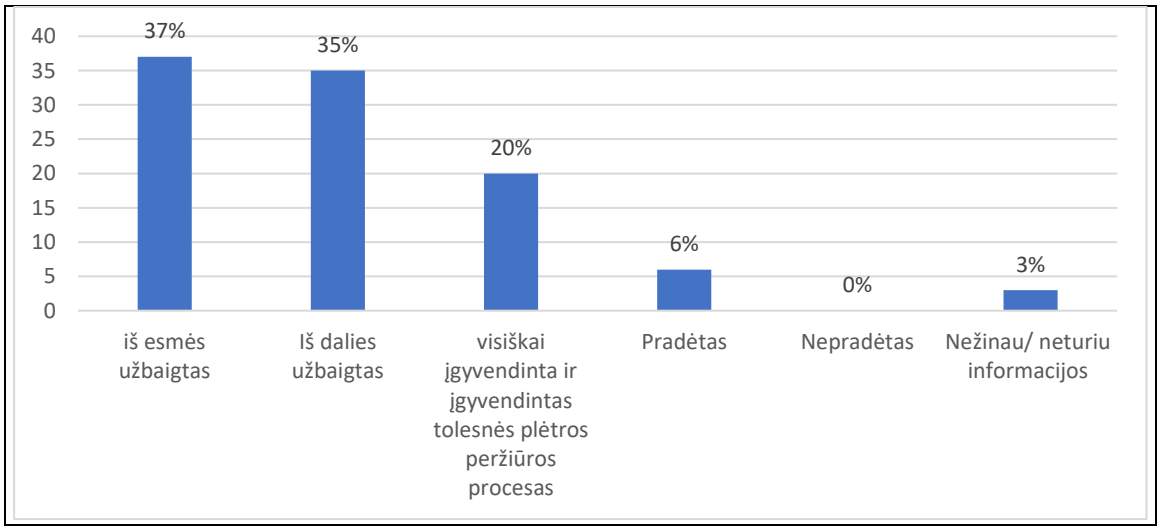
2.3 Vokietija

Institucijos pavadinimas	Trumpas aprašymas	Pagrindinis tikslas	Tinklapis
Vokietijos duomenų apsaugos asociacija (DVD)	DVD yra atsakinga už pranešimų, susijusių su duomenų apsauga (DANA), skelbimą. Taip pat dalis veiklos apima viešuosius ryšius ir darbą su žiniasklaida aktualiomis temomis, spaudos konferencijas ir pranešimus spaudai. Be to, rengiami susitikimai bendradarbiaujant su organizacijomis partnerėmis ir DVD taip pat dalyvauja kasmetiniuose "Didžiojo brolio" apdovanojimuose.	DVD tikslas patarti ir informuoti visuomenę apie riziką, susijusią su elektroninių duomenų tvarkymu ir galimu informacinio apsisprendimo teisės apribojimu.	https://www.datenschutzverein.de
Duomenų apsaugos ir duomenų saugumo draugija (GDD)	1977 m. įkurta GDD šiuo metu vienija daugiau nei 3 800 narių. Visoje šalyje veikia 34 rateliai, kuriuose dalijamasi nauja patirtimi. Juose dalyvauja daugiau kaip 3 500 dalyvių, o GDD akademijoje jau apmokyta daugiau kaip 10 000 duomenų apsaugos pareigūnų.	Duomenų apsauga, duomenų saugumu ir tinkamu duomenų tvarkymu siekiama apsaugoti visas suinteresuotąsias šalis nuo pavojų, kartu užtikrinant informacijos laisvę ir informacijos pusiausvyrą. Teisinės prievolės turi įtakos visoms įmonėms ir administraciniams vienetams, nepriklausomai nuo jų dydžio ar pramonės šakos. GDD nori įnešti svarų indėlį.	https://www.gdd.de/
Forumas "Informatika taikai ir socialinei atsakomybei (FIfG)	FIfG dirba apie 700 mokslo ir praktikos atstovų, ypač kompiuterių mokslo ir informacinių technologijų specialistų. Tikslas - sudaryti sąlygas keistis informacija tarp visų su kompiuterių mokslu ir informacinėmis technologijomis susijusių asmenų. FiFG yra atvira visiems, kurie norėtų dalyvauti veikloje arba tiesiog norintiems gauti informacijos.	FiFG įspėja visuomenę apie žalingus pokyčius informacijos saugumo srityje. Be to, asociacija kovoja prieš informacinių technologijų naudojimą kontrolei ir sekimui. FiFG taip pat remia lygias neįgaliųjų teises kuriant ir naudojant informacines technologijas ir kovoja su moterų diskriminacija informatikos srityje.	https://www.fiff.de/
Digitalcourage e.V.	Asociacija buvo įkurta 1987 m. Be kita ko, ji remia fondines teises ir duomenų apsaugą, vykdo šviečiamąjį darbą per viešuosius ryšius, pvz., kampanijas ir	Didžiąją darbo dalį sudaro projektų ir kampanijų organizavimas, taip pat politinių kongresų rengimas. Be to, asociacija spaudoje ir žiniasklaidoje pasisako duomenų	https://digitalcourage.de/

	projektus, ir yra atsakinga už kasmetinį "Big Brother Award" apdovanojimą.	apsaugos klausimais. Pagrindinis tikslas – rūpintis duomenų apsauga ir gyvenimo verte skaitmeniniame amžiuje.	
Federalinis duomenų apsaugos ir informacijos laisvės komisaras (BfDi)	Pagrindinės 1978 m. įkurtos institucijos užduotys - stebėti ir užtikrinti BDAR, **BDSG** ir kitų duomenų apsaugos reglamentų laikymąsi. Be to, ji rūpinasi informuotumo didinimu ir viešaisiais ryšiais.	Pagrindinis tikslas – užtikrinti ir plėtoti duomenų apsaugą. Nuo 2006 m. kiekvienas, manantis, kad jo teisė gauti informaciją pagal Informacijos laisvės įstatymą (IFG) buvo pažeista, gali kreiptis į federalinį komisarą. Šiuo metu šias pareigas eina profesorius Ulrichas Kelberis.	https://www.bfdi.bund.de/

Lentelė 3: Vokietijos socialiniai partneriai

Europos Bendrasis duomenų apsaugos reglamentas (BDAR) įsigaliojo 2016 m. gegužės 24 d. Nuo 2018 m. gegužės 25 d. jame nustatyti duomenų apsaugos reikalavimai yra privalomi atitinkamose valstybėse narėse net ir atskirai neperkėlus jų į nacionalinę teisę. Europos duomenų apsaugos reglamentu visų pirma siekiama sustiprinti vartotojų teises. Duomenų tvarkymo įstaigos turi tikėtis griežtesnio reglamentavimo. Bendrojo duomenų apsaugos reglamento reikalavimų nesilaikymas atitinkamai įmonei gali kainuoti iki 20 mln. eurų baudos arba iki 4 proc. jos pasaulinių pardavimų (priklausomai nuo to, kuri vertė didesnė) (datenschutz 2021). Vokietijoje veikiančių įmonių BDAR įgyvendinimo būklė parodyta 3 paveiksle. Statistika buvo paskelbta praėjusių metų rudenį. Tai naujausias turimas tyrimas apie BDAR įgyvendinimą. Tyrimo metu 37 proc. respondentų nurodė, kad jau įgyvendino BDAR gaires. Daugiau nei pusė dalyvių nurodė, kad gairės yra iš dalies įgyvendintos arba visiškai įgyvendintos ir nustatytos tolesniam tobulinimui (2020)[1].

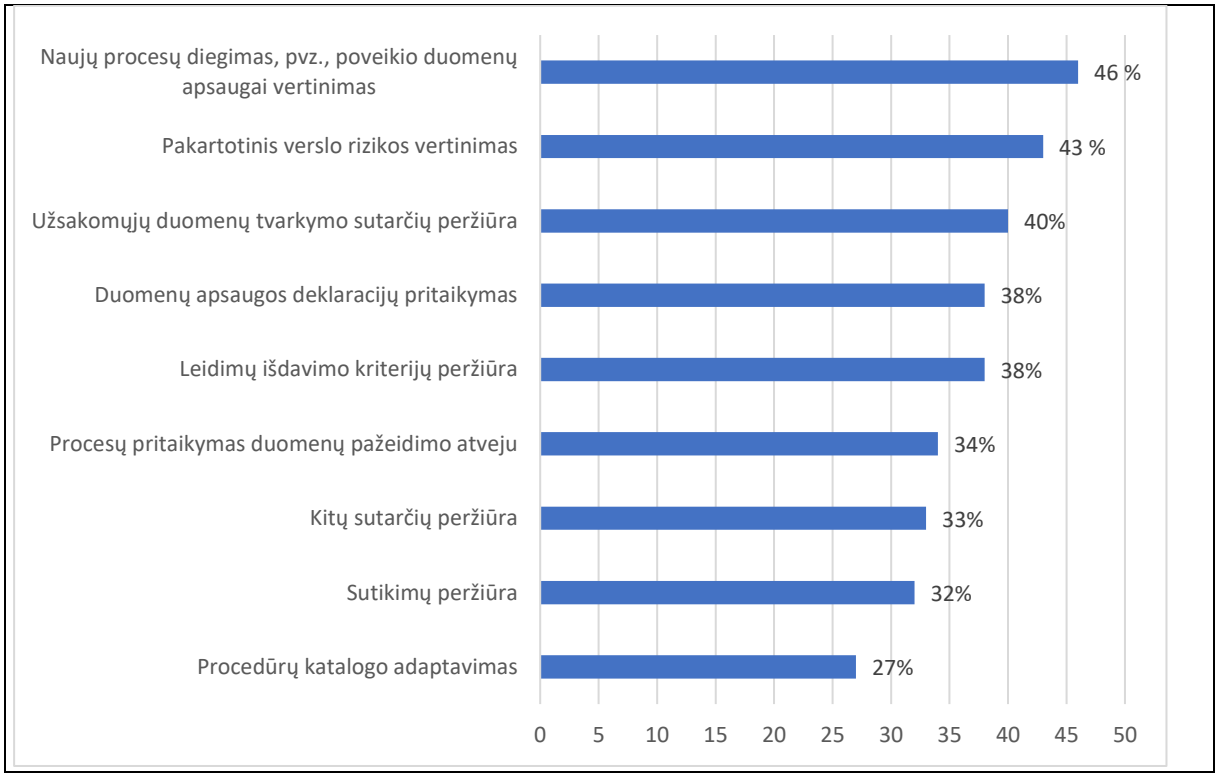


Pav. 6: Bendrojo duomenų apsaugos reglamento įgyvendinimo padėtis Vokietijos įmonėse (09/2020 m.)

[1] Daugiau informacijos apie tyrimą: paskelbimo data 2020-09-09, Vokietija, tyrimo laikotarpis 09/2020, respondentų skaičius: 504 įmonės, kuriose dirba 20 ir daugiau darbuotojų, apklausa telefonu

Atsižvelgiant į tai, kad praėjo maždaug 5 metai nuo paskelbimo ir 3 metai nuo įsigaliojimo, galima daryti išvadą, kad įmonėms kyla rimtų kliūčių, trukdančių visiškai įgyvendinti BDAR. Konkretūs padariniai išsamiai aprašyti Bitkom E.V. (2020) atliktame tyrime. Viena iš priežasčių, kodėl įmonėms sunkiai sekasi įgyvendinti BDAR, gali būti siejama su dideliu pastangų kiekiu, pradedant pradinėmis (ir vienintelėmis) papildomomis išlaidomis (63 proc.), nuolatinių papildomų išlaidų lūkesčiais (palyginti su ankstesniu teisiniu statusu, 29 proc.) ir papildomų darbuotojų poreikiu (26 proc.). Personalo poreikis taip pat atsispindi įmonių sprendime pirkti duomenų apsaugos paslaugą iš paslaugų teikėjų, teikiant išorines teisines konsultacijas (40 %), išorines duomenų apsaugos konsultacijas (31 %) arba išorines peržiūras (28 %). Nepaisant to, dauguma įmonių mano, kad BDAR teigiamai prisideda prie įmonės veiklos ir jos rezultatų. Atsižvelgiant į poveikį vienodai konkurencinei aplinkai visoje ES (57 proc.).

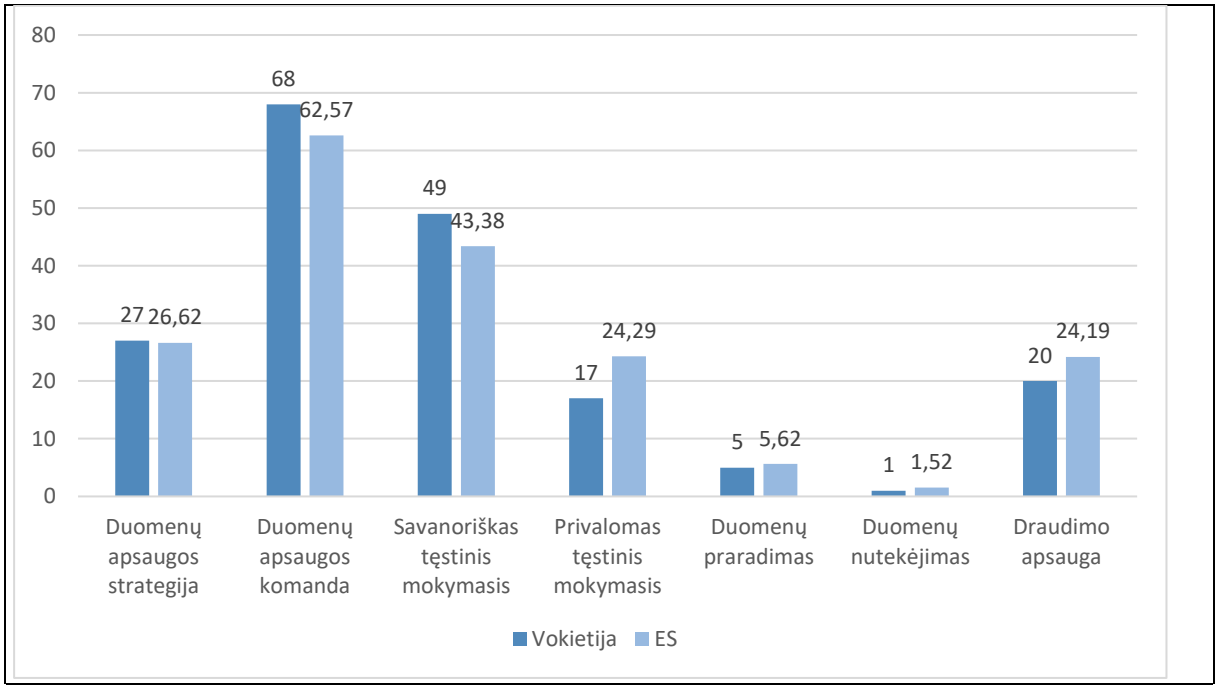
Vis dėlto, atsižvelgiant į sudėtingus reguliavimo pokyčius, keli aspektai kelia abejonių dėl teigiamo poveikio ekonominei veiklai. Be kita ko, kyla susirūpinimas dėl ilgalaikio teisinės aplinkos gerinimo (43 proc.), naujovių diegimo kliūčių (35 proc.) ir verslo procesų apsunkinimo (25 proc.). Kaip matyti 4 pav., su BDAR įgyvendinimu susijusi rizika taip pat atsispindi priemonėse, kurių įgyvendinimui skiriama daugiausia dėmesio.



Pav. 7: Kokias BDAR įgyvendinimo priemones labai skubiai įgyvendinsite?
Šaltinis: Bitkom e.V. (2020)

2021 m. atliktame tyrime pabrėžiama, kad Vokietijoje duomenų apsaugai apskritai teikiamas aukštas prioritetas, o pagal bendrą ir tinkamą duomenų apsaugos traktavimą ji užima antrą vietą tarp visų Europos šalių (HeyData, 2021 m.). Iš visų nagrinėjamų kategorijų pažymėtina, kad "įmonės" užima žemiausią vietą, palyginti su "teisėsauga", "duomenų apsaugos kompetencija" ir "visuomenės nuotaikomis", o "privatūs asmenys"

- palyginti aukščiausią. Kiekvieną kategoriją galima išskaidyti į kelis kriterijus, kurie atskleidžia konkrečias stipriąsias ir silpnąsias puses. Nagrinėjant įmonių padėtį, kaip matyti 5 pav., matyti, kad tik 17 proc. įmonių yra įdiegtos privalomo kvalifikacijos kėlimo priemonės, palyginti su 24,29 proc. įmonių ES vidurkiu. Antras didelis trūkumas, palyginti su likusia ES dalimi, išryškėja kalbant apie draudimo apsaugą - Vokietijos rezultatai yra 4 procentiniais punktais prastesni už ES vidurkį.



Pav. 8: Vokietijos ir ES vidurkio duomenų apsaugos balų sudėtis procentais
Šaltinis: heyData (2021 m.). Autoriaus iliustracija

Atsižvelgiant į duomenų privatumo pažeidimus, Vokietijoje taikomos griežtos bausmės. Už duomenų apsaugos pažeidimus griežtai baudžiama, nes 2020 m. skirta apie 69 mln. eurų baudų. Ši išvada siejasi su tuo, kad Vokietijoje iš viso užregistruota daugiausia duomenų apsaugos pažeidimų. Ypač per visą pandemijos laikotarpį, kai buvo dirbama namų biure, pažeidimų padaugėjo apie 76 %, palyginti su praėjusiais metais. Šios išvados pasekmės paaiškinamos taip: "Lyginant su likusia Europos dalimi, Vokietijos įmonės dažniausiai elgiasi labai pavyzdingai. Tačiau tai taip pat būtina. Teisėsaugos institucijos Vokietijoje elgiasi griežtai." (Milos Djurdjevic, CEO heyData, 2021 05).

Atsižvelgiant į šiuos duomenis, nenuostabu, kad buvo įkurtos kelios asociacijos, kurios rūpinasi būtent tinkamu duomenų apsaugos įgyvendinimu viešojoje ir verslo srityse. "Teisė į informacinį apsisprendimą" (1983 12 15 BVerfG) ir asmens teisių apsauga nuo vis labiau akcentuojamų saugumo interesų yra šių asociacijų veiklos sudedamoji dalis. Todėl manoma, kad grėsmė duomenų apsaugai ir informacijos saugumui išlieka ne tik tarp nusikalstamų ir priešiškai nusiteikusių subjektų, bet ir iš federalinės vyriausybės ir jos saugumo interesų.

2.4 Italija

Įstaigos pavadinimas	Trumpas aprašymas	Pagrindinis tikslas	Tinklapis
Apindustria Vicenza - MVĮ asociacija Vičencoje.	Apie 1000 narių (dauguma jų yra labai smulkūs ir smulkūs verslai, juose dirba mažiau nei 20 darbuotojų). Jie siūlo tokias paslaugas kaip: ryšys su vietos ir regionų valdžios institucijomis (regioninis departamentas, rūmai, regioninė politika); mokesčiai ir teisinės paslaugos nariams; mokymo kursai; konkrečias paslaugas (t. y. eksportui, tinklui, tinkamumui, teisiniams klausimams, ES projektams, sertifikatams ir kt.). Kontaktinis asmuo: Mr Manuel Maraschin (Vadovas; mail: m.maraschin@apindustria.vi.it)	Kai kurios įmonės (susijusios su „Apindustria Vicenza“) jau turi IT ir VB vadovą. Tokiu atveju galima patikrinti ir išbandyti (dalinį) sertifikavimo procesą su šiais vadovais, tikrindami mokymo kelius per IO3 turinį (internetinis klausimynas). Ir atvirkščiai, pasitelkus išorės ekspertus (konsultantus, IT tiekėjus, teisininkus ir kt.), kurie remia MVĮ, galima patikrinti, ar sertifikavimas atitinka jų kasdienį darbą. „Apindustria Vicenza“ gali organizuoti kai kuriuos susitikimus su vietos MVĮ ir tuo pačiu metu pasiūlyti IT ir VB vadovams keletą interviu, kurie galėtų būti naudingi projekto IO. „Apindustria“ nėra viešoji įstaiga; bet tam tikra „tarpinė“ organizacija, atstovaujanti ir vietos / regioniniams kolektyviniams interesams. „Apindustria Vicenza“, kaip prekybos asociacija, dalyvauja regioninėse darbo ir techninėse lentelėse. Šiuose susitikimuose taip pat daugiausia dėmesio skiriama profesiniam profiliui, konkrečių kompetencijų apibrėžimui, (daliniams) sertifikavimo procesams ir pan. Taigi „Apindustria“ galėtų paremti šio naujo profilio įgyvendinimą, taip pat ir todėl, kad atstovauja kelioms vietos MVĮ. Kai kurių ESF - Europos socialinio fondo kursų dėka „Apindustria“ projekto pabaigoje galėtų įgyvendinti ir konkrečius mokymo būdus, kuriuos galėtų (iš dalies) patvirtinti mūsų regioninis mokymo biuras. Tvarkaraštis: naujas ES 2021–2027 m. planavimas vis dar svarstomas. Šiuo metu regioniniame lygmenyje vyksta keli techniniai susitikimai (pagrindinis mokymo strategijos tikslas, naujas turinys, darbo profilių suderinimas nacionaliniu ir europiniu lygiu, ESCO prioritetai ir kt.). Tačiau „Apindustria“ taip pat galėtų informuoti regionų valdžią apie projekto turinį. Taigi dėl to kai kurie projekto rezultatai galėtų būti įgyvendinti naujose programose.	www.apindustria.vi.it
CPV – CentroProduttivitàVeneto	Ji yra viena didžiausių mokymo paslaugų teikėjų Veneto regione, turinti beveik 70 metų patirtį. CPV siūlo platų mokymo kursų spektrą, skirtą MVĮ, darbuotojams, vadovams, padėjėjams ir bedarbiams. Per pastaruosius 2/3 metus jie surengė keletą mokymo kursų projekto temomis. Kontaktinis asmuo: Enrico Bressan (mokymo departamento ir ES projektų direktorius; paštas: bressan@cpv.org). Jis yra ilgametės mokymosi agentūros Romoje išorės ekspertas.	J. Bressanas turi didelę patirtį (dėka kai kurių regioninių, nacionalinių ir tarpvalstybinių projektų) ESCO platformos, „Ecvet“ sistemos, EKS schemų ir t.t srityje. Jis galėtų paremti projektą ir keistis savo patirtimi. Be to, CPV gali įtraukti keletą vietinių smulkių įmonių. Būdama mokymo paslaugų teikėja, CPV sukūrė stiprų regioninį tinklą profesinio mokymo ir suaugusiųjų švietimo srityje. Jame yra daug ekspertų (pavyzdžiui, konsultantų ir instruktorių), kurie galėtų patikrinti ir patvirtinti tam tikrą kompetencijų sąrašą. CPV gali įtraukti vietos smulkųjį verslą, pavyzdžiui, organizuoti interviu su potencialiais kandidatais ir susitikimus (seminarus) su įmonėmis. CPV taip pat vadovauja „tyrimo grupei“ (nuo 1985 m.), Orientuotai į IT, informatiką, duomenų apsaugą, skaitmeninimą ir kt. Jiems galėtų būti pateikti projekto tarpiniai ir galutiniai rezultatai. Būdama „viešoji/privati“ institucija, CPV yra įtraukta į keletą regioninio lygmens techninių lentelių (pavyzdžiui, ekspertų grupės kompetencijų ir darbo profilių pripažinimo ir vertinimo komitetas). Ji galėtų peržiūrėti mūsų regioninį prisitaikymo planą ir po to atlikti tam tikrą lobistinę veiklą su mūsų regionų valdžios institucijomis.	www.cpv.org
Cesar srl	Tai mokymo centras Vičencoje, skirtas vietinei amatų asociacijai (turinčiai daugiau nei 20 000 mikro ir smulkaus verslo įmonių). Ji siūlo platų mokymo paslaugų spektrą, įskaitant IT saugumo, duomenų apsaugos, BDAR ir kt.	Cesar dirba tik su labai mažomis ir mažomis įmonėmis (iki 10 darbuotojų). Paprastai šiose įmonėse nėra vidinio eksperto, pavyzdžiui, IT saugumo ir duomenų apsaugos vadovo ar atsakingo. Mokymo kursų (finansuojamų ar ne) dėka Cesar gali paremti (dalinį) sertifikavimo procesą. „Cesar“ gali būti įtrauktas į kelis etapus, tokius kaip: smulkiųjų įmonių dalyvavimas; poreikių analizė; pagrindinių kompetencijų apibrėžimas; pilotavimas ir mokymas. Ateityje jie taip pat galėtų pasiūlyti vietos įmonėms TEBEISI sertifikuotus kursus	www.confartigianatovicenza.it

	kursus. Kontaktinis asmuo: ponia Daniela Bucci (mokymo skyriaus direktoriaus pavaduotoja; paštas): d.bucci@confartigianatovicenza.it).	su visais projekto rezultatais. „Cesar“ yra regioninio mokymo centrų tinklo, skirto labai mažoms ir mažoms įmonėms, dalis, kurią sudaro 7 provincijos (iš viso 75 000 narių). Cezaris labai dažnai dalyvauja keliose regioninėse techninėse lentelėse ir darbo profilių bei sertifikavimo proceso darbo grupėse. Ji galėtų žinoti mūsų regioninę valdžią apie projekto tikslus ir rezultatus, visų pirma labai mažoms įmonėms.	
Vičencos prekybos rūmai	Tai yra viešoji įstaiga Italijoje ir siūlo privalomas paslaugas visoms įmonėms. Pavyzdžiui, kiekviena vietinė įmonė turi būti užregistruota vietinėje duomenų bazėje (visais verslo etapais nuo pradžios iki pabaigos). Vicenza rūmai atstovauja daugiau nei 90 000 įmonių, dauguma jų yra labai mažos arba mažos. Kontaktinis asmuo: Diego Rebesco (statistikos departamento ir reklamos vadovas; paštas: diego.rebesco@vi.camcom.it).	Rūmai siūlo platų paslaugų spektrą, kuris apima daugiau ar mažiau visus įmonės poreikius (administracinės pareigos, mokymai, eksportas, sertifikatai, patentai ir kt.). Rūmai taip pat aktyviai dirba profesinių kvalifikacijų pripažinimo srityje, pavyzdžiui, per Švietimo ir darbo ministeriją Romoje. Organizuoja praktikas jauniems žmonėms (iš aukštųjų mokyklų), kurie siekia įgyti patirtį įmonėje, per tam tikrus patvirtintus susitarimus, kurie galiausiai yra įvertinti. Tai galėtų būti įtraukta ne tik į projekto skatinimą ir sklaidą (pvz., Informacinis biuletenis ar vietinis seminaras), bet ir į sertifikavimo procesą, nes yra ryšys su mūsų nacionaline ministerija. Bent jau būtų galima informuoti apie projekto eigą. Tačiau jie taip pat galėtų sudaryti vietinę (Vičencos provincijos) darbo grupę. Pasibaigus projektui ši įstaiga galėtų pristatyti galutinį (dalį) TEBEISI sertifikavimo procesą mūsų regioninei institucijai, kad ji būtų visiškai pripažinta. Tai gali būti mūsų viešoji įstaiga, kuri tikrina ir patvirtina visą regioninį prisitaikymo planą, atsižvelgdama į jo funkcionalumą ir tikslą. Išsamiau jie galėtų patikrinti tvarkaraštį, pavienių dalyvių vaidmenis ir, visų pirma, patvirtinti pagrindinį plano turinį, taip pat atsižvelgiant į būsimus konkrečius teisės aktus, susijusius su projekto tema, arba konkrečius poreikius, kurie galėtų būti įtraukti į regionines mokymo programas.	www.vi.camcom.it
Proservizi srl	Tai regioninis „ConfProfessioni Veneto“ mokymo centras (kuriame yra daugiau nei 45 000 narių, tokių kaip teisininkai, fiskaliniai ekspertai, notarai, konsultantai ir kt.). Jis siūlo platų mokymo paslaugų spektrą, įskaitant IT saugumo, duomenų apsaugos, BDAR ir tt kursus. Kontaktinis asmuo: Greta Cosentino (mokymo skyriaus direktorė, el.paštas: greta.cosentino@proservizi.it).	„Proservizi“ kaip klientai turi tik konsultantus (ne įmonę). Taigi, jie gali įtraukti daug, pavyzdžiui, teisininkų, kurie specializuojasi IT saugumo ir duomenų apsaugos teisės aktų srityje. Be to, jie labai dažnai siūlo GPPR ir privatumo kodų mokymo kursus (pagrindinius ir išplėstinius). Taigi jie gali patikrinti ir palyginti projektų kelius (pavyzdžiui, pagal konkrečių kompetencijų sąrašą) ir tai, ko reikia rinkai (įmonėms). Proservizi jau dalyvavo projekto veikloje. Pavyzdžiui, kai kurie nariai (t. Y. Teisininkai) atliko projekto interviu. Jie taip pat siūlo finansuojamus mokymo kursus (dėka ESF - Europos socialinio fondo ir (arba) specialių dotacijų iš jų mokymo sistemos, vadinamos „Fondo ConfProfessioni“). Taigi jie gali ateityje finansuoti TEBEISI profilio kursus. „Proservizi“ galėtų remti visų pirma bandomuosius etapus, t. Y. Įtraukti kai kuriuos vietinius teisininkus su mažomis įmonėmis (jų klientais) tik tam, kad patikrintų projekto turinį. Bet ir norint įgyti naujų kompetencijų IT saugumo ir duomenų apsaugos valdytojo srityje. Jie taip pat galėtų organizuoti konkretų narių mokymo kursą, į kurį būtų įtraukti visi TEBEISI rezultatai ir rezultatai. Proservi labai dažnai dalyvauja keliose regioninėse darbo grupėse mokymo poreikių ir kompetencijų pripažinimo srityje. Taigi, ji galėtų pasiūlyti mūsų regioninei mokymo institucijai, pavyzdžiui, naujos informacijos apie kitą ESF programą (kuri apims 2021–2027 m. laikotarpį).	www.proservizi.it
SATEF srl	Tai regioninis mokymo centras. Ji siūlo platų mokymo paslaugų spektrą, įskaitant IT saugumo, duomenų apsaugos, BDAR ir tt kursus. Jis taip pat specializuojasi sveikatos ir saugumo sektoriuje, įskaitant pagyvenusių žmonių priežiūros centrus. Kontaktinis asmuo: Paolo	Direktorius P. Pedronas yra ESCCO / „Ecvet“ ekspertas regioniniu ir nacionaliniu lygiu. Jis sukūrė specialią mokymo platformą, skirtą kompetencijų pripažinimui ir (dalies) atestavimui. Šiuo metu jis vykdo veiklą dviejuose sektoriuose: sveikatos ir saugos bei turizmo. Taigi, mes galėjome išbandyti savo projekto turinį jo platformoje. Šiame bandyme taip pat galėtų dalyvauti mažos įmonės ir kai kurie konsultantai/ ekspertai. „Satef“ galėtų išbandyti projekto turinį, pavyzdžiui, turizmo srityje. Iš tikrųjų, atsižvelgiant į ankstesnę patirtį, platforma jau egzistuoja, taip pat ir mokymo kryptimi. Taigi, TEBEISI mokymų turinį būtų galima išbandyti, tačiau taip pat būtų galima atlikti (dalį) sertifikavimo procesą ir regioniniu	www.satef.com

	Pedron (mokymo skyriaus įkūrėjas ir direktorius; el: pedron@satef.com).	lygiu. R. Pedronas dalyvauja kai kuriose regioninėse darbo grupėse „darbo profilių sertifikavimo ir vertinimo“ tema. Taigi jis gali tvirtai paremti mūsų įgyvendinimo etapą. Dėl Pedrono vaidmens regioniniu lygmeniu jis gali reklamuoti mūsų valdžios institucijas apie projekto turinį ir rezultatus (įskaitant bandymų etapus). Jis taip pat galėtų neoficialiai patvirtinti mūsų „regioninį prisitaikymo planą“ prieš pat siunčiant jį (galutinei diskusijai) į mūsų regioninį mokymo ir darbo departamentą Venecijoje.	
ENGIM Veneto	Tai yra didžiausia mokymo įstaiga Veneto regione, turinti beveik 90 metų patirtį. ENGIM siūlo platų mokymo kursų spektrą, skirtą MVĮ, darbuotojams, vadovams, pagalbininkams ir bedarbiams. Per pastaruosius 2/3 metus jie taip pat surengė keletą mokymo kursų projekto temomis. Kontaktinis asmuo: Manuel Fochesato (mokymo departamento ir ES projektų direktorius; paštas: manuel.fochesato@engimvi.it).	J. Fochesato turi didelę patirtį (dėka kai kurių regioninių, nacionalinių ir tarpvalstybinių projektų) ESCO platformos, „Ecvet“ sistemos, EKS schemų ir tt srityje. Jis galėtų paremti projektą ir keistis savo patirtimi. Be to, ENGIM gali įtraukti keletą vietinių smulkių įmonių, taip pat konsultantų, instruktorių ir ekspertų. „Engim“ taip pat veikia kaip profesinis mokymas; todėl dalis mokymo kursų yra skirta jaunimui, suaugusiems, kuriems reikia papildomo mokymo, ir, svarbiausia, bedarbiams. „Engim“ jau vykdo (ir planuoja) kelias mokymo platformas, kuriose yra ne tik mokymo medžiaga (t. Y. Internetiniai kursai įvairiems švietimo poreikiams), bet ir IT sistemos, kurios tam tikrą laiką iš dalies atpažino konkrečias kompetencijas. „Engim“ gali tvirtai remti darbo profilių įgyvendinimą keliais būdais: surasti galutinius vartotojus (smulkaus verslo įmones ir (arba) konsulantus/ekspertus); įtraukti stažuotojus (jaunus ir (arba) suaugusius), kurie ieško naujos darbo specializacijos ir, galiausiai, bet ne mažiau svarbu, diskutuoti ir keistis vietinėmis (regioninėmis) mokymo institucijomis. Dėl Fochesato vaidmens ir patirties regioniniu lygmeniu jis gali reklamuoti mūsų valdžios institucijas apie projekto turinį ir rezultatus (įskaitant bandymų etapus). „Engim“ taip pat galėtų pasidalyti regioniniu prisitaikymo planu su keliais viešaisiais suinteresuotaisiais subjektais. Bet taip pat galėtų sukurti naują turinį savo internetinėse mokymo platformose, įskaitant TEBEISI turinį.	www.engimvi.it
Veneto lavoro	Tai valstybinė regioninė agentūra, kuri kuruoja visą su darbo rinka susijusį turinį (kursai, pažymėjimai, vietiniai bedarbių darbo centrai ir kt.). Kontaktinis asmuo: Mirco Casteller (atsakingas už gerovės departamentą ir ES projektus; paštas: mirco.casteller@venetolavoro.it).	Veneto regionas per Veneto Lavoro vadovauja „Darbo ir mokymo departamentui“; taigi valdžios institucija, valdanti visas lėšas (t. y. ESF - Europos socialinius fondus) darbuotojams, įmonėms, vadovams ir konsultantams/treneriams. Veneto Lavoro taip pat valdo „RRSP - Repertorio Regionale Standard Professionali“ (regioninė profesinių standartų ir kvalifikacijų duomenų bazė / repertuaras). Veneto Lavoro, kaip viešoji įstaiga, yra svarbiausia suinteresuotoji šalis regioniniu lygmeniu, visų pirma todėl, kad valdo RRSP. Ponas Castelleris yra pagrindinis mūsų kontaktas šiems strateginiams mainams ir diskusijoms. Veneto Lavoro vaidina lemiamą vaidmenį įgyvendinant TEBEISI profilį, visų pirma paskutiniuose projekto etapuose (kai Italijos partneris turi išplatinti kai kurias gaires ir rekomendacijas). Veneto Lavoro, kaip nepriklausoma ir vieša įstaiga, negali tiesiogiai dalyvauti procese; tačiau ji galėtų veikti kaip „viešasis patarėjas“. „Veneto Lavoro“ žingsnis po žingsnio gali patvirtinti mūsų „regioninį prisitaikymo planą“. Tai reiškia, kad mes nuo pat pradžių galėjome informuoti Veneto Lavoro apie projekto eigą ir pabaigoje pasiūlyti šį naują darbo profilį, kuris galėtų būti (dalis) sertifikatas ir įterpti į regioninę profesinių standartų duomenų bazę (RRSP).	www.venetolavoro.it
INAPP - Darbo ministerija	Tai yra naujoji nacionaliniu lygmeniu veikianti agentūra, kuri vykdo ir tikrina visus nacionalinius (ir Europos) projektus, susijusius su kompetencijos vertinimu ir sertifikavimu. Kontaktai: urp@inapp.org (arba kai	Kaip ir anksčiau minėta suinteresuotoji šalis (Veneto Lavoro), INAPP galėtų tvirtai paremti mūsų projektą, keisdamasi ir siūlydama visą pripažinimo procesą. Visų pirma INAPP valdo naują „Atlante del lavoro e delle qualificazioni“ (darbo ir kvalifikacijos atlasas). „Atlas“ yra bendra (nacionalinė) profesinių standartų ir kvalifikacijų duomenų bazė. Ji taip pat apima studentų (aukštųjų mokyklų ir universitetų) profilį ir profesinio mokymo bei mokymo centrų gaires. Neseniai INAPP taip pat pristatė „Atlasą profesionalams“ (pvz.,	www.inapp.org

	kurie konkretūs skyriai, pvz atlante_lq@inapp.org)	konsultantams, instruktoriams, teisininkams ir kt.) Jie turėjo galimybę stebėti projekto eigą „TEBEISI IT Secure and DP manager“ naujų profilių kūrimo laikotarpiu ir eigoje koreguoti ir reklamuokite šį naują profilį. INAPP taip pat galėtų patikrinti projekto turinį būsimo ESF laikotarpiu - Europos socialiniai fondai - nauji mokymo kursai (programa: 2021 m. - 2027 m.), Remiantis TEBEISI rezultatais. INAPP galėtų būti informuotas apie pažangą regioniniu lygiu. Be to, jie galėtų bent jau nacionaliniu lygmeniu įvertinti mokymo medžiagą, visų pirma kompetencijos (dalies) sertifikavimo procesą. NAPP vadovauja dešimtims darbo grupių nacionaliniu lygiu. Šios grupės dažnai veikia regioniniu lygmeniu. Taigi, prieš baigdami projektą, galėtume susitikti ir diskutuoti su kai kuriais grupės nariais, siūlydami jiems regioninį adaptavimo planą.	
AIPSI	Italijos IT saugumo specialistų ir ekspertų asociacija (Associazione italiana dei professisti sicurezza informatica). Tai Italijos ISSA, tarptautinės ne pelno siekiančios profesionalų ir patyrusių praktikų organizacijos, skyrius. Aktyviai dalyvaujant atskiriems nariams ir jų skyriams visame pasaulyje, AIPSI, kaip ISSA skyrius, yra didžiausios ne pelno siekiančios saugumo profesionalų asociacijos, turinčios daugiau nei 13 000 visame pasaulyje, dalis. Kontaktinis asmuo: Yvette Agostini (direktorius, info@aipsi.org)	AIPSI yra viena iš svarbiausių Italijos IT saugumo ekspertų asociacijų. Taaip pat ji veikia ir su duomenų apsaugos valdytojais. Asociacija siūlo platų paslaugų spektrą, naudingą TEBEISI projektui, pavyzdžiui: apklausas ir tyrimus, ataskaitas, mokymus ir konsultacijas ir, žinoma, (dalinį) profesinių profilių vertinimą ir sertifikavimą. Dauguma jų kursų (nemokamai vedami) jau gavo nacionalinės ar regioninės institucijos sertifikatą. Asociacija taip pat yra platesnio tarptautinio tinklo dalis; todėl tai galėtų suteikti mums platesnę viziją ir daugiau informacijos. AIPSI galėtų patikrinti projekto turinį ir vertinimo etapus. Visų pirma, jie galėtų įvertinti kai kurias naujas mokymo medžiagas, pavyzdžiui, tam tikras kompetencijas (pvz., minkštus įgūdžius ar asmeninius įgūdžius). AIPSI turi kelis narius, kilusius iš Veneto regiono (taip pat yra vietinis biuras Venecijoje; dauguma vietinių narių yra informatikos kūrėjai). Su jais galėtume pasikeisti turiniu ir, svarbiausia, patikrinti galutines parengtų dokumentų versijas. Be to, mūsų projektas galėtų susieti „Clusit“ narius (kurie yra profesionalai) su MVĮ. AIPSI jau dalyvauja keliose techninėse darbo grupėse nacionaliniu lygmeniu (ypač Inovacijų ir švietimo ministerijoje) ir keliose regioninėse darbo grupėse. Visų pirma, jų ataskaitos ir publikacijos yra mokslinis pagrindas tolesniam teisėkūros tobulinimui (naujų) darbo profilių pripažinimo srityje. Mūsų regionui vietos AIPSI prezidentas ar direktorius galėtų atstovauti mokslininkams ir technikos ekspertams.	www.aipsi.org
CLUSIT	Italijos asociacija IT saugumui (Associazione Italiana per la sicurezza informatica). „CLUSIT Italy“ buvo sukurta remiantis kitų Europos kompiuterių saugumo asociacijų, tokių kaip „CLUSIB“ (Belgija), „CLUSIF“ (Prancūzija), „CLUSIS“ (Šveicarija) „CLUSIL“ (Liuksemburgas), patirtimi, kuri buvo atskaitos taškas kompiuterių saugumui atitinkamose šalyse. daugiau nei 20 metų. Pagrindinis tikslas: skleisti informacijos saugumo kultūrą įmonėms, viešajam administravimui ir piliečiams. Kontaktinis asmuo: Gabriele Faggioli (Prezidentas; president@clusit.it)	„Clusit“ yra viena iš svarbiausių Italijos IT saugumo ekspertų asociacijų. Tačiau tai veikia ir su duomenų apsaugos valdytojais. Asociacija siūlo platų paslaugų spektrą, naudingą TEBEISI projektui, pavyzdžiui: apklausas ir tyrimus, ataskaitas, mokymus ir konsultacijas ir, žinoma, (dalinį) profesinių profilių vertinimą ir sertifikavimą. Dauguma jų kursų (nemokamai vedami) jau gavo nacionalinės ar regioninės institucijos sertifikatą. „Clusit“ galėtų patikrinti projekto turinį ir vertinimo etapus. Visų pirma, jie galėtų įvertinti kai kurias naujas mokymo medžiagas, pavyzdžiui, tam tikras kompetencijas (pvz., minkštus įgūdžius ar asmeninius įgūdžius). „Clusit“ turi keletą narių iš Veneto regiono (dauguma jų yra informatikos kūrėjai). Su jais galėtume pasikeisti turiniu ir, svarbiausia, patikrinti galutines versijas. Be to, mūsų projektas galėtų susieti „Clusit“ narius (kurie yra profesionalai) su MVĮ. „Clusit“ jau dalyvauja keliose techninėse darbo grupėse nacionaliniu lygmeniu (ypač Inovacijų ir švietimo ministerijoje) ir keliose regioninėse darbo grupėse. Visų pirma, jų ataskaitos ir publikacijos yra mokslinis pagrindas tolesniam teisėkūros tobulinimui (naujų) darbo profilių pripažinimo srityje.	www.clusit.it
Paduvos universitetas	In the last years they made several surveys on project	Paduvos universitetas jau rengia antrojo lygio magistrantus projekto temomis (duomenų apsaugos vadybininkas, IT	www.unipd.it

- informatikos ir kompiuterių inžinerijos katedra.	topics.Contact person: Prof. Antonio Scipioni (scipioni@unipd.it).	saugumo ekspertas ir kt.), Taip pat mokymo kursus. Jų mokymo turinys gali būti naudingi plėtojant kompetencijas ir darbo profilius. Jie galėtų įtraukti vadovus, ekspertus ir MVĮ, pavyzdžiui, rengti interviu, seminarus ir pan. Kaip universitetas jie galėtų „garantuoti“ mokslinį požiūrį ir tinkamas metodikas. Kaip aukštoji mokykla, įvairiose veiklose galėtų dalyvauti keli skyriai (ekonomikos, teisės, IT - informatikos, vadybos ir kt.). Universitetas yra viešoji įstaiga, dalyvaujanti keliuose regioniniuose valdymo komitetuose ir darbo grupėse, įskaitant ekspertų grupes projekto temomis. Taigi, jei jie žino apie projekto eigą, jie galėtų paremti sertifikavimo procesą regioniniu lygiu.	
APCO – Italijos vadybos konsultantų asociacija	Tai Italijos valdymo konsultantų asociacija, įkurta 1968 m. dabar ji turi per 400 narių. APCO nariams siūlo keletą paslaugų, tokių kaip: mokymai, tinklų kūrimo iniciatyvos, lobis su institucijomis ir kt. Kontaktinis asmuo: Cesara Pasini (Presidentas; mail: presidenza@apcoitalia.it)	APCO turi keletą „praktikos bendruomenių“, kurios dirba skirtingos temomis. Visų pirma, dvi iš jų (skaitmeninės transformacijos / inovacijų vadybininkas ir atitikties / ISO standartai) galėtų mums padėti atlikti dalinį sertifikavimą. APCO paskelbė specialų nacionalinį įstatymą (Nr. 4, 2013 m.), kuris pripažino ir konsultantus, kurie nėra įregistruoti profesinėje organizacijoje (pagal įstatymą); bet turi sertifikatą ir nuolatinį mokymą. APCO gali organizuoti kai kuriuos susitikimus (taip pat ir internetu), kai kurie nariai dirba projekto tematikoje. APCO nėra viešoji įstaiga; bet tam tikra „tarpinė“ organizacija, atstovaujanti ir vietos / regioniniams kolektyviniams interesams. Pavyzdžiui, yra „Šiaurės rytų“ grupė (Venetas, Trentino Alto Adige ir Friuli Venezia Giulia regionas), kuri galėtų būti įtraukta į tam tikras projekto veiklas. Vietinė grupė (Veneto regionas, koordinatorius - Paolo Ferrarese) galėtų prisidėti aktyvinant santykius su mūsų vietos valdžios institucijomis (regionu, darbo ir mokymo departamentu).	www.apcoitalia.it

Lentelė 4: Italijos socialiniai partneriai

BDAR Italijoje jau kurį laiką, būtent nuo 2018 m. gegužės 25 d., buvo oficialiai taikomas. Tada, 2018 m. rugsėjo 19 d., įsigaliojo įstatymas, kuriuo Italijos teisės aktai pritaikomi prie Bendrojo duomenų apsaugos reglamento (101/2018 Dekretas).

Italijos BDAR: kur mes esame po trejų metų?

2021 m. birželio mėn. „Privatumo priežiūros institucijos biuras“ paskelbė ataskaitą apie savo veiklą per trejus reglamento įgyvendinimo metus ir paaiškėjo, kad duomenų subjektai tapo labiau informuoti apie savo teises. Buvo išnagrinėti 27 192 skundai ir pranešimai apie pažeidimus (BDAR 2020). Didelis pranešimų skaičius, maždaug 24 per dieną, 365 dienas per metus trejus metus, rodo, kad priėmus BDAR tikrai padidėjo duomenų subjektų informuotumas apie jų teisių egzistavimą ir prašymą jų apsaugos.

Praėjusių metų ketvirtį nuo 2021 m. sausio 1 d. iki kovo 31 d. pranešimų skaičius išaugo iki 2839, o tai rodo, kad pandemijos metu, kai skaitmenizuojama daug veiklos, taip pat padidino vartotojų dėmesį asmens duomenų apsaugos klausimams.

Buvo gauta 3873 pranešimai apie duomenų pažeidimus (apie 3,5 per dieną), o tai yra nedaug, palyginus su statistika apie kibernetines atakas, tačiau tai rodo, kad svarbu priimti saugumo politiką ir priemones, padedančias jų išvengti. Bet kuriuo atveju esminis aspektas yra darbuotojų mokymas ir informuotumo didinimas saugumo klausimais ir elgesys, kurio reikia imtis, jei prašymai neatitinka įmonės procedūrų. 59 838 duomenų apsaugos pareigūnų (dar žinomų kaip DAP) pavardės buvo paskelbtos, o ne visų - viešosios administracijos, kurios pagal reglamentą privalo paskirti DAP. Kalbant apie sankcijas, Europoje buvo pravestos 654 bylos, kurių bendra suma buvo

283 757 083 eurai. Žvelgiant į statistiką pagal šalis, Italija užima pirmąją vietą pagal skirtą sankcijų, 76 298 601 EUR už 79 priemones, sumą, patvirtinančią, Italijos „Garante“ veiklą ir dėmesį, kuriuo sprendžiami skundai ir pranešimai. Skaičiuojant žinoma, atsižvelgiama tik į sankcijas, nustatytas pagal BDAR 83 straipsnį, ir neatsižvelgiama į tai, kokia žala ar kompensacija yra sumokėta duomenų subjektams, kurių teisės buvo pažeistos. Kaip ES priežiūros metinių proga sakė priežiūros institucijos nariai, dar reikia daug nuveikti, kad valstybių narių skaitmeninimas būtų sujungtas su saugiu infrastruktūros valdymu. Padidėjęs įmonių pažeidžiamumo perimetras dėl daugiau ar mažiau priverstinio nuotolinio darbo sprendimų priėmimo reikalauja, kad savininkai permąstytų duomenų srautus ir saugumo procedūras savo organizacijose.

Bet ką tai reiškia mūsų šalies verslui? Laimei, tendencija atrodo teigiama. Praėjus beveik dvejiems metams po visiško Reglamento taikymo, Italijoje padaryta didelė pažanga, kad būtų laikomasi reglamento, didėja organizacijų turimas biudžetas ir auga branda, projektų konkretumas ir tiksliniai organizaciniai pokyčiai.

Tačiau dėl dalyko sudėtingumo ir svarbos įmonės turi nuolat stengtis prisitaikyti prie duomenų apsaugos teisės aktų nustatytų principų ir reaguoti į valdžios institucijų prašymus. Šiuo atžvilgiu pirmosios baudos už reglamento pažeidimus buvo skirtos keliose Europos šalyse. Italijoje, priešingai, priežiūros institucijos požiūris iš pradžių buvo palankus, taip pat ir dėl to, kad vėluojama išrinkti naują priežiūros institucijos kolegiją. Tačiau pastaruoju laikotarpiu sustiprėjo tikrinimai bei buvo taikomos pirmosios sankcijos, numatytos vietos ir tarpvalstybiniuose duomenų apsaugos teisės aktuose. Kibernetinio saugumo ir duomenų apsaugos observatorijos atliktų tyrimų dėka galime pamatyti, kaip šie teisės aktai keičia Italijos kontekstą.

Italijos BDAR laikymosi būklė

Siekdama ištirti Italijos bendrovėse vykstančius duomenų apsaugos pokyčius, Observatorijos leidinys apsvarstė keturis aspektus:

- atitikties projektų būklė
- skirtas biudžetas
- įgyvendinti veiksmai
- kritinės problemos

Tyrimas rodo, kad beveik visos Italijos įmonės įgyvendino arba ištobulino BDAR atitikties projektus. Daugiau nei pusė organizacijų teigė, kad laikosi teisės aktų reikalavimų, o tuo pačiu sumažėjo įmonių, kurios teigė nežinančios BDAR pasekmių, skaičius.

Tačiau dėl pastarojo reikia pažymėti, kad tai yra įmonės, kuriose duomenų apsaugos klausimas dar nepasiekė aukščiausio lygio, tačiau vis dėlto yra žinomas tokios specializuotos funkcijos kaip IT saugumas, teisinis aspektas ir atitiktis. Kitas teigiamas BDAR brandos ir žinomumo požymis Italijoje yra mažas procentas įmonių (5%), kurios dar tik analizuoja reikalavimus ir rengia atitikties planus, o prieš dvejus metus ši dalis

siekė 34%. Vaizdas taip pat teigiamas atsižvelgiant į biudžetą, skirtą BDAR laikymosi priemonėms: 45% Italijos įmonių padidino savo biudžetą. Nors šis skaičius teigiamas, taip pat tiesa, kad dėmesys dar turi būti nukreiptas į konkrečią veiklą, pavyzdžiui, periodinius auditus, procedūrų atnaujinimą ir saugumo bei duomenų apsaugos technologijas. (Andrea Antonelli 2020)

DPR atitikties veiksmai

Ką konkrečiai daro Italijos įmonės, siekdamos laikytis BDAR? Reikėtų prisiminti, kad atitikties procesas būtinai turi būti sudarytas iš kelių etapų, kurie šiuo metu yra skirtingi:

- Duomenų apdorojimo registro sukūrimas (85%): privalomo registro, kuriame būtų galima sekti visas atliktas apdorojimo operacijas, sukūrimas;
- Vaidmenų ir pareigų nustatymas (81%): visų už duomenų tvarkymą atsakingų asmenų nustatymas ir sutarčių sudarymas;
- Formų keitimas (76%): formų atnaujinimas pagal BDAR reikalavimus;
- Pranešimo apie duomenų pažeidimą procedūra (68%): pranešimo priežiūros institucijai apie konfidencialių duomenų pažeidimus procesas;
- Saugumo politikos apibrėžimas ir rizikos vertinimas (66%): priemonių, skirtų užtikrinti, kad tvarkymas atitiktų reglamentą, patvirtinimas;
- Poveikio duomenų apsaugai vertinimas (56%): privalomas poveikio duomenų apsaugai vertinimas (PPDA), kai apdorojimas gali kelti didelę riziką duomenų subjektų teisėms ir laisvėms;
- Duomenų subjektų teisėms įgyvendinti skirtų procesų įgyvendinimas (54%): veiksmai, kuriais siekiama užtikrinti duomenų subjektams suteiktas tvarkymo tvarkos suteiktas teises. (Antonelli A., 2020)

Be šių veiksmų, taip pat būtina apsvarstyti duomenų apsaugos pareigūno (DAP) pareigybės įtraukimą į įmones. Šis skaičius, kurio paskyrimą daugeliu atvejų numato BDAR, yra 65% organizacijų. Šis skaičius neabejotinai teigiamas, nes parodo, kad padaugėjo įmonių, įvedusių šias pareigas

Kokias svarbias problemas susijusias su BDAR įgyvendinimu patiria Italijos įmonės?

Jei tiesa, kad Italijos BDAR laikymosi būklės vaizdas apskritai yra teigiamas, tai taip pat tiesa, kad organizacijos susidūrė su tam tikrais sunkumais. Tiesą sakant, daugelis įmonių vis dar patiria sunkumų organizaciniu požiūriu, pavyzdžiui, nustatydamos vaidmenis ir pareigas įmonėje, o kitos praneša apie labai sulėtėjusią kasdienę veiklą.

Tačiau šie neigiami elementai yra mažai svarbūs, palyginti su brandžiu scenarijumi, kai Italijos bendrovės rodo, kad yra ne tik orientuotos į iššūkius, susijusius su duomenų apsauga, bet ir žino visas problemas.

2.5 Lietuva

Įstaigos pavadinimas	Trumpas aprašymas	Pagrindinis tikslas	Tinklapis
Alytus Business Consulting Centre (AVKC)	Alytaus verslo konsultacijų centras (AVKC) yra pirmasis verslo konsultacijų centras Lietuvoje, įregistruotas 1993 m. gegužės 13 d. kaip ne pelno organizacija, vėliau perregistruota kaip viešoji įstaiga. Alytaus verslo konsultacijų centras - Alytaus regioninės plėtros strategijos tarptautinio vystomojo bendradarbiavimo regioninės plėtros srityje dalyvis, aktyviai bendradarbiaujantis su Švedijos Jonkompingo apskritimi, Lenkija, Danija, Vengrija, Italijos regionų valdžios institucijomis, esamų verslo plėtros agentūrų ministerija, Alytaus apskrities savivaldybėmis ir susijusiomis struktūromis.	Alytaus verslo konsultacijų centro misija-skatinti ir plėtoti smulkų ir vidutinį verslą, teikiant verslo mokymus, konsultacijas, informaciją, naujas verslo plėtros iniciatyvas kuriant ir įgyvendinant tinklų plėtrą Alytaus regione. Asociacijos tikslas - padėti išspręsti visų grupių žmonių socialinės globos vartotojų problemas, gerinant jų kokybę ir integraciją į visuomenę.	https://www.avkc.lt/lt/
Savivaldybių socialinės rūpybos įstaigų vadovų asociacija	Savivaldybių vadovų asociacija Socialinės rūpybos įstaigos - nepriklausoma, savanoriška ne pelno organizacija, kurią sudaro 30 savivaldybių globos įstaigų	Asociacijos tikslas - padėti išspręsti visų grupių žmonių socialinės globos teikimo problemas, gerinant jų kokybę ir integraciją į visuomenę.	http://ssgivasociacija.blogspot.com/
Advokatų kontora ALIANT Tarvainyte Vilys Bitinas	ALIANT® komanda Lietuvoje teikia integruotas teisines paslaugas visuose verslo valdymo ir plėtros procesuose bei verslo ginčuose nacionalinėse ir tarptautinėse teismų institucijose. Jie taip pat dirba duomenų apsaugos srityje	ALIANT® komanda Lietuvoje teikia integruotas teisines paslaugas visuose verslo valdymo ir plėtros procesuose bei verslo ginčuose nacionalinėse ir tarptautinėse teismų institucijose.	https://www.aliantlaw.lt/
LDAPA - Lietuvos duomenų apsaugos pareigūnų asociacija	LDAPA jungia narius, siekiančius sukurti naujovišką, naujos kartos nekomercinę platformą, skirtą asmens duomenų apsaugos specialistams dalytis specializuotomis teisinėmis žiniomis, gerąja patirtimi, praktine ir naujovėmis	LDAPA narių prioritetas yra sukurti naujovišką, naujos kartos nekomercinę platformą, skirtą asmens duomenų apsaugos specialistams dalytis specializuotomis teisinėmis žiniomis, gerąja patirtimi, praktine ir nauja	https://ldapa.lt/
Informacijos Saugumo Centras	Siekiant Centro veiklos tikslų, su duomenų valdytojais ir duomenų tvarkytojais konsultuojamasi dėl tinkamų techninių ir organizacinių duomenų apsaugos priemonių įgyvendinimo. Duomenų subjektai tariasi dėl žmogaus teisių įgyvendinimo duomenų apsaugos srityje.	Informacijos saugumo centro tikslas - gerinti visuomenės sąmoningumą saugaus asmens duomenų tvarkymo, informacijos apsaugos ir kibernetinio saugumo klausimais.	https://infosec.mobi/

Lentelė 5: Lietuvos socialiniai partneriai

Lietuvos Respublikos smulkaus ir vidutinio verslo plėtros įstatyme (2017) nurodyta, kad smulkaus ir vidutinio verslo subjektai yra vidutinės, mažos ir labai mažos įmonės, atitinkančios tam tikrus reikalavimus (darbuotojų skaičius, pajamos, nepriklausomumas) ir fiziniai asmenys, turintys teisę dirbti savarankiškai. komercinė ir kita panaši veikla. Per 2019 metus mažų ir vidutinių įmonių padaugėjo 0,4 proc. (registruotas 11153). Didžiausią dalį - 83% - MVĮ sudarė labai mažos įmonės (0–9

darbuotojai). Mažos įmonės sudarė 14% (10–49 darbuotojai), vidutinės įmonės (50–249 darbuotojai) - 3% 2019 m. Per metus mažų ir vidutinių įmonių skaičius padidėjo 2,2%.

Nepaisant pažangos smulkaus ir vidutinio verslo sektoriuje, gerinant bendrą verslo aplinką ir mažinant kliūtis patekti į rinką, verslumo dinamika Lietuvoje tebėra silpna. Naujų įmonių steigimo administracinės procedūros yra sudėtingos, o verslininkams trūksta pradinio kapitalo ir valdymo bei finansinių įgūdžių, rinkodaros ir eksporto įgūdžių bei informacijos. Sprendimai įveikti pandeminę krizę, paskatinti ekonomiką ir pagerinti verslo aplinką yra sunkiai įgyvendinami ir neduoda laukiamų rezultatų.

„TebeISi“ projekto tyrimai Lietuvoje rodo, kad šiam klausimui skiriama per mažai dėmesio. Nepakankamas dėmesys skiriamas viešajam sektoriui ir mažoms bei vidutinėms įmonėms. Dėmesio trūkumas susijęs su finansavimo trūkumu. Didesnį dėmesį informacijos saugumui skiria visuomenės dalis, kuri vienaip ar kitaip susiduria su informacijos saugumu. Pasak ekspertų, daug dėmesio skiriama valstybės institucijoms. Kalbant apie verslą - dėmesys yra mažiau reikšmingas, nes nedaugelis žmonių iki galo supranta šią problemą. Visuomenės dėmesys informacijos saugumui taip pat didėja stebint viešojo saugumo incidentus. Tyrimai rodo, kad MVĮ nepakankamai dėmesio skiria mokymams viduje. Paprastai tai priklauso nuo pačių darbuotojų iniciatyvos surasti mokymus ir juose dalyvauti. Pastaruoju metu ekspertai taip pat susiejo mokymo trūkumą su sunkia COVID-19 pandemijos situacija, kai daugelis įmonių buvo sustabdytos ir daugiausia dėmesio skyrė išlikimui.

M. Lipinskienes atliktas kiekybinis tyrimas (2019) apie Bendrojo duomenų apsaugos reglamento įgyvendinimą Lietuvos įmonėse atskleidė, kad apklausoje dalyvaujančios įmonės Lietuvoje, kurios pačios tvarko asmens duomenis ir patikėjo duomenų tvarkymą duomenų tvarkytojui, pakankamai atitinka BDAR. Anketinės apklausos metu respondentai atsakė į teiginį: „mano atstovaujama įmonė efektyviai įgyvendino BDAR reikalavimus“ nuo 1 „visiškai nesutinku“ iki 100 „visiškai sutinku“. Atsakymai buvo koduojami SPSS programoje intervalų skalėje ir apskaičiuotas vidutinis respondentų balas. Iš viso į klausimyną atsakė 77 respondentai, žemiausias įvertinimas-0, aukščiausias-100, o vidutinis balas-77 balai, kas reiškia „sutinku“. Respondentai dažniausiai savo įmones įvertino 100 balų - 23 respondentai, 8 respondentai - 95 balais, 6 - 90 balų, 7 - 85 balų, 6 - 80 balų. Iki 80 balų atsakymai įvertinami „visiškai sutinku“, o tai reiškia, kad visiškai laikomasi BDAR. Iš 77 respondentų tokių įmonių buvo 50, tai yra 65 proc. Daugiau nei pusė bendrovių atstovų sutinka su teiginiu, kad bendrovė atitinka BDAR standartą kaip „visiškai sutinkanti“.

Apklausa atskleidė, kad respondentų nuomone, reglamentas yra gana abstraktus, lakoniškas, sunkiai skaitomas ir sunkiai suprantamas ne teisininkams. Įmonėms, kurios pačios tvarko duomenis, trūksta žinių ir supratimo apie BDAR, o tai sukelia nežinojimą ir dvejones. Tačiau mokymai įmonėje yra svarbūs ir reikšmingi kiekvienam įmonės darbuotojui ir pačiai įmonei. Kad atitiktų BDAR, duomenų valdytojas turi išsiaiškinti, kokie asmens duomenys yra saugomi, kur, kokiu tikslu, kiek laiko, kaip jie tvarkomi ir saugomi. Tik suprasdamas, ką turi, duomenų valdytojas žinos, kaip elgtis ir valdyti. Tai patvirtino „TebeISi“ projekto tyrimo tyrimas (IQ1), duomenų apdorojimas ir

asmens duomenų apsaugos vertinimai, kaip galimybė nustatyti perteklinę informaciją ir peržiūrėti verslo procesus. Tokiu būdu įmonėse būtų atpažįstami efektyvūs verslo procesai, sumažėtų arba būtų panaikinti neefektyvūs ir pertekliniai proceso etapai. Tai padėtų įmonėms užtikrinti informacijos saugumą ir asmens duomenų apsaugą.

Mokymų situacija

Lietuvoje duomenų ir informacijos saugumo mokymai (nuo 1,5 val. iki kelių dienų) yra labai įvairūs. Dažniausiai mokymus rengia privačios institucijos, pvz: Kibernetinio saugumo akademija, įkurta UAB "Hermitage Solutions", kurios tikslas - parengti IT specialistą, gebantį laiku ir efektyviai spręsti sudėtingus kibernetinio saugumo klausimus ir įvertinti savo organizacijos IT infrastruktūros pažeidžiamumą. UAB "Atea", kuri yra pirmaujanti IT sprendimų ir paslaugų tiekėja Baltijos šalyse ir padeda klientams specializuotomis kompetencijomis, produktais, paslaugomis ir sprendimais IT infrastruktūros, programinės įrangos kūrimo ir saugumo srityse. NRD Cyber Security, kuri yra kibernetinio saugumo technologijų konsultavimo, reagavimo į incidentus ir taikomųjų tyrimų bendrovė. Bendrovė daugiausia dėmesio skiria paslaugoms specializuotiems viešųjų paslaugų teikėjams (teisėsaugos institucijoms, nacionalinėms CERT, telekomunikacijų, nacionalinėms ryšių reguliavimo institucijoms, nacionalinei ypatingos svarbos infrastruktūrai), finansų pramonei ir korporacijoms, kurių duomenys yra labai jautrūs. UAB "Kompetencijų ugdymas", kurie siūlo mokymus, skirtus pasirengti populiariausiems sertifikatams, kurių pagrindu galima dirbti su kitų gamintojų įranga, todėl šiuos sertifikatus dažnai renkasi darbdaviai ne tik Lietuvoje, bet ir užsienyje.

Informacijos saugumo mokymai organizuojami įvairioms tikslinėms grupėms: tiek pradedantiesiems, tiek pažengusiems IT naudotojams, tiek IT specialistams. Pagrindinės informacinių mokymų temos: "Informacijos saugumo mokymai"; "Kibernetinio saugumo mokymai"; "Informacijos saugumo mokymai neprofesionalams". Atskira informacijos saugumo mokymų grupė skirta IT profesionalams. Jie mokomi tokiomis temomis: "Informacinės saugos mokymai: "Kibernetinio saugumo pagrindai"; "Įsilaužimas į IT, siekiant apginti IT"; "Etinis įsilaužėlis praktikas"; "Saugus programavimas"; "IT saugumo praktikas"; "Kibernetinio saugumo incidentų valdymas" ir "Informuotumo apie IT saugumą mokymai".

Įvairaus lygio profesiniai mokymai duomenų apsaugos temomis dažniausiai skirti IT specialistams. Pagrindinės tokių mokymų temos yra susijusios su asmens duomenų apsaugos pagal BDAR reikalavimus mokymais. Taip pat organizuojami mokymai duomenų saugumo temomis įmonių teisininkams, administratoriams, vadybininkams, personalo vadovams. Tokiuose mokymuose supažindinama su BDAR; "Asmens duomenų apsauga ir atsakomybė už BDAR pažeidimus"; "Asmens duomenų apsauga ir asmens duomenų teisės aktų pažeidimai 2018 m."

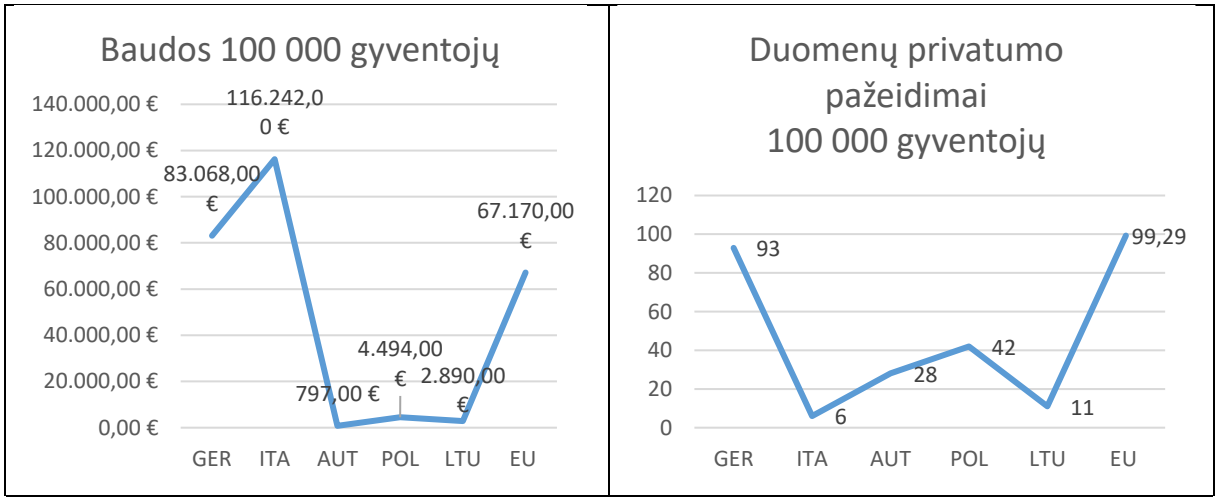
2.6 BDAR ir ekonominė veikla

2018 m. pradėjusi taikyti BDAR, Europos Komisija nustatė nuoseklias gaires, užtikrinančias pagrindinę teisę į duomenų apsaugą ir suteikiančias pagrindą įgyvendinti Europos Sąjungos pagrindinių teisių chartiją. Bendrasis duomenų apsaugos reglamentas paskatino daugelį kitų pasaulio šalių imtis aktyvaus duomenų apsaugos reglamentavimo ir sekti ES keliu bei daryti įtaką visų suinteresuotųjų šalių pozicijai ir elgesiui Europos piliečių labui.

Vis dėlto priimant Europos duomenų strategiją (Europos Komisija 2020a) susiduriama su keliomis kliūtimis, apie kurias Europos Komisija pranešė komunikate dėl BDAR įgyvendinimo (Europos Komisija 2020b). Tuo tarpu bendras piliečių supratimas apie asmens duomenų vertę padidėjo, o procesinės teisės sustiprino galimybę pranešti apie netinkamo elgesio atvejus, ypač tarpvalstybinio duomenų naudojimo srityje. Šiuo atžvilgiu turi būti išnagrinėta teisė į duomenų perkeliamumą iš vienos tarnybos į kitą viešųjų gėrybių naudojimo labui ir atskleisti ribojantys veiksniai. (European Commission 02.06.2020).

Kalbant apie MVĮ poreikius, BDAR padidino laisvo duomenų judėjimo galimybes ES viduje ir pagerino duomenų judėjimą su ES nepriklausančiomis įmonėmis, taip skatindamas inovacijas ir ekonominę veiklą. Tačiau MVĮ, norėdamos pasinaudoti šiomis naujomis galimybėmis, turi susidoroti su gana sudėtingu BDAR įgyvendinimu, nes duomenų apsaugos pažeidimų rizika nemažėja priklausomai nuo įmonės dydžio. Todėl reikia dėti daugiau pastangų, kad MVĮ būtų suteikta praktinė ir lengvai naudojama priemonė. Komisija siekia remti būtent MVĮ, pateikdama sutarčių ir nuostatų, atitinkančių BDAR, šablonus.

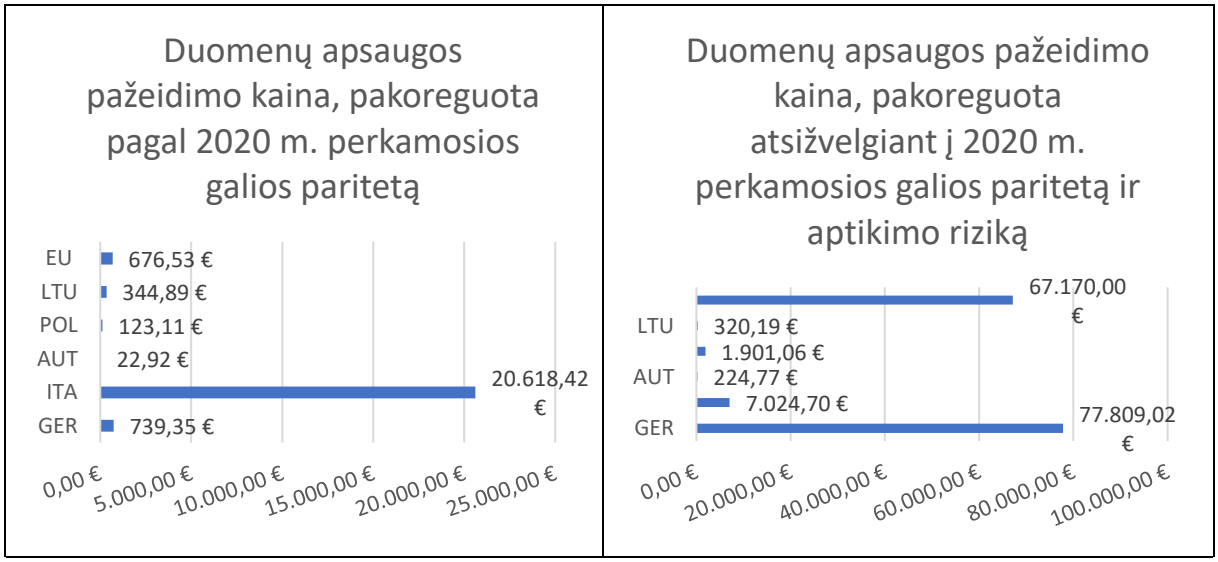
Sėkmingą įgyvendinimą galiausiai atspindi sėkmingas nacionalinių duomenų apsaugos institucijų vykdymas. Kaip matyti 6 paveiksle, tarp valstybių narių pastebimi dideli skirtumai.



Pav. 9: Duomenų apsaugos teisės aktų vykdymas valstybėse narėse. Grynosios vertės 100 000 gyventojų.

Šaltinis: heyData (2021). Sudaryta autoriaus

Tuo tarpu visose šalyse bendras duomenų saugumo pažeidimų skaičius, tenkantis 100 000 gyventojų, išlieka mažesnis už ES vidurkį, kuriame dominuoja Airijos (245), Danijos (325) ir Nyderlandų (382) duomenys, tačiau pastebimi dideli sumokėtų baudų šuoliai. Siekiant geriau suprasti sumokėtų baudų ir pažeidimų skaičiaus santykį, grynosios vertės buvo pakoreguotos pagal perkamosios galios paritetą[2] užtikrinti šalių palyginamumą. Rezultatai rodo, kad Vokietijos aptikimo rodiklis yra artimas ES vidurkiui, o Italijoje, Austrijoje, Lenkijoje ir Lietuvoje – gerokai mažesnis. Panašios išvados pastebimos ir kalbant apie sumokėtas baudas, išskyrus Italiją, kur sumokėtos baudos beveik dvigubai viršija Europos vidurkį ir maždaug 40 proc. viršija baudas Vokietijoje. Šis smaigalys paskatino atlikti tolesnę analizę, apskaičiuojant duomenų saugumo pažeidimo išlaidas, pakoreguotas pagal perkamosios galios paritetą 7 pav. (kairėje), ir vėl pagal aptikimo riziką, o vidutinis rizikos lygis buvo apskaičiuotas nustačius, kad ES vidutinė vertė yra 1.



Pav. 10: Duomenų apsaugos pažeidimų kaina, pakoreguota atsižvelgiant į perkamosios galios paritetą ir aptikimo riziką

Šaltinis: heyData (2021). Sudaryta autoriaus.

Tuo tarpu, kiekvienu atveju, apie kurį pranešta, Italijoje stebimas itin didelis šuolis, o rizikos koregavimas aiškiai parodo, kad tai yra labai nedaug atvejų, kai skiriama didelė bauda. Vis dėlto matyti, kad duomenų apsaugos pažeidimų rizikos ir sąnaudų apskaičiavimas labai skiriasi: Austrijoje, Lietuvoje ir Lenkijoje skiriamos tik nedidelės bausmės, o Vokietijoje – griežtos bausmės. Todėl galima daryti išvadą, kad teisėsaugai dar teks nueiti ilgą kelią, kol ji bus vienodai veiksminga visose valstybėse narėse.

Atsižvelgiant į individualią situaciją šalyse partnerėse, ypač MVĮ, įgyvendinimo proceso iššūkiai tampa akivaizdūs. Kaip pagrindinės lėto įgyvendinimo priežastys įvardytos laiko ir išteklių trūkumas. Visose šalyse MVĮ turi galimybių tobulinti procesus ir BDAR svarbios informacijos kontrolę įmonėje. Galiausiai, tinkamo įgyvendinimo klausimas yra glaudžiai susijęs su personalo prieinamumu ir į praktiką orientuotų mokymo kursų

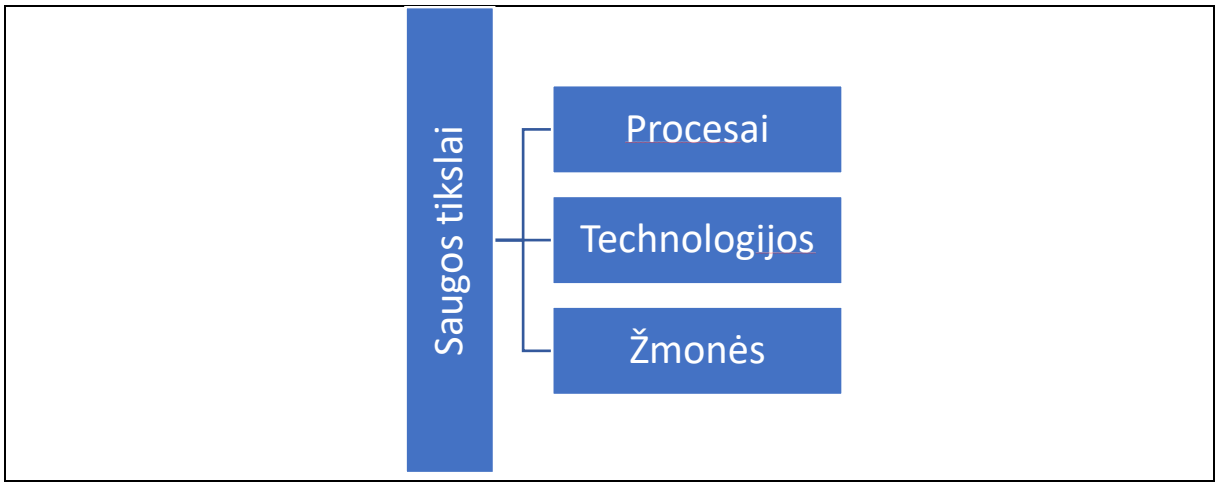
[2] Duomenys paimti iš Eurostato 2021.

poreikiu. Didelė kvalifikacijos kėlimo kursų (tiek savanoriškų, tiek privalomų) paklausa parodė, kad rinkoje trūksta glaustų, perkeliamų ir skaidrių kursų, kaip siūloma TeBeISi mokslinių tyrimų darbotvarkėje.

2.7 Silpniausia grandis – darbuotojų vaidmuo ir privatumo skaičiavimas

Atsižvelgiant į įmonių, nevyriausybinių organizacijų ir valdžios institucijų pastangas įgyvendinti BDAR, sėkmingas įgyvendinimas susiduria su tais pačiais apribojimais, kaip ir informacijos saugumo srityje: žmogiškuoju veiksniu. Kaip parodyta 2.6 skyriuje, egzistuoja didelis personalo ir ypač kvalifikacijos tobulinimo kursų poreikis. Darbuotojai, kurie yra pagrindinė informacijos praradimo ir duomenų apsaugos pažeidimų priežastis, atlieka pagrindinį vaidmenį vykdant duomenų apsaugą ir informacijos saugumą bei užtikrinant jų laikymąsi.

Įmonės turi daug galimybių užtikrinti savo duomenų apsaugą tiek organizaciniu, tiek techniniu lygmeniu. Organizaciniu požiūriu jos gali įdiegti procesus, kuriais užtikrinama, kad būtų renkamas tik nedidelis duomenų kiekis, kad fizinės ir skaitmeninės saugyklos būtų apsaugotos, kad prieiga prie duomenų būtų suteikta tik atitinkamiems darbuotojams ir pan. Šių priemonių analizė ir įgyvendinimas priklauso informacijos saugumo pareigūno kompetencijai kartu su įmonės vadovu ir jo palaikomi.



Pav. 11: Rizikos saugumo matmenys

Techniniu lygmeniu galima kurti programas ir taikomąsias programas, kurios užtikrintų atitiktį duomenų apsaugos teisės aktams ir konkrečioms įmonės nuostatoms, t. y. privatumą projektuojant. Paslaugų teikėjai pradėjo kurti verslo modelį iš programinės įrangos kaip paslaugos (SaaS) platformų, įgyvendindami privatumą kaip paslaugą (PaaS). Tokiu būdu, gavus naudotojo sutikimą, informacijos saugojimas ir tvarkymas orientuotas į tinkamą elgesį pagal individualų reikalavimą. Be to, pastaraisiais metais labai išaugo saugios programinės įrangos svarba, nes informacijos nutekėjimas tampa lengviau žinomas visuomenei ir gali pakenkti įmonių reputacijai. Todėl įmonės susidomėjo saugios programinės įrangos kūrimu ir vartotojų pasitikėjimo stiprinimu - tai suteikia konkurencinį pranašumą rinkoje.

Galiausiai, saugodamos savo praktinę patirtį ir svarbius duomenis, įmonės turi atsižvelgti į žmogiškąjį aspektą. Tai įmonės naudotojas ir veikėjas, valdantis mašinas ir technologijas, atliekantis užduotis ir prižiūrintis procesus. Tuo tarpu tiek technologijos, tiek procesai pasižymi labai dideliu patikimumu, darbuotojai linkę klysti, nes jiems galioja "ribotas racionalumas" (Simon 1990). Iš tikrųjų apie 88 % duomenų

pažeidimų ar informacijos praradimo atvejų galima priskirti žmogiškoms klaidoms, todėl šis aspektas yra svarbiausias siekiant užtikrinti duomenų saugumą įmonėje. (Tessian 2021)

Trumpai tariant, riboto racionalumo sąvoka atmeta prielaidą, kad žmonių mąstymas, elgesys ir veiksmai grindžiami visišku racionalumu, nes tam reikėtų neribotų pažintinių gebėjimų nedelsiant apdoroti visą turimą informaciją ir priimti visapusiškai pagrįstus sprendimus. Vietoj to daroma prielaida, kad žmonės maksimizuoja savo individualų naudingumą, t. y. pasirenka veiksmą, kuris labiausiai tenkina jų pačių suvoktą poreikį (vadinamasis "pasitenkinimas"). Galiausiai žmogus taip pat gali prieiti prie išvados, kad jam trūksta informacijos sprendimui priimti, tačiau šios informacijos paieška pareikalautų daug laiko ir energijos. Todėl asmuo nusprendžia imtis veiksmo turėdamas neišsamią informaciją, nes alternatyviosios sąnaudos (laiko ir energijos) viršija tos konkrečios informacijos turėjimo naudingumą.

Tarp tokių veiksmų - lengvų slaptažodžių nustatymas (arba jų užrašymas ant lapelio), saugumo atnaujinimų atidėliojimas, neskelbtinos informacijos laikymas spintelėse, lifte rastos lazdelės naudojimas - tai tik keletas neapgalvotų pasekmių. Išsamios informacijos neturėjimas ir tariamos didelės alternatyvios sąnaudos skubėjimo ir spaudimo akimirkomis vis dažniau išnaudojamos socialinės inžinerijos atakose, kai įsilaužėlis paštu ar telefonu sukuria scenarijų, kuris skatina skubiai imtis veiksmų, tikintis, kad darbuotojas paliks nuošalyje saugumo protokolus ir savanoriškai pateiks svarbią informaciją (pvz., slaptažodžius, finansinę informaciją ir pan.).

Deja, tinkamo elgesio laikymasis kasdieniame darbe reikalauja papildomų energijos sąnaudų, kurios produktyvioje ar įtemptoje darbo aplinkoje dažnai yra ribotas išteklius. Esant nusistovėjusiai darbo tvarkai, keisti požiūrį, įsitikinimus ir galiausiai elgesį yra didelis iššūkis ne tik įmonei, bet ir jos darbuotojams. Iki šiol kaip niekad svarbu mokyti, darbuotojus, siekiant didinti jų sąmoningumą dėl nuolatinės grėsmės vertingiausiam įmonės turtui - jos praktinei patirčiai ir duomenims. Mažėjant sunkumams pradėti bet kokią ataką, vis daugiau MVĮ turi susidurti su nauja realybe: jos jau patiria arba greičiausiai patirs tikslinių atakų. Taigi, ką galima padaryti?

3 TeBeISi strategija

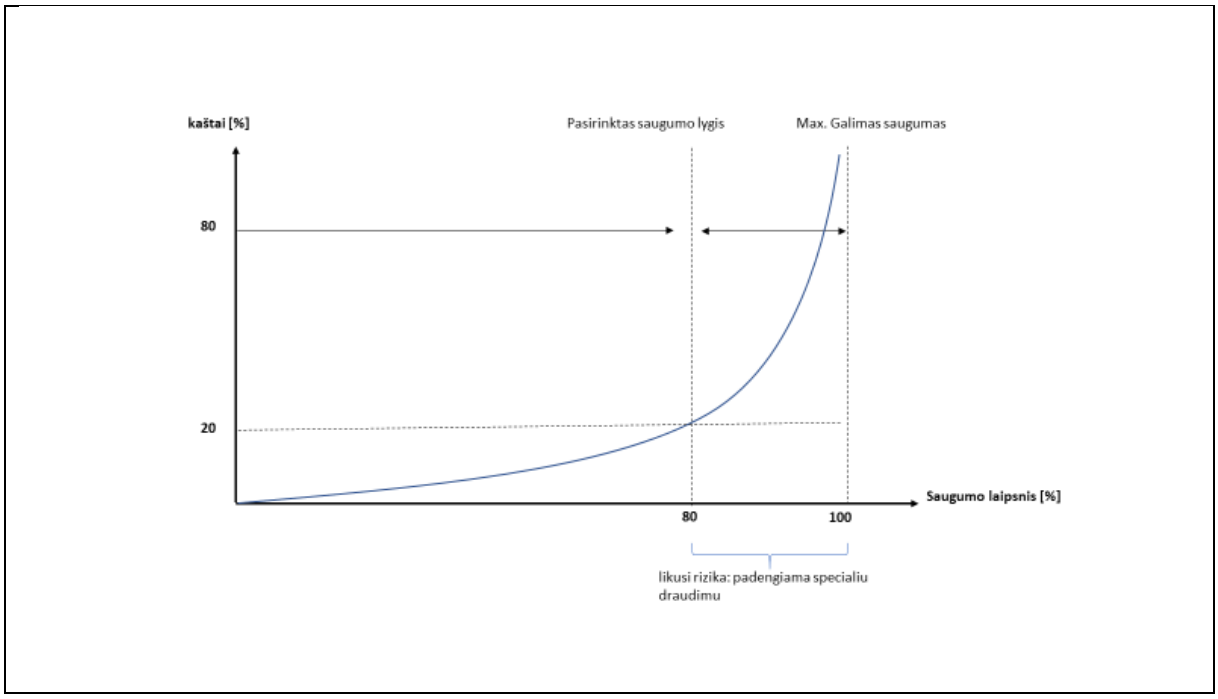
Vykdant projektą "TeBeISi" išanalizuota informacijos saugumo situacija atsižvelgiant į BDAR įgyvendinimą įmonėse valstybėse narėse partnerėse. Peržiūrėjus šiuo metu egzistuojančius pareigybių profilius, formalias kvalifikacijas ir sertifikavimą, buvo atliktas šiuo metu egzistuojančių, perkeliamų kompetencijų ir kiekybinės bei kokybinės analizės metu nustatytų reikalavimų atitikimas.

3.1 Aukštojo mokslo ir profesinio mokymo sąsajos

Peržiūrėjus visą kiekybiniais ir kokybiniais tyrimais grįstą informaciją, padaryta išvada, kad informacijos saugumas yra numatytas kaip profesinio mokymo ir aukštojo mokslo derinys. Šią mintį pagrindžia trys priežastys:

1. Operatyvinė veikla. Daugelis užduočių, kurias reikia atlikti MVĮ, yra gana rutininio pobūdžio. Žinių perdavimo ir rekontekstualizavimo lygis išlieka žemas, nes technologijos ir procesai išlieka standartizuoti, įmonės naudojasi standartizuota EDA (angl. *Electronic data processing*) programine įranga ir ryšių kanalais. Dauguma MVĮ gali gerokai padidinti savo saugumo lygį laikydamosis 20:80 taisyklės (ar panašios) - 80 proc. saugumo jos pasiekia atlikdamos 20 proc. darbo, reikalingo 100 proc. saugumui pasiekti. Žinoma, tai neįmanoma atsižvelgiant į duomenų apsaugą, kuri yra privaloma pagal įstatymą ir dėl kurios įmonės privalo laikytis BDAR reikalavimų. Šios išvados pasekmės yra įvairios: įmonės turi atsižvelgti į tai, ar jos nori siekti konkretaus sertifikavimo (dėl savo produkto pobūdžio, rinkos reikalavimų ir t. t.), ar turi išteklių, kuriems reikia daugiau nei įprastų apsaugos priemonių, ir pan. Taigi MVĮ dažnai atsiduria tokioje padėtyje, kai struktūrinis pagrindinių apsaugos priemonių laikymasis leidžia gerokai padidinti bendrą saugumo lygį ir gerokai sumažinti rizikos poveikį ekonomiškai efektyviu kompromisu.

2. Teisiniai įsipareigojimai. Kai kurie informacijos saugumo aspektai taip pat susiję su teisiniais aspektais, ypač su tinkamu duomenų tvarkymu pagal Bendrąjį duomenų apsaugos reglamentą (BDAR). Dėl darbo su nacionaliniais teisės aktais sudėtingumo atsakingi darbuotojai privalo turėti kompetencijos, susijusios su teisės aktais ir teisingu jų įgyvendinimu. Ši atsakomybė susijusi su gebėjimu rekontekstualizuoti ir perduoti abstrakčias žinias darbo aplinkoje. Tuo tarpu 1 punkte aprašyto techninio informacijos saugumo aspekto sudėtingumo laipsnis išlieka prižiūrimas, o teisinis aspektas reikalauja kruopštaus mokymo ir vykdymo, kad būtų laikomasi atitinkamų teisės aktų.



Pav. 12: Investicijų į informacijos saugumą sąnaudų ir saugumo santykis

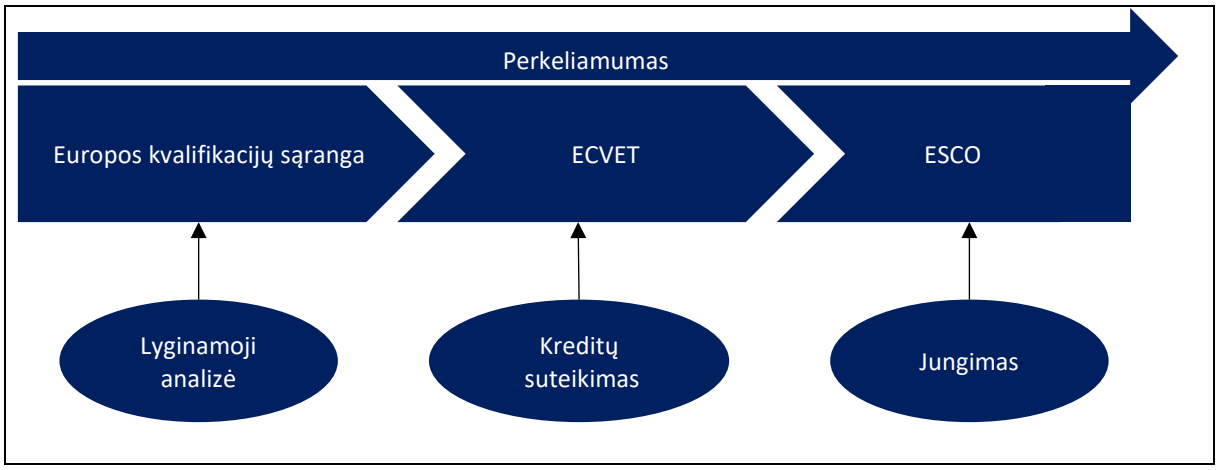
3. Už informacijos saugumą atsakingų asmenų darbas reikalauja įvairių socialinių įgūdžių. Kaip aprašyta 2.3 punkte, didžiausią grėsmę įmonės saugumui kelia jos darbuotojai. Pakeisti bendradarbių požiūrį, daryti įtaką jų darbo įpročiams ir sukurti informacijos saugumo kultūrą įmonėje, ko gero, yra didžiausias iššūkis įgyvendinant informacijos saugumo sistemą. Atsakingas asmuo turi aktyvinti, bendradarbiauti, vadovauti, konsultuoti, globoti ir derinti darbuotojus, vadovus ir informacijos saugumą. Nenuostabu, kad įmonės vertina specialistus, turinčius darbo patirties, - ir praktinę patirtį vertina labiau nei bet kokią formalią kvalifikaciją (plg. tyrimą "Informacijos saugumo mokymas MVĮ"). Gavus praktinį išsilavinimą išmokstama kasdienio bendradarbiavimo su kolegomis spąstų ir įgyjama įgūdžių, kaip produktyviai bendrauti su įmonės suinteresuotosiomis šalimis.

Švietime, informacijos saugumo kontekste, jei toks yra, šiuo metu daugiausia dėmesio skiriama techninių kompetencijų mokymui ir lavinimui IT arba teisės srityje. Praktinės patirties, ypač veiksmingų komunikacijos strategijų, įgijimas tik retai patenka į mokymo programas. Todėl "TeBeISi" siūlo sujungti tai, kas geriausia abiejuose švietimo segmentuose, ir švietimą vykdyti pasitelkiant profesinį mokymą ir rengimą bei aukštąjį mokslą.

3.2 Europos priemonių taikymas

Europos Komisija nustatė, kad profesinio mokymo ir aukštojo mokslo ryšys yra įmanomas pagal Europos kvalifikacijų sąrangą (EKS). Be to, siekiant užtikrinti profesinio mokymo skaidrumą ir palyginamumą, diegiama Europos profesinio mokymo kreditų sistema (ECVET). Galiausiai, remiantis Europos įgūdžių ir (arba) kompetencijų, kvalifikacijų ir profesijų sąranga (ESCO), galima suformuluoti bendrus gebėjimus taip, kad juos būtų galima pakartotinai naudoti ir atpažinti įvairiose profesinėse srityse.

Europos priemonių taikymas išskiria skaidrų sertifikavimo procesą iš jau egzistuojančios neorganizuotos privačių teikėjų sertifikavimo rinkos. Reikia dar kartą pabrėžti, kad egzistuoja įvairūs sertifikatai, taip pat ir MVĮ srityje, tačiau vis dar neaišku, kiek taikomi bendri kokybės ir kokybės užtikrinimo standartai, todėl trūksta skaidrumo ir perimamumo įvairiose šalyse. Europos masto akreditavimo, kokybės užtikrinimo ir kompetencijos standartų sistemų kūrimo srityje atlikti darbai sudaro sąlygas plačiai ir skaidriai diegti sertifikatus visose švietimo sistemose ir institucionalizuotose sertifikavimo srityse.



Pav. 13: ES profesinio rengimo ir mokymo skaidrumo priemonės

Trumpai tariant, šiomis priemonėmis remiama kompetencijų ir kvalifikacijų sklaida visoje ES. EKS, kaip lyginamosios analizės sistema, skirsto kvalifikacijas pagal jų pagrindinius įgūdžius, kompetencijas ir savarankiškumą ir suteikia galimybę kiekvieną kvalifikaciją iš skirtingų švietimo sistemų įtraukti į vieną atskaitos schemą, todėl skirtingas kvalifikacijas galima palyginti įvairiuose švietimo kontekstuose. Tuo tarpu ECVET suteikia pagrindą mokymosi rezultatus susieti į mokymosi kreditus, taip suteikiant galimybę suprasti, kiek ir kokio gilumo mokymosi apimties yra kvalifikacija. Be to, ji padeda užtikrinti kokybę, suteikia tęstinio mokymosi galimybes regionams būdingomis sąlygomis ir padeda pripažinti profesines kvalifikacijas įvairiose sisteminėse ar nacionalinėse švietimo sistemose. Galiausiai, ESCO yra vienijanti duomenų bazė, kurioje kaupiamos visoje ES egzistuojančios kvalifikacijos ir kompetencijos. Kuriant naujas mokymo programas, grįžtant prie šios duomenų bazės, galima užtikrinti, kad kompetencijos vienodai būtų suprantamos įvairiuose mokymosi kontekstuose.

3.2.1 Europos kvalifikacijų sąranga

Europos kvalifikacijų sąranga nustato Europos Sąjungos švietimo sistemų formalios kvalifikacijos sisteminimą. Šios sistemos tikslas - užtikrinti, kad kvalifikacijos būtų palyginamos tarp šalių, o tai leistų geriau suprasti kvalifikacijos vertę užsienyje. Kadangi švietimo sistemos ES valstybėse narėse labai skiriasi, EKS gali būti naudojama kaip orientyras siekiant užtikrinti ugdomų kompetencijų lygiavertiškumą. Nustatyta, kad TeBeISi kontekste 5 EKS lygis suteikia vertingų galimybių įmonėms ir besimokantiesiems.

5 EKS lygiui svarbūs mokymosi rezultatai		
Žinios	Įgūdžiai	Kompetencijos
išsamios, specializuotos, faktinės ir teorinės žinios darbo ar studijų srityje ir šių žinių ribų suvokimas	įvairūs kognityviniai ir praktiniai įgūdžiai, reikalingi kuriant kūrybiškus abstrakčių problemų sprendimus.	vadovavimas ir priežiūra darbo ar studijų kontekste. veikla, kai vyksta nenuspėjami pokyčiai peržiūrėti ir tobulinti savo ir kitų veiklą

Lentelė 6: EKS 5 lygio mokymosi rezultatai - žinios - įgūdžiai - kompetencijos

Šaltinis: Europos Komisija (2008)

Atsižvelgiant į pagrindinę projekto išlygą, kad dauguma turimų darbuotojų greičiausiai yra per daug kvalifikuoti, kad atitiktų MVĮ poreikius (tai taip pat atsispindi esamuose ESCO profesiniuose profiliuose), reikia rasti tinkamų priemonių, kaip suderinti informacijos saugumo užduočių sudėtingumą (t. y. IT žinias ir teisines žinias) ir minimalius MVĮ reikalavimus, kad būtų galima atsižvelgti į naujus besimokančių asmenų šioje srityje poreikius. Galima daryti išvadą, kad dėl kai kurių užduočių pobūdžio, ypač susijusių su nestandartizuotomis veiklomis arba apimančių teisines kompetencijas, kai kurie informacijos saugumo mokymo MVĮ elementai turi būti įsišakniję aukštosiose mokyklose, o tai leidžia besimokantiesiems veikti mažiau struktūruotoje ir savarankiškesnėje aplinkoje. Konkrečiai į šią kategoriją patenka su teise susijusios kompetencijos, t. y. daugiausia BDAR.

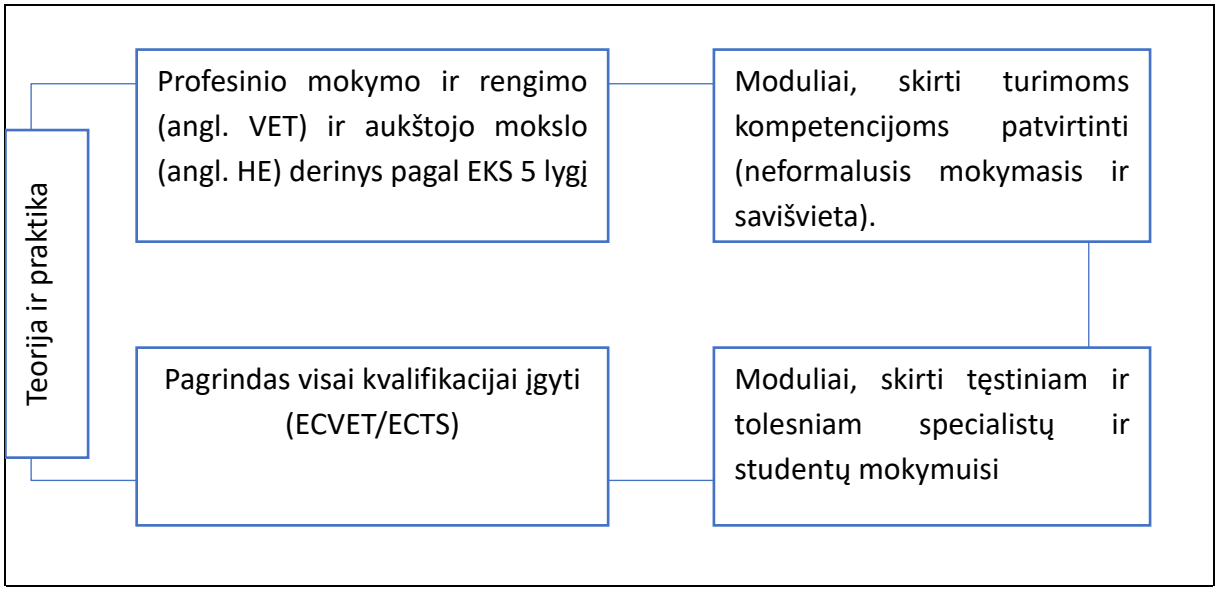
EKS 5 naudojimas turi keletą privalumų, kuriais galima pasinaudoti. Pirma, jis suteikia pagrindą daugeliui darbuotojų, turinčių EKS 4 kvalifikaciją, pradėti tęstinį mokymąsi. Todėl dalinį šio lygmens patvirtinimą galima palengvinti pripažįstant ankstesnę darbo patirtį, neformalųjį mokymąsi ir savišvietą. Sąsaja su 6 EKS panaikina atotrūkį ir suteikia galimybę prisitaikyti aukštosioms mokykloms, kurios siekia suteikti arba visą kvalifikaciją informacijos saugumo kontekste, arba papildomą kvalifikaciją savo studentams.

3.2.2 Europos profesinio mokymo kreditų sistema (ECVET)

Žvelgiant iš funkcinės perspektyvos, į mokymosi rezultatus orientuota kompetencijų operacionalizacija reiškia, kad perspektyva keičiasi nuo "Ko aš noriu mokyti?" prie "Ko turėtų išmokti besimokantieji?". Mokymosi proceso rezultatas yra mokymosi proceso dėmesio centre ir suteikia besimokantiesiems aiškesnį požiūrį į savo mokymosi

pažangą. Naudojant skaidrią kreditų sistemą galima realizuoti keletą teigiamų išorinių efektų, kurie modulinę mokymosi formą išskiria iš esamų sertifikavimo sistemų.

TeBeISi informacijos saugumo ir duomenų apsaugos pareigūno MVĮ kompetencijų profilio išskaidymas į modulines mokymosi sritis (žr. "Mokymo programą") palengvina mokymosi sričių moduliavimą ir kreditų perkėlimo sistemų, tokių kaip ECTS ar ECVET, taikymą. ECVET. Modulavimas (mikrokreditų suteikimas) suteikia keletą privalumų, pavaizduotų 11 pav. ir lemiančių didesnį dalinių kvalifikacijų skaidrumą, mobilumą ir patikimumą. Moduliai gali būti naudojami tiek darbuotojų ar studentų mokymo ir ugdymo tikslais, tiek kaip dalinio patvirtinimo priemonė, suteikianti galimybę sertifikavimo procesą taikyti vėliau į informacijos saugumo sritį ateinantiems asmenims.



Pav. 14: Modulinių kvalifikacijų privalumai

Atsižvelgiant į egzistuojančias patvirtinimo sistemas, patikimumas, priimant sertifikavimo procesą, darbdaviams ir mokymo paslaugų teikėjams yra labai svarbus. Be galiojančių kokybės užtikrinimo standartų (pvz., EQAVET), siekiant užtikrinti kuo didesnį patvirtinimo procedūros patikimumą, reikia atsižvelgti į konkrečias kompetencijos vertinimo detales.

3.3 Mokymosi rezultatų vertinimas

Mokymosi rezultatų vertinimas tebėra daug diskusijų keliantis klausimas, tuo tarpu geriausios praktikos pavyzdžių, pavyzdžiui, VALIKOM arba MySkills iš Vokietijos, yra, tačiau platus šių metodų pritaikymas negali atsakyti į visas įmonių ir vertinimo specialistų iškeltas kritines pastabas. Tarp švietimo paslaugų teikėjų išlieka klausimas, ar trumpi vertinimai yra tinkama forma pakeisti visą formavimo programą. Siekiant padidinti vertinimo proceso pagrįstumą, reikia atsižvelgti į keletą dalykų:

1. Skaidrūs procesai. Svarbiausia yra viso pripažinimo proceso skaidrumas. Priėmimo aptarimas, specialaus mentoriaus paskyrimas ir tinkamas

pasirengimas vertinimui turi būti įtraukti į holistiškai apgalvotą, žingsnis po žingsnio suplanuotą pripažinimo procesą.

2. Pačiame pripažinime reikia atsižvelgti į keletą priemonių, kad būtų užtikrintas kuo didesnis vertinimo pagrįstumas. Apskritai tam tikros vertinimo formos labiau tinka konkrečioms kompetencijoms vertinti. Tuo tarpu testai raštu, nesvarbu, ar jie būtų su atvirais atsakymais, ar su keliais atsakymų variantais, tinka žinioms vertinti, o vaidmenų žaidimai, pašto dėžutės užduotys ar pristatomieji žaidimai yra skirti komunikacinėms ir socialinėms kompetencijoms, tokioms kaip interviu, retorika, argumentacija, empatija, asertyvumas, įtikinamumas, jautrumas (elgesio stebėjimas), tikrinti. Jie taip pat naudingi vertinant pasirengimą veikti, orientaciją į tikslą, frustracijos toleravimą, atkaklumą, problemų sprendimo įgūdžius, analitinius įgūdžius, sprendimų priėmimo įgūdžius ir kt. Taikant biografinius metodus, pavyzdžiui, kriterijumi pagrįstus pokalbius, struktūruoto portfolio peržiūrą ir technines diskusijas, kandidatai įgyja visapusišką supratimą apie savo pasiekimus ir išmoksta vertinti save ir savo savybes. Galiausiai, stebėjimai vietoje ir imituojamoje aplinkoje leidžia stebėti reakcijas į realaus gyvenimo scenarijus, savitvardą ir požiūrį į spontaniškus įvykius. Taigi, derinant vertinimo metodus, galima trianguliuoti kompetencijas ir patikimai nustatyti dispozicijas.

3. Kad vertinimas būtų objektyvus, vertintojai turi būti apmokyti sąžiningai, skaidriai ir objektyviai taikyti skirtingus vertinimo metodus skirtingiems kandidatams. Vertintojai turi žinoti skirtingas kandidatų mokymosi biografijas ir skirtingus tikslus bei suprasti visą patvirtinimo ir pripažinimo procesą.

4. Rekomenduojama atlikti savęs vertinimą kaip žingsnį vertinimo link, tačiau nerekomenduojama atlikti savęs vertinimo kaip vertinimo šaltinio. Savęs vertinimas techninio vertinimo forma ("kandidatas X žino..." "taip", "ne") arba asmenybės testų forma gali duoti orientacinių rezultatų, tačiau reikia abejoti šių rezultatų patikimumu ir objektyvumu.

Todėl reikia sukurti išsamią struktūrą ir kokybės užtikrinimo sistemą, kad būtų užtikrintas patikimas, objektyvus ir skaidrus vertinimas bei sukurtas švietimo įstaigų ir darbdavių pasitikėjimas.

4 Apžvalga ir rekomendacijos

Kvalifikuotos darbo jėgos trūkumas IT sektoriuje ES vis dar yra ženklus. Techninės kompetencijos tarp profesionalų tampa ne mažiau reikšmingomis už socialines kompetencijas ar asmenines savybes. Investicijos į žmogiškuosius išteklius, pavyzdžiui, tinkamas darbuotojų apmokymas, ilgainiui tampa pelningu, atremiant rizikingas situacijas pasireiškiančias įvairiomis formomis skaitmeninėje ir fizinėje erdvėse. Įmonių pažangiosios patirties apsauga bei vidinių ir išorinių paslaugų paruoštumas grėsmėms neišvengiamai sietinas ir su netinkamu jų panaudojimo potencialu. Galiausiai, visos technologijos bei gairės, skirtos atremti priešiškas atakas yra bevertės jei įmonės personalas nėra linkęs prisidėti prie vidinės saugumo kultūros.

Saugumo politikų bei standartų įsisąmoninimas bei laikymasis sumažina galimų duomenų saugos atakų riziką. Siekiant tai užtikrinti, vertybės, įsitikinimai ir, galiausiai, žmogiškoji elgsena turi pasikeisti kuriant gyvybiškai svarbią rizikos valdymo kultūrą. Norint persiorientuoti nuo technologinio požiūrio prie žmogiškųjų savybių ugdymo būtina stiprinti mokymo bei švietimo sritis.

Skaitmeniniame amžiuje padidėjusi nusikalstamų veikų elektroninėje erdvėje rizika, susieta su konfidencialia informacija, kelia iššūkius ne tik profesinėje sferoje bei darbe, bet ir privačiame Europos piliečių gyvenime. Greta kibernetinių atakų bei dėl jų patiriamų nuostolių elektroninėje erdvėje prieš verslo subjektus bei Europos ekonomiką, nemažiau svarbūs ir padariniai konfidencialios asmeninės informacijos kontekste, kuomet taikomasi ne į įmones, o į individualius asmenis. Dėl šios priežasties piliečių išsilavinimo didinimas šioje tematikoje galėtų turėti teigiamą poveikį verslui bei visuomenei. Gebėjimų ugdymas turėtų tapti ne tik paskirų įmonių interesu, bet ir visos visuomenės tikslu. 2018 metais ES Taryba iš naujo apibrėžė pilietines kompetencijas kaip: “gebėjimą elgtis atsakingai bei visiškai dalyvauti pilietiniame ir socialiniame gyvenime, grįstame socialinių, ekonominių, teisinių bei politinių koncepcijų bei struktūrų, taip pat globalaus vystymosi bei tvarumo suvokimu.”

Brandžių piliečių dalyvavimas kuriant šiandienos bei rytojaus pasaulį yra glaudžiai susietas su gebėjimu atskirti sąmoningai daromą žalą nuo pavienių incidentų. Klaidingos informacijos, manipuliacijų atpažinimas bei privačios informacijos branginimas yra svarbūs pilietinio atsparumo klausimai, kurie neturėtų apsiriboti privačių korporacijų pelningumo kriterijumi.

Galiausiai tai yra ir esminis ES bei jos valstybių narių interesas, kuris turėtų būti realizuojamas ne tik per informacinių technologijų padalinius, bet ir per švietimo ministerijas. Atsižvelgiant į šiuos teiginius, toliau pateikiamos rekomendacijos, siekiant stiprinti minėtus gebėjimus Europos piliečių tarpe:

1. Europinės organizacijos, skirtos privačios informacijos ir duomenų apsaugai sukūrimas. To pasėkoje būtų kuriama sutartinė, kritiniais klausimais bendru sutarimu besivadovaujanti žinių apykaitos erdvė, tapsianti kelrodžiu derinant

pilietinius, verslo ir privačiuosius interesus. Šios organizacijos tikslu galėtų būti toliau skelbiamų rekomendacijų viešinimas bei populiarinimas.

2. Sukurti informacijos apsaugos mokymo planą. Atsižvelgiant į tai, kad žmogaus vertybių, tikėjimo bei veikimo transformacijos yra ekonominiu požiūriu neįgyvendintinos, svarbu dalyvauti šių nuostatų formavimo procesuose ir mokyti asmenis atpažinti bei suvaldyti galimos grėsmės scenarijus, įskaitant manipuliacijas ar neteisingos informacijos atpažinimą skaitmeniniame amžiuje.

3. Sukurti Mikro-kredencialų ir dalinio sertifikavimo schemas informacijos saugumo užtikrinimui privačiame bei profesiniame kontekste. Dabartinė tęstinio mokymo šioje srityje būklė nėra skaidri bei stokoja struktūrizuotos vizijos, nukreiptos į ateitį. Greta egzistuojančių sertifikavimo formų, visaverčio modulinio mokymus plano sukūrimas leistų užtikrinti informacijos ir asmens duomenų svarbos suvokimo sklaidą. Pavieniai moduliai galėtų būti integruoti į profesinių švietimo įstaigų (EQF 4) bei aukštųjų mokyklų (EQF 6-7) kursus, pritaikant temas skirtingiems dalykams bei apjungiant modulius į vientisą mokymų kursą, susietą su profesine veikla ir aukštosios mokyklos programa (EQF5). Alternatyviai, šiuos modulius galima pasiūlyti darbdaviams kaip tęstinio mokymosi galimybę. Modulinis kursų pobūdis leistų koreguoti mokymosi intensyvumo spektrą, taip sumažinant sąnaudas bei padidinant prieinamumą mažoms bei vidutinėms įmonėms.

4. Daugiau naudotis Europos skaidrumo priemonėmis, kad būtų skatinamas darbo rinkos lankstumas ir pritraukiami nauji talentai.

5 Literatūra

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.

Strateginė ataskaita

Dėkojame bendraautoriams iš:

BF/M-Bayreuth

Mykolo Romerio universitetats

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

„Dalinis sertifikavimas informacinės saugos profesinėje srityje“ - TeBeISi

Finansuojama pagal Europos Sąjungos programą "Erasmus+

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