ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА

Kadir Ider

Заглавие:

„Намаляване на сложността и прилагане на GDPR: Концептуализация на ориентирана към потребителя онлайн система за контрол на поверителността и оценка на нейните ефекти върху организационната надеждност“

АВТОРЕФЕРАТ
на дисертация за получаване на образователна и научна степен „доктор“

по докторска програма 05.02.21 „Организация и управление на производството (индустрия)“
в професионално направление 5.13 „Общо инженерство“

Научни ръководители:
1. **проф. д-р инж. Тодор Ганчев**
2. **проф. д-р Светлана Лесидренска**

Рецензенти:
1. **проф. д-р Сийка Демирова**
2. **доц. д-р Капка Манасиева**

Варна, 2023 г.

Автор: Kadir Ider

Заглавие: „Намаляване на сложността и прилагане на GDPR: Концептуализация на ориентирана към потребителя онлайн система за контрол на поверителността и оценка на нейните ефекти върху организационната надеждност“

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – ВАРНА

Kadir Ider

Заглавие:

„Намаляване на сложността и прилагане на GDPR: Концептуализация на ориентирана към потребителя онлайн система за контрол на поверителността и оценка на нейните ефекти върху организационната надеждност“

АВТОРЕФЕРАТ /ПРОЕКТ/

на дисертация за получаване на образователна и научна степен „доктор“

Варна, 2023 г.

Дисертационният труд съдържа 125 страници, включително 32 фигури, 32 таблици и приложения, оформени в 4 глави, общи изводи и списък на използваната литература от 67 заглавия.

Защитата на дисертационния труд ще се състои на ..... г. от ……..... ч. в ..... на открито заседание на жури, сформирано със заповед на Ректора № ...../..... г.

Материалите по защитата (дисертацията, рецензиите и становищата) са на разположение на интересуващите се в Докторантския център, стая 318 НУК

Съдържание

А. ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Настоящата дисертация има за цел да разработи ориентирана към потребителя система за контрол на поверителността на данни, която да е в помощ на организациите при спазването на изискванията свързани с Общия регламент за защита на личните данни (GDPR). Проучването се основава на преглед на литературата в областта, първично и вторично събиране и анализ на данни, както и на дизайнерско мислене, с цел създаване на практична, мащабируема и междуиндустриално приложима система за контрол на поверителността, която да взима под внимание въздействието върху обществото, неяснотата на законовите наредби и технологията. Методологията на изследването включва международно уеб-базирано проучване, използващо Qualtrics и Google Forms, целящо да се определи информираността на потребителите, доверието към организациите и оценката на елементите за контрол на поверителността на данни.

Дисертационният труд се състои от четири глави. Глава Първа предоставя обосновка и общ преглед на целите на дисертацията. Глава Втора дефинира използваните в изследването термини: „потребител“, „организация“, „контрол“, „доверие“, „надеждност“ и „рамка за измерване“. Глава Трета очертава методологията, използвана при събиране и анализиране на данни за факторите влияещи върху изграждането на надеждност от страна на потребителите и организациите. Глава 4 обобщава резултатите от проучването, предлага бъдещ план за развитие и завършва като подчертава необходимостта от работна група, която да изследва нуждите на потребителите и предизвикателствата пред организациите.

Дисертацията предлага нов и практичен подход към трудностите при спазването на GDPR чрез интегриране на фактори като влияние над обществото, неприкосновеност на личния живот, намаляване на неяснотата на законовите наредби и технологичните аспекти в система, ориентирана към потребителя. Предложената

система за контрол на неприкосновеността на личния живот ще даде възможност на лицата да контролират личните си данни, като противовес на тенденцията този контрол да бъде прехвърлян към организациите за обработка на данни. Резултатите от проучването дават представа за информираността и отношението на потребителите към поверителността, както и за тяхното доверие към организациите, което ще предостави информация за развитието на ориентираната към потребителя система за контрол на поверителността.

В заключение, настоящата дисертация допринася за дискусията по спазването на изискванията свързани с GDPR, като предлага практичен и ориентиран към потребителя подход към системите за контрол на поверителността. Проучването дава представа за информираността и отношението на потребителите към поверителността, както и за тяхното доверие към организациите, което може да бъде използвано за подобряване на индивидуалния контрол върху личните данни и насърчаване на доверието между лица и организации.

В следствие от гореизложеното, проблемите, разгледани в дисертационното изследване, могат да бъдат обобщени, както следва:

1. Влиянието на неприкосновеността на личния живот върху обществото, разкриващо липсата на ориентираност към потребителя и поставящо фокус върху нарастващия брой крайни точки за събиране на данни.
2. Неясни законови наредби и липса на практически насоки, отразяващи трудностите при разбирането и законосъобразното и последователно превръщане на изискванията в оперативни процеси.
3. Технологията като фактор и пречка, като се отдава значение на недостатъчното развитие на инфраструктурите на информационната система, които са в основата на ефективния механизъм за защита.

Б. ОБЕКТ И ПРЕДМЕТ НА ИЗСЛЕДВАНЕ

Обектът на това проучване е разработването на ориентирана към потребителя система за контрол на поверителността, която да подпомага организациите при спазването на Общия регламент за защита на личните данни (GDPR). Предмет на изследването е практическата, мащабируема и междуиндустриално приложима система за контрол на поверителността, която отчита влиянието върху обществото, неясните законови разпоредби и технологичните аспекти. За постигане на тази цел, проучването включва преглед на литературата, първично и вторично събиране и анализ на данни и дизайнерско мислене.

Основен фокус на проучването е спазването на GDPR да бъде практично и мащабируемо, тъй като от съществено значение за организациите е да запазят поверителността на потребителите, като същевременно се придържат към законовите разпоредби. Основният акцент на проучването е ориентираната към потребителя система за контрол на поверителността, вземаща предвид тяхната информираност, доверието към организациите и елементите за контрол. Това е иновативен и практичен подход към трудностите при спазването на GDPR. Проучването също така предоставя ценна информация за информираността и отношението на потребителите към поверителността, което подпомага разработването на системата за контрол на поверителността.

Основните теоретични и методологични подходи отнасящи се за концепцията на системата за контрол на поверителността са следните:

- Изследването ще се проведе чрез поредица от международни проучвания, систематичен преглед на литературата и прилагане на процеса на дизайнерско мислене. Получената рамка ще бъде оценена чрез внедряване на прототип.
- Дефинициите са извлечени от Общия регламента на GDPR, работна група по член 29 и теорията за социалното обучение.

● Оценка на резултатите от външни проучвания и цялостни пазарни проучвания.

● Анализ на правни и технически контролни елементи.

● Оценка на психологическия контрол чрез анкети и проучвания.

Въпреки че самото проучване е планирано и изпълнено в рамките на Европейския съюз (ЕС), методът за анализ отчита възгледите на жители извън ЕС, тяхното разбиране за система за контрол на поверителността, както и нейното влияние върху корпоративната надеждност. Този подход осигурява по-широка приложимост, като по този начин се разширяват териториалните възможности за използване на изследването.

В. ПУБЛИКАЦИИ ПО ДИСЕРТАЦИОННИЯ ТРУД

1) Ider, K. (2022). Assessment of the quality of user awareness of GDPR in healthcare IOT. In Proceedings of the International Conference on Biomedical Innovations and Applications (BIA-2021) (pp. 1-6). IEEE. https://doi.org/10.1109/BIA52594.2022.9831287

2) Ider, K. (2021). Secure Public WiFi durch Network Access Control – Ansätze, Chancen und datenschutz-rechtliche Implikationen. In Proceedings of the Nachwuchswissenschaftler*innenkonferenz 2020/21, EAH Jena.

3) Ider, K., & Faustino-Bauer, M. (2020). DSGVO Compliance und Datenschutz-Managementsystem als Erfolgsfaktor für die Digitale Transformation nutzen. ZRFC Risk, Fraud & Compliance Magazine, 75(6), 327-332. https://doi.org/10.37307/j.1867-8394.2020.06.04

4) Ider, K., & Schmietendorf, A. (2020). Data Privacy For AI Fraud Detection Models – A framework for GDPR compliant AI. In Proceedings of the Fourteenth International Conference on Digital Society (ICDS 2020) (pp. 17-22). IARIA XPS Press. ISBN: 978-1-61208-760-3

5) Ider, K. (2020). Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity. In Proceedings of the 2020 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG) (pp. 143-148). Shaker Verlag GmbH. ISBN: 978-3-8440-7515-1

6) Ider, K. (2019). Barriers for the Utilization of Open Data. In Proceedings of the 2019 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG) in cooperation with Hochschule für Technik und Wirtschaft Dresden (pp. 97-102). Shaker Verlag GmbH. ISBN: 978-3-8440-6837-5

Г. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

I. Одобряване на разработката

Дисертационният труд е докладван и обсъден както в отделните му части, така и в завършен вид, на заседание на катедрения съвет на катедра „Индустриален мениджмънт“ към Факултет по машиностроене и технологии на Технически университет – Варна.

II. Кратко изложение на дисертационния труд

Структурата на дисертационния труд се състои от четири глави, отговарящи на следните изисквания:

1) Да се подчертаят обхвата, методите, резултатите и иновативността на всяка глава в изследването.
2) Всяка глава да съдържа заключение, обобщаващо напредъка и резултатите.
3) Да се обобщи приноса в резултат на докторантурата.

1. ВЪВЕДЕНИЕ

С въвеждането на стандартизиран Общ регламент за защита на личните данни (GDPR), Европейският парламент се стреми да наложи по-стриктно спазване на отчетността при обработката на лична информация. Следователно организациите трябва да осигурят адекватно и ефективно оповестяване на условията за поверителност, за да се изгради правилното ниво на доверие в отделните лица. Териториалният обхват на регламента обхваща и чуждестранни компании, които предлагат стоки и услуги на жители на ЕС. Последващо неспазване на регламента може да доведе до глоби, които възлизат общо на 1,6 милиарда евро, платени към средата на 2022 г. (Ider, 2020b).

Въвеждането на общоевропейски стандартизиран регламент за защита на личните данни е значима стъпка, тъй като нарастващият брой лични устройства и прогресивната

цифровизация на услугите добавят допълнителни вертикали за събиране на лични данни, което налага тяхната защита. Към 2020 г. 90% от всички жители на Европа имат редовен достъп до интернет, основно чрез мобилен телефон, следван от настолен компютър и по-незначителен брой чрез таблет (ContentSquare, 2020; Kemp, 2020). В Германия, където всеки човек има достъп до повече от седем (свързани с интернет) устройства, домакинствата се състоят средно от двама членове. Някои устройства се използват споделено, но на всеки човек се падат приблизително по два лични мобилни телефона (Werliin & Kokholm, 2020 г., стр. 10; Statistisches Bundesamt (Destatis), 2020 г., стр. 44). Трите най-често достъпни цифрови услуги са развлечения, покупки на продукти и банкови транзакции (Betti et al., 2020).

Поради увеличаващите се точки за достъп до данни и методи за тяхното събиране и обработка, регламентът си поставя за цел подобряването на тяхната защита. Въпреки това, почти 2,5 години след въвеждането на GDPR, ⅔ от всички германски организации все още се борят да постигнат пълното спазване на регламента (Dehmel & Kelber, 2020 г., стр. 2). Имайки предвид нарастващия брой наложени глоби в цяла Европа, може да се направи заключението, че нивото на спазване на регламента е подобно за всички европейски организации (Ider, 2020a, p.105).

Във връзка с гореизложеното, тази дисертация си поставя за цел предоставянето на рамка за намаляване на сложността и подобряване на оперативната реализация на Европейския регламент за защита на личните данни (GDPR). Това се постига чрез концептуалното разработване на прагматична, мащабируема и междуиндустриално приложима, ориентирана към потребителя система за контрол на поверителността с характеристики минимално нарушаващи организационния дизайн. Темата и основното изследване имат съвременна значимост и непосредствено въздействие върху обществото. В момента както потребителите, така и организациите, са засегнати от три аспекта, които дават допълнителна обосновка на изследването. Те включват

неясните законови разпоредби и липсата на практически насоки, технологичните предизвикателства, както и дилема при спазване на защитата на данните.

2. ГЛАВА ПЪРВА: АНАЛИТИЧНО ИЗСЛЕДВАНЕ И ПРЕГЛЕД НА ГЛОБАЛНИТЕ И РЕГИОНАЛНИ РЕШЕНИЯ НА ПРОБЛЕМА

2.1. Постановка на проблема

В GDPR не се предвижда предоставяне на практически насоки за системите и процедурите за неговото спазване. Вместо това, се определят принципите за обработка на данни, т.е. фокусира се върху това „какви критерии трябва да бъдат изпълнени“, но има пропуск по отношение на това „как трябва да се осъществят“.

Към момента на провеждане на изследването, няма консенсус за цялостното прилагане на GDPR, нито в световен мащаб, нито в рамките на една индустрия, особено що се отнася до оповестяването на условията за поверителност. Следователно, засегнатите организации срещат трудности при тълкуването на законовите регламенти и свързаните с тях правни задължения, а следователно и с приспособяването на съществуващите ИТ инфраструктури (Jiang et al., 2019, стр. 13). Почти 40% от 1100 интервюирани организации твърдят, че една от най-значимите трудности е съгласуването с GDPR на съществуващата ИТ инфраструктура (Jiang et al., 2019, стр.13).

Липсата на правно и техническо разбиране на GDPR причинява несъответствие между дизайна на системата за спазването му и оперативната ефективност. Въпреки усилията на организациите да предадат и обяснят на гражданите въпросите свързани с поверителността, настоящата правна неяснота води до преизползване на правен език в политиките на организациите, тъй като свързаните с това документи често се пишат от професионалисти в областта (Faustino-Bauer & Ider, 2020 г., стр. 248). Тази неразбираемост и сложност води до обратния ефект, т.е.

до неспазване и създаване на неефективни политики. Следователно, организациите в нарушение не спазват принципите за обработка на данни съгласно чл. 5 GDPR. Ако се обобщят описаните трудности, основните крайъгълни камъни на дилемата за спазване на изискванията за защита на данните са:

1) въздействието върху обществото на неприкосновеността на личния живот, разкриващо липсата на ориентиране към потребителя и фокусиране върху нарастващия брой крайни точки за събиране на данни.

2) неясни законови разпоредби и липса на практически насоки, отразяващи предизвикателството да бъдат разбрани изискванията и превърнати в оперативни процеси по законосъобразен и последователен начин.

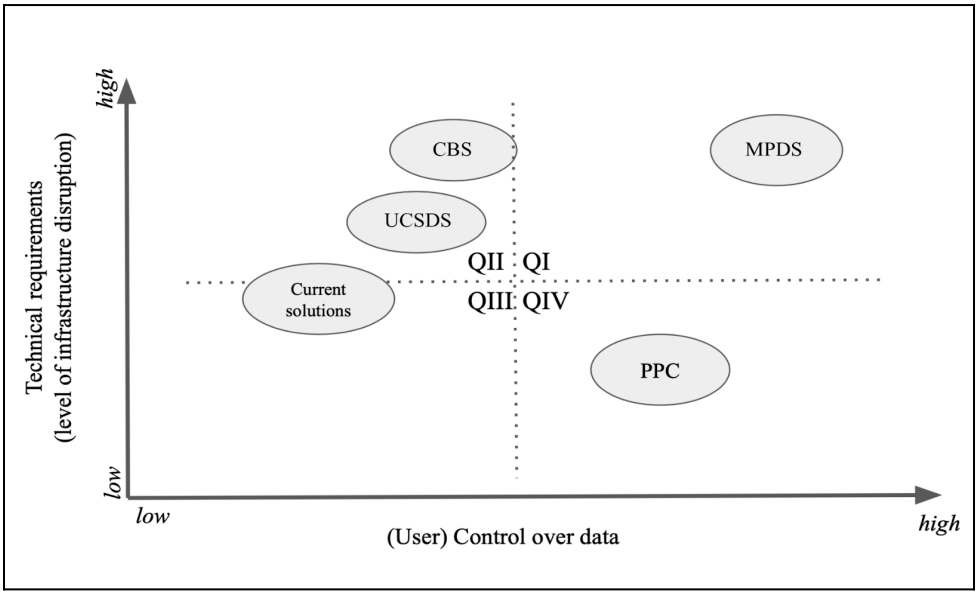
3) технологията като фактор и пречка, подчертаващи изоставането на инфраструктурите на информационните системи, които са в основата на ефективния механизъм за защита.

2.2. Обосновка на изследването

Организациите търсят възможности за постигане на конкурентно предимство чрез генериране на ценна информация за отделните лица, тъй като личните данните се считат за „новия нефт“ на 21-ви век. Мотивацията на настоящото изследване е създаването на подходящи инструменти за съобразено използване на личните данни. В основата е справянето с нуждите на обществото и приноса към по-добрата защита на правата предоставени от GDPR. Разработката има за цел да създаде справедлива рамка за обработка на лични данни, която ще подобри настоящите процедури по GDPR и тяхната комуникация в полза на обикновения гражданин, обществените организации и всички бизнес субекти. Изследването също има за цел да осигури и така необходимата практически ориентирана социална иновация за подобряване на защитата на данните и осигуряване на по-добра поверителност.

Изследователската работа в областта на ориентираните към потребителя решения за управление на данни може да се обобщи в три основни групи (Ider, 2020a, стр.104). Първо – модели, базирани на Механизми за съхранение на лични данни (MPDS), второ – Ориентирано към потребителя защитено споделяне на данни (UCSDS) (Grashöfer et al., 2017, стр.1244) и трето – Криптографски базирани решения (CBS) за създаване на прозрачност на данните и тяхната проследимост (Truong et al., 2020, стр.1746).

Първата концепция, MPDS, включва решения като Solid (Sambra et al., 2016), Digi.me или Mecco (Sjöberg et al., 2017), които по същество предоставят социално свързани и лични микробази данни за съхранение на физически лица и разкриват на доставчиците на услуги само избрани данни от централизирано достъпен интерфейс. При второто решение, UCSDS поставя фокуса върху инфраструктурата за достъп до данни и механизма за оторизация, като по този начин се набляга по-малко на действителната собственост върху данните и повече на технологичното решение за опростяване на споделянето на отделни елементи или категории лични данни. Третият вариант, т.е. CBS, има за цел използването на данни да е винаги проследимо. Представените решения – MPDS, CBS, UCSDS – са нанесени спрямо измеренията *контролируемост на потребителя* и *технологични изисквания*, както е показано на Фигура 1. Графиката показва нивото на контрол на потребителя върху своите данни спрямо размера на очакваното прекъсване на ИТ инфраструктурата на организацията, с цел да се постигане контрол на потребителите върху поверителността.



Фиг. 1: Вероятност на адаптивността на системата за поверителност

2.3. Сравнителен анализ на моделите

На Фигура 1, означена като *current solutions (текущи решения)*, за целите на сравнителния анализ, е изобразена междуиндустриална сравнителна оценка на съвременната готовност за спазване на разпоредбите за поверителност на организации в Германия. Самата готовност е резултат от способността да се гарантират изцяло, частично или изобщо да не се спазват следните изисквания на GDPR (Pricewaterhouse Coopers, 2018):

1. Техническа и организационна сигурност (TOMs),
2. Записи на дейностите по обработка (RoPAs),
3. Системи за изтриване и задържане,
4. Потребителски права за достъпа до данни.

Направеното обобщение предоставя изводи за определяне на нивото на контрол върху данните, както и основните технически изисквания, както е показано в балончето на Фигура 1 – *текущи*

решения. Кокпитът за лична поверителност (PPC) е начертан допълнително. Той е поставен близо до центъра на QIV, тъй като представлява предвиденото ниво на контрол и техническа сложност, което трябва да се постигне.

Както е показано на Фигура 1, разделяме двумерната равнина на четири квадранта. Това подчертава, че представените решения в рамките на QI и QII по своята същност изискват по-висока технологична адаптация, като по този начин потенциално в по-голяма степен нарушават съществуващите инфраструктури. Въпреки че MPDS (Механизъм за съхранение на лични данни) предлага най-значимия контрол на поверителността, може да се заключи, че това не е непременно най-желаното решение поради присъщата му техническа сложност. Много организации вече виждат най-голямото предизвикателство в адаптирането на ИТ инфраструктурата. Понастоящем, повечето организации могат да бъдат класифицирани в сегмента QIII и трябва да се стремят да се придвижат по-нататък към QIV, чрез ограничаване на техническите усложнения и увеличаване на степента на потребителски достъп и контрол върху данните. Всички опции осигуряват важни градивни елементи за разработване на ефективно, създаващо доверие, сигурно, прозрачно и ориентирано към потребителя решение (Ider, 2020a, стр.104). Тези алтернативи обаче са обект на по-строги технологични изисквания и не разполагат с възможности за масова адаптация на организации и потребители. В допълнение към казаното, основното предназначение на посочените решения не е спазване на изискванията свързани с GDPR.

Заключението направено от горния анализ е, че може да бъде постигната значително по-висока степен на приложимост, ако решението свързано със защита на данните е с пропорционално по-висока степен на потребителски контрол в сравнение с техническата сложност. Това допълнително ще доведе до по-малко проблеми, тъй като ще се намалят сложните технологични изисквания. Съществуващите концепции и услуги за контрол на поверителността предоставят важни елементи, които ще бъдат допълнително разгледани в рамките на това изследване.

Независимо от това, тази концептуализация има за цел да намали технологичната сложност както за организациите, така и за отделните лица.

2.4. Ограничения при изследването

Изследването се ограничава до теоретичната концептуализация на ориентирана към потребителя онлайн система за контрол на поверителността. Следователно, разработването и тестването на решението ще бъде извършено само върху малка извадка от него. По време на изследването ще бъдат проведени множество проучвания, за да се вземат под внимание и приложат специфичните за потребителите изисквания, като се гарантира използването на най-съвременни технологии. Освен това, възможността за успешно внедряване на системата за контрол на поверителността в организациите ще бъде преценена чрез теоретична оценка на характеристиките на инфраструктурата на системата за информационни технологии (ИТ), както и чрез последваща оценка на съвместимостта между системата за поверителност и ИТ. В този контекст, основната предпоставка е, че организациите могат да покажат минимално ниво на технически опит.

Ограниченото време и недостатъчния достъп до статистически данни, както и ограниченията на ресурсите, могат да повлияят на представителността на изследването. Също така, културните предпочитания могат да повлияят на обективността на резултатите. И накрая, събраните данни са съставени въз основа на обратната връзка, предоставена от участниците в проучването като по този начин оценката ще бъде извършена предимно въз основа на тяхната самооценка, а не въз основа на наблюдавано поведение. За да се компенсира възможната дихотомия – нагласа и поведение – (Kokolakis, 2017, стр. 124), някои въпроси ще бъдат проектирани по такъв начин, че да изискват от участниците в проучването да бъдат активно ангажирани с потребителския интерфейс. Следователно,

рискът който остава е, че получените данни може да не отразяват изцяло действителното поведение на участниците, тъй като въпросите са създадени за целите на проучването, а не за действително събитие, за което лицата са помолени да споделят информация (напр. регистрация в уебсайт за получаване на услуги).

Следователно, самооценката на дадено поведение, за целите на изследването, може да е различна от тази на наблюдаваното поведение. За да се сведе до минимум дихотомията, проучването има за цел да симулира обстоятелства от „реалния живот“, за да подбуди действителното потребителско поведение. По този начин, въпросите в анкетата са частично така конструирани, че да улавят самооценка на мнения (отношения) от потребителска гледна точка и до известна степен да открият поведенчески саморазкрития чрез активно участие във въпросите на анкетата, като напр. включване на макети на системни интерфейси. Проучването е конструирано така, че да има за цел допълнително да минимизира всякакви асоциации свързани с работа, като на участниците ще бъде предложено да предоставят по желание своите имейл адреси, ако искат да участват в томбола в рамките на изследването.[1] Пропорционалният брой потребители, които ще въведат своите данни, допълнително ще предостави доказателства и валидиране за целия набор от данни.

2.5. Резюме на Глава Първа

- Обхват:
  - Обсъжда се значението на неприкосновеността на личния живот в дигиталната ера, като се подчертава нарастващата нужда хората да дават съгласието си при събиране на лични данни.
  - Обсъждат се предизвикателствата, пред които са изправени организациите при спазването на Общия

[1] Участниците в проучването могат да спечелят онлайн ваучери за пазаруване.

регламент за защита на личните данните (GDPR) и непълното разбиране на политиките за поверителност от страна на лицата.

- Методи:
  - Първично и вторично събиране и анализ на данни, систематичен преглед на литературата и процес на дизайнерско мислене.
- Резултати:
  - Дефиниране на обхвата, т.е. дисертацията ще доведе до концептуализация на практически приложима, мащабируема и междуиндустриална система за контрол на поверителността, която ще подобри разбирането на условията за поверителност и ще намали сложността на GDPR.
- Принос:
  - Проучването предлага нов и практичен подход към настоящите предизвикателства при спазването на GDPR чрез интегриране на фактора въздействие на неприкосновеността на личния живот върху обществото, намаляване на тежестта на нееднозначните законови разпоредби и технологията в ориентирана към потребителя система за контрол на поверителността.
- Изводи:
  - Тази глава подчертава важността на поверителността и предизвикателствата, пред които са изправени организациите при спазването на GDPR. Изследването има за цел да отговори на тези предизвикателства чрез разработване на ориентирана към потребителя система за контрол на поверителността.

3. ГЛАВА ВТОРА: ТЕОРЕТИЧНА ФОРМУЛИРОВКА НА РЕШЕНИЕТО И ЗАДАЧИ ЗА ПОСТИГАНЕ НА ЦЕЛТА.

Настоящата глава идентифицира съответните термини и дава техните дефиниции. Въз основа на констатациите се определят и изискванията за защита на данните и въздействието на GDPR върху системата за поверителност на потребителите.

3.1. Дефиниция на термините

3.1.1. Дефиниция на термина „потребител“

В рамките на това изследване терминът „потребител“ винаги се отнася до „физическо лице“ и се използва еквивалентно за „респондент“, „участник в проучването“ и „субект на данни“.

Понятието „физическо лице“ е изведено от чл. 4 (1) от GDPR. Това означава всяко лице, което разкрива лична информация на организация в замяна на платени или безплатни продукти или услуги. В контекста на чл. 4 (1) от GDPR физическо лице или субект на данни съществува, когато една или повече информации водят до недвусмисленото идентифициране на това лице. Точната дефиниция на регламента е следната:

> „[…] **лични данни** означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.“

Следователно системата за контрол на неприкосновеността на личния живот следва да маркира или обозначава специални категории данни и да предоставя подробна информация за основната обработка и засилените мерки за сигурност за защита на тези данни. Работната група по член 29 предоставя изчерпателна дефиниция за идентификация на непреките потребителите, която включва (документи на работната група по член 29, 2014 г., стр. 18):

- Извеждане на лицето: Все още ли е възможно дадено лице да бъде изведено?
- Намиране на връзка: Все още ли е възможно да се намери връзка между записите отнасящи се до конкретно лице?
- Извършване на предположение: Може ли да се извърши предположение относно информацията за дадено лице?

3.1.2. Дефиниция на термина „организация“

Терминът „организация“ в рамките на това изследване се отнася до всяка институция, която обработва лични данни, както и до всички видове администратори, обработващите данни и техните задължения. В контекста на GDPR концепцията за администратор и обработващ по същество е предназначена да дефинира задълженията и отговорностите между организациите, които участват в обработката на лична информация. GDPR определя в чл. 4 (7), че администраторът е институция, която определя целта и средствата за обработване.

Обработващият не определя нито един от факторите, а е изпълнител на услуги, действащ от името на администратора.

3.1.3. Дефиниция на термина „контрол“

В дисертационния труд понятието „контрол“ е дефинирано от правна, техническа и психологическа гледна точка. Разбирането на такива дефиниции е от съществено значение за формулирането на подходящи ключови сегменти за оценка на надеждността на

организациите. Обобщение на някои ключови точки е представено по-долу:

А. Правна дефиниция на контрол на потребителя:
- правата на потребителите са посочени в чл.12-23 от GDPR
- изграждане на основата за определяне на изискванията за контрол на потребителя

Б. Психологическа дефиниция на контрол на потребителя
- включва емоционална оценка, която се счита за психологическо състояние
  - власт, сила или влияние върху събития, поведение, ситуации или хора
  - регулиране [...] на независима променлива [...]

В. Технологична дефиниция на контрол на потребителя
- физически средства за изпълнение на изискванията за контрол, посочени в правния контекст
- отнася се до функциите, които системата за обработка на информация предоставя, за да:
  - управлява информацията и поддържа свързаните с това системи и
  - даде възможност за притежание и прозрачност на данните в контекста на потребителя.
- осигуряване на контрол на организационно и оперативно (бизнес) ниво и на ниво информационна система.

Трите гледни точки са избрани въз основа на резултатите от предходния анализ. Оценката на контрола от правна гледна точка е важна, тъй като полага правната основа, от която се извличат технически и потребителски контролни елементи. От подробното разглеждане на проблема в дисертацията се разкрива, че техническият контрол е факторът, който позволява и определя

степента на управление на данните от потребителите или организациите. Психологическата перспектива определя осъзнаването и възприемането на контрола, което може да се счита за най-чувствителния аспект. Констатациите ще доведат до преценка дали нивото на контрол, което хората имат върху своите лични данни, корпоративни процеси и системи, оказва влияние върху надеждността на организациите.

3.1.4. Дефиниция на термините „доверие“, „надеждност“ и „рамка за измерване“

В теорията за социалното учене, „доверието“[2] се формира от очакването за изход от дадена ситуация, както и нивото на опит в подобни междуситуационни обстоятелства (Rotter, 1980, p.2). Решаващ елемент за формиране на доверие е увереността в истинността на доверието (Rotter, 1980, стр.4) в човек или институция, т.е. до каква степен някой заслужава доверие. Следователно може да се очаква, че (1) опитът на доверяващия се, (2) резултата, който човек очаква и (3) нивото на надеждност на довереното лице определят степента на доверие.

Поради тези причини, доверието особено се различава при различните възрастови групи (Sutter & Kocher, 2007, стр.373) или професии на индивидите, тъй като може да се очаква, че възрастта и опитът са в положителна корелация (Gul, 1983, p.86). Предполага се, че опитът се изразява чрез комбинация от възрастта и професията на индивидите, свързани с целите на това изследване.

Според по-новите дефиниции, доверието се разглежда като социално предпочитание (Ashraf et al., 2006, p.194), при което очакването за възвръщаемост се замества от алтруистичното поведение на индивидите, като на преден план се поставя

[2] За да се осигури точен и ясно очертан обхват на приложение, тази дефиниция не взема предвид зависимостта от полето (Gul, 1983), т.е. степента, в която междуситуационните обстоятелства са податливи на външни влияния повече отколкото от личното чувство за ред.

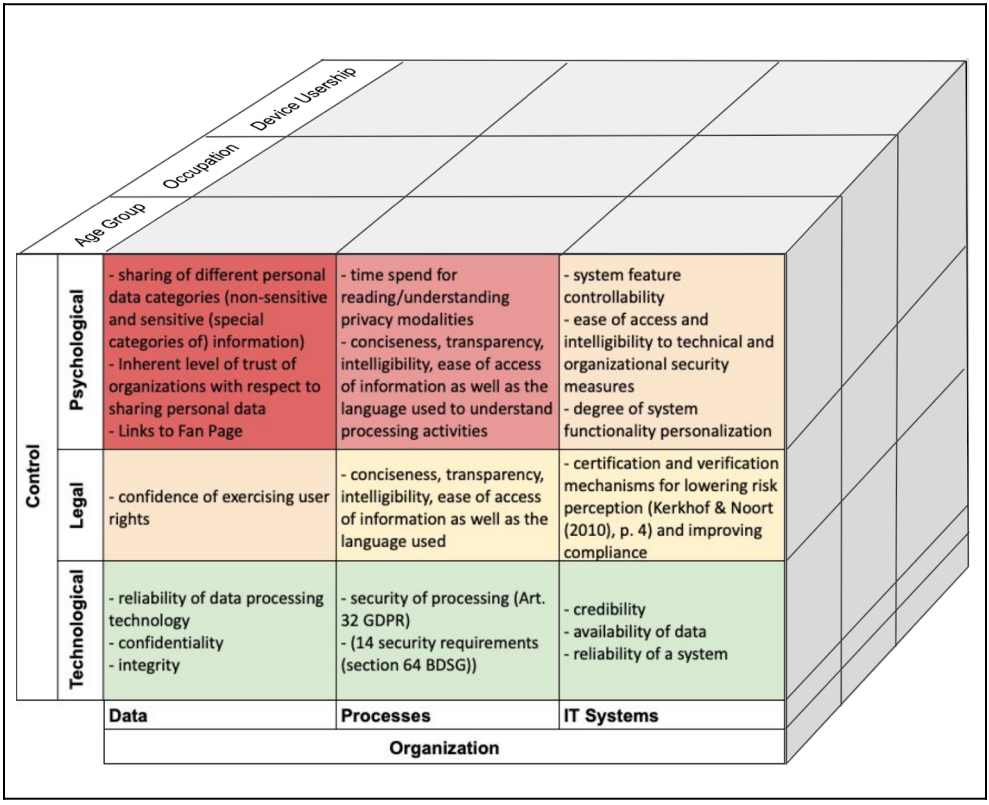
вродената безкористност и радост да бъдат добри и справедливи към другите (Andreoni & Miller, 2002, p.737). Въпреки това, по-новите дефиниции са по-малко подходящи за това изследване, тъй като обект на изследването не е алтруистичният капацитет на индивидите спрямо организациите, а е точното установяване на терминологична дефиниция и определянето на по-нататъшния обхват на приложимост на това изследване.

3.2. Заключение

Въз основа на ключовите елементи, посочени в уводната глава, дефинициите на термините и понятията предоставиха цялостно разбиране на термините „доверие“ и „контрол“ от гледна точка на различни дисциплини, включително психология и технологии, както и от интердисциплинарна правна гледна точка.

Дефинициите бяха въведени в многоизмерна рамка, която ще бъде използвана като работен модел за последващ анализ. Наблюденията върху техническите и психологически аспекти са допълнително съпоставени с изискванията на GDPR. Обединението на тези измерения дава възможност за холистичен подход към анализа и по-нататъшно уточняване на точните мерки и функции на системата за контрол на поверителността. Цветовете представляват нивото на влияние, което участниците имат върху развитието на надеждността. Участниците включват потребители, организации и юридически органи, които определят законодателната основа за GDPR. Освен това, частичното заключение, направено в рамките на дисертацията, дава възможност за последващ анализ, който да бъде стеснен до по-нататъшно задълбочено изследване основаващо се на: (1) възрастова група, (2) професия и (3) потребители (оста z). Следователно оценката предоставена в следващите параграфи ще бъде реализирана в три етапа, а изследването на данните ще се извърши въз основа на трите сегмента.

Всяка констатация ще има своето обобщение в заключението, както и последващо сравнение и дискусия. Следователно съществуващата рамка е разширена чрез добавяне на трето измерение или ос - z. Това измерение определя трите критерия, според които се оценяват елементите, създаващи надеждността (представени от осите x и y), както е представено на Фигура 2.



Фиг. 2: 3D концепция на факторите изграждащи надеждността

3.3. Резюме на Глава Втора

- Обхват:
  - Тази глава се фокусира върху дефинирането на

основните термини използвани в изследването – „потребител“, „организация“, „контрол“, „доверие“, „надеждност“ и „рамка за измерване“.
    - В Глава Втора още се разглежда въздействието на GDPR върху системата за поверителност и изискванията за защита на данните.
- Методи: Дефиниции, извлечени от регламента на GDPR, работна група по член 29 и теорията за социално обучение.
- Резултати:
    - Три гледни точки (правна, психологическа и технологична) са използвани за оценка на въздействието на контрола на потребителите върху личните данни и ефектите му върху надеждността на организацията.
- Принос:
    - Подчертава значението на разглеждането на трите перспективи при оценката на надеждността на организацията и разкрива въздействието на контрола върху личните данни, процесите и системите върху надеждността.

4. ГЛАВА ТРЕТА: УСЛОВИЯ И СРЕДА ЗА ПРИЛОЖЕНИЕ НА РЕШЕНИЕТО

За да се намери решение на проблемите, очертани във въведението, са разработени специални анкети, чрез които се събират данни необходими за разбирането на нуждите на потребителя, както и се определя рамката и работните пакети за организациите. Следователно фокусът в тази глава се поставя върху методологията на процеса на събиране на данни, дизайна на проучването и структурата на анализа на данните.

Прецизно подбраната методология включва описателен и аналитичен подход за изследване на данните и тяхната структура. Основно се използва Qualtrics Stats iQ, който включва визуализация

на числа, рангове и категории и позволява анализ между различни таблици.

Изследването започва с очертаване на методите, използвани за събиране на данни, последвано от описателна оценка на получените данни. В първата част се обсъждат инструментите и процедурите за събиране, докато във втората част данните се представят, като се използват различни техники за извличане на заключения и разпознаване на модели.

В третата част се изследва връзката между отговорите. Изследват се много възможни връзки, като се представят тези, които са статистически или по друг начин значими, включително и чрез визуализации.

В четвъртия раздел се конкретизират факторите за изграждане на надеждност като се използва предходно споменатия анализ на отговорите, определя се относителната им тежест и тяхното въздействие върху системата за контрол. В хода на това разглеждане ще бъде допълнително демонстрирано как резултатите от анализа на данните се използват за изграждане на работна рамка (вж. Фигура 5).

4.1. Въведение в методологията на изследването

През март и април 2021 г. беше проведено международно уеб базирано проучване, което бе разпространено чрез Qualtrics и Google Forms. И двете проучвания са идентично структурирани, за да се гарантира, че качеството и количеството на събраните данни са сравними. Анкетата се състои от 25 въпроса с 84 подкатегории, групирани в четири раздела в това число и въвеждащата страница. Връзката към проучването на Qualtrics е споделена единствено между потребители, работещи във вътрешна технологична организация, която се занимава с различни марки в повече от 50 държави. Връзката на Google Forms е споделена с по-широка обществена група и основно е достъпна в LinkedIn и Twitter, но също така и в различни други социални платформи чрез коментари към тематично свързани публикации. Демографските въпроси на

първа страница са задължителни, а следващите въпроси могат да бъдат пропуснати или да се отговори частично.

Трите раздела за поверителност са предназначени да конкретизират факторите за изграждане на надеждност, обсъдени в предходните глави. Всеки раздел се фокусира върху различна област и включва валидиращи въпроси, за да се определят отговорите на потребителите. Всеки фактор на надеждността, т.е. организацията за контрол и обработка на данни, както и техните съответни измерения, т.е. ос x (данни, процеси и ИТ системи) и ос y (психологически, юридически, технологични фактори), показва пресечна точка с отделните личности. Следователно, разбирането на потребителите за всяко измерение, тяхното възприятие и действителното ниво на контрол върху елементите (във всяко измерение) са от особен интерес.

Вторият раздел има за цел да установи нивото на разбиране на GDPR от потребителите, за да се определи действителното им поведение при споделяне на данни. Тези наблюдения ще бъдат сравнени с желанието за споделяне на подобни данни[3] и по този начин ще бъдат използвани за целите на валидирането. В рамките на раздела ще бъдат оценени и предпочитанията за поверителност. По този начин резултатите от първия раздел позволяват да се измери средното ниво на осведоменост и експертен опит на лицата относно поверителността. По този начин правните фактори ще бъдат количествено измерими. Тази предпоставка улеснява подробната оценка на последващите отговори и посочва основните предпочитания, от които трябва да се състои интерфейсът за поверителност.

В третия раздел се оценяват психологическите фактори, за да се определи присъщото ниво на доверие, или съответно недоверие на потребителите към организациите, както и подробно се изследват измеренията и факторите за изграждане на надеждност. За да се изследват психологическите фактори в

[3] Към всеки раздел ще бъдат задавани въпроси.

дълбочина, проучването допълнително предоставя и набор от цветове, от които участниците избират този, който свързват с надеждността, което има положителен ефект върху емоциите. Събраните данни имат за цел да определят статистически значимите връзки между психологическите фактори и техния ефект върху цялостното удовлетворение от контрола върху поверителността. Това е особено интересно, тъй като, както е посочено в докторската дисертация, активният контрол на потребителите върху техните данни е ограничен.

Основният фокус на четвъртия раздел е задълбочения анализ на елементите за контрол на поверителността чрез сравнение на изявления, съдържащи оценка на параметри, които биха подобрили надеждността, както и оценка на интерфейса на кокпита за персонална поверителност (PPC). Събраните данни ще бъдат използвани за анализиране на предпочитанията за поверителност и за сравняването им с действителното поведение на участниците. Данните ще бъдат използвани и за валидиране на съществуващите резултати от изследванията. Както вътрешното, така и външното валидиране засилва значимостта на събраните данни. Пример за външно валидиране включва въпрос относно времето, прекарано в четене на политика за поверителност, което ще бъде сравнено с това колко време е необходимо за действителното ѝ прочитане. Това ще бъде извършено въз основа на изследователската статия „The Cost of Reading Privacy Policies“ (Mcdonald & Cranor, 2008).

В края на анкетата е включено пространство за свободен текст, в което могат да се попълнят допълнителни идеи и желания за подобряване на контрола на поверителността, както и обратна връзка относно качеството на анкетата. Написаното се оценява чрез Text iQ, вградена услуга за обработка на естествен език, предоставена от Qualtrics.

4.2. Процес на събиране на данни

Общо 431 участници са взели участие в анкетата, като приблизително 90% от отговорите са събрани чрез Google Forms, а останалите 10% чрез Qualtrics. По-голямата активност в Google Forms вероятно се дължи на по-широкото разпространение на проучването чрез различните платформи на социалните медии. Всяка зададена анкета съдържа 84 възможни отговора. Четири от тях – страна на пребиваване, възрастова група, професия и пол са задължителни. Тези задължителни демографски въпроси улесняват по-добрата контекстуална оценка на въпросираните. Около 7,6% от всичките 84 въпроса (вкл. задължителните) са оставени празни, т.е. 2745 от 36120 индивидуални отговора. По-голямата част от въпросите са оставени като незадължителни, като мярка за улесняване на процедурата по отговаряне.

Въпреки че потребителите могат да отговорят с „0“, което показва, че конкретното лице не притежава устройство, на някои въпросите не е даден никакъв отговор. Изтриване от списъка (Saunders et al., 2006, p.21), т.е. премахване на цели отговори от получените данни, няма да се разглежда, тъй като това намалява размера на извадката и следователно води до загуба на представителност и значимост на данните. Също така не се извършва замяна на празните клетки със средни стойности, тъй като стандартното отклонение ще бъде леко намалено и по този начин ще се получи отклонение в наблюдаваните данни. В единия или в другия случай (на замяна или незамяна), средната стойност и целия диапазон от стойности се запазва, както се запазват и извънредните стойности. Друг фактор, който е в подкрепа на незамяната на празните места със средни стойности е наличието на категориални стойности, за които не е възможно да се определи средната такава. Поради това се изисква прилагането на различни методи за елиминиране на празните места.

Hotdecking (Saunders et al., 2006, стр. 21) е едно възможно решение на проблема, тъй като идентифицира респондентите с

подобни отговори и замества липсващите стойности при непълни отговори. Тъй като данните са равномерно разпределени между различни полове, възрастови групи или професии и са необходими усилия за разработване на съответен алгоритъм за справяне с множество отговори (36 120 индивидуални отговора), се налага използването на по-прагматично решение. Прилага се комбинация от функцията Index и Randbetween за генериране на данни от съществуващото референтно разпределение, вместо това Excel да избира произволно стойности от произволен диапазон (Fish et al., 2017, стр.86). Моделът генерира стойност за категорични и числови данни въз основа на равномерно разпределение, независимо от типа на данните. Следователно честотата на съществуващите данни се запазва до голяма степен, като може да се добави известен шум, представен от колоната за относителна процентна разлика в таблицата по-долу.

Таблица 1 показва разпределението за наблюдаваните и генерираните стойности на отговорите за „Моля, посочете вида и броя устройства, които притежавате, както и това дали устройството е лично или споделено [SmartTV]“. Необходимо е да се обърне внимание, че таблицата по-долу показва само честотата на SmartTV, а не дали устройството е лично или споделено.

Table 1: Примерно сравнение на наблюдаваните и генерирани данни

стойност	**наблюдавани**	**%от всички**	**генерирани**	**%от всички**	**Относител на разлика**
0	77	24.37%	30	25.00%	-0.63%
1	220	69.62%	82	68.33%	1.29%
2	19	6.01%	8	6.67%	-0.65%
3	0	0.00%	0	0.00%	0.00%
сума	316	100%	120	100%	0.00%

В горната таблицата, 120 празни клетки са заменени с произволно генерирани стойности. За осигуряване на качеството, този тест е проведен и върху колони с по-малко, и върху такива с повече празни клетки. Резултатите са подобни както за наблюдаваните, така и за генерираните данни.

В рамките на процеса на събиране на данни съществуват неконтролируеми параметри, на които си заслужава да бъде обърнато внимание. Резултатите от Qualtrics предоставят функция за начална и крайна дата, от която се изчислява времето, прекарано за попълване на анкетата. Средното време е 18 минути, най-бързото време за реакция е $\leq$ 3 мин., а най-дългото време е 51 минути. Въпреки това, тъй като този размер на извадката представлява 10% от всички отговори, не може да се изключи, че всички наблюдения имат отклонение от тези стойности.

Освен това, съществува риск от възможни ботове, известни също като автоматизирано попълване на формуляри (Buchanan & Scofield, 2018, стр.2588). Тези ботове могат лесно да бъдат инсталирани като плъгин. Те избират произволно отговори от името на респондента, което води до по-ниско качество на данните и липса на представителност. Таймерът на страницата Qualtrics измерва времето между първото и последното щракване (Buchanan & Scofield, 2018, стр.2589), като липсата на щракване не се записва. Въз основа на отговорите дадени през Qualtrics, има 16 отговора с време между 0 и 3 минути. Прагът се определя чрез оценка на качеството и количеството на отговора, като всички респонденти с време 4 или повече минути, са отговорили напълно средно на 70 от 84 въпроса, а под границата от 4 минути са отговорили на 5 от 84 въпроса. Всъщност, данните показват, че повечето от отговорите, т.е. тези които са дадени между 4 и 30 минути до пълното завършване на анкетата, имат най-висок процент на попълнени отговори.

Сравнението с отговорите през Google Form показва, че потребителите на Qualtrics отговарят средно на 7,6 въпроса по-малко. Всички отговори под времевия праг показват подобно

поведение, т.е. те отговарят на първите няколко въпроса и пропускат останалите с цел да завършат анкетата. Това не симулира поведението на бота. Данните показват ясно, че вместо това, участниците в проучването са преустановили попълването. По този начин, използването на ботове може да бъде изключено, тъй като няма индикация за висока честота на отговори предоставени в рамките на прага до 3 минути. Случайните отговори са друг проблем, от който качеството на данните може да бъде засегнато, но това не подлежи на контрол. Начин за противодействие и ограничаване на подобни случаи е проучването да бъде предоставено чрез конкретни платформи, с цел да се насочи към различни лица, като същевременно се запази представителния набор от данни.

Не е възможно всички базирани на Google отговори, които съставляват 90% от всички събрани отговори, да бъдат разделени по потребители, тъй като това би изисквало потребителите да влизат в акаунтите си в Google. Поради липса на целесъобразност, беше взето решение това да не се прави. Оценката на времевите марки обаче не показва никакви съмнителни събития. Следователно, ще се приеме, че никой не е попълнил анкетата повече от веднъж.[4] Като обобщение може да се каже, че представеният методологичен подход представя начинът за събиране на данни, както и рамката на основното проучване.

За целите на настоящото изследване и като предпоставка за последващия анализ, различни методи за извличане и трансформиране на данни са сравнени и оценени, въз основа на тяхната ефективност. Съответното качество на данните е представено и анализирано по прозрачен начин и се предоставя на читателите чрез последващия анализ. Освен това, неконтролируемите параметри се идентифицират чрез влиянието им върху данните.

[4] Също така, се има предвид, че респондентите се стремят да увеличат шансовете си за спечелване на ваучер за подарък от Amazon

4.3. Заключение

Целта на тази глава е да се разгледат по-задълбочено данните като се анализират и оценят направените наблюдения по отношение на определянето на елементите и характеристиките, които увеличават контрола върху данните и подобряват надеждността на организациите. В крайна сметка се определят зависимите от тези данни характеристики необходими за концептуализацията на една ориентирана към потребителя система за контрол на поверителността.

Резултатите са показани в 3D концепция илюстрираща факторите изграждащи надеждността (вж. фиг. 2). Избраният подход е елементите от куба да бъдат прогресивно оценени в целево ориентиран метод. Основните резултати са документирани в рамките на този автореферат, докато подробната оценка на тази глава е поместена заедно с общите резултати от анализа в рамките на дисертационния труд.

Ключов извод, въз основа на по-широкия поглед върху данните и отделните клъстери е, че има ограничена прозрачност на обработваните данни по отношение на потребителите, тъй като те не отделят достатъчно време за разбиране на основните дейности по обработката. Беше определена и контрамярка по отношение на необходимостта от сертифициране. Спорно е дали сертификатите са ефективни като елемент за изграждане на доверие, който може да се използва за намаляване на разлома в разбирането на технологиите и процесите, използвани от организациите.

Сертификатите обаче не са заместител на независимото търсене на информация. Съществува остатъчен риск потребителите да разчитат на сертификати и да пропуснат търсенето на информация, тъй като предишен анализ (Ider, 2020a, стр. 108) установи, че повечето хора прекарват две минути в даден уебсайт, за да се запознаят с условията за поверителност. Това обстоятелство показва, че комбинацията от елементи за изграждане на надеждност може да ограничи или в най-лошия случай да

анулира ефективността на съответната друга мярка. Резултатите допълнително потвърждават, че организациите трябва да бъдат по-прозрачни и да предоставят допълнителна информация както за своите дейности по обработката, така и по отношение на използваните технологии, тъй като това са двете области, в които даденото лице не може упражнява активен контрол, т.е. следователно правото на потребителя трябва да зависи от качеството и количеството на информацията, предоставена от организацията[5].

Общо заключение, което може да се направи от наблюденията и следователно от гледната точка на потребителите е, че респондентите разбират и правят разлика между различните категории лична информация. Участниците в проучването изглежда, че имат повече предразсъдъци и са по-малко склонни да търгуват с чувствителните си лични данни, докато се чувстват по-удобно да споделят нечувствителни данни срещу по-малка отплата.

Подробният преглед на клъстерите от сегменти допълнително позволява стесняване и уточняване на отделните елементите на факторите за изграждане на надеждност. Предпочита се, функциите, които намаляват търсенето на информация да са: достъп до информация, прозрачност на обработката на данни и използване на неспециализиран език, което улеснява лесното разбиране и придава допълнително значение на информацията за поверителност. Това е начин за подобряване на работата с политиките и отговаряне на очакванията на потребителите.

Анализът акцентира върху елементите, които са от по-голямо значение за потребителите в контекста на работата с условията за поверителност на организациите. Съответно, резултатите от изследването потребителските очаквания показват,

[5] Вж. Фиг. 16 за подробности, цветовата схема е използвана за подчертаване на активната сила на потребителите да упражняват контрол върху своите данни.

че обикновеният текст е по-малко предпочитан в сравнение с по-лесно достъпните блокове, организирани в подтеми и подкрепени от интерактивни икони и видеоклипове, които подобряват разбирането на съдържанието.

Като допълнение може да се каже, че достъпът до лични данни е силно свързан с по-високо възприятие за контрол и по този начин с повишаване на надеждността. Този достъп се улеснява чрез опростена навигация в потребителския интерфейс, която изисква по-малко, но избрани функции.

Противно на характеристиките на създаването на надеждност, представени по-горе, връзките към фен страници (напр. във Facebook, Twitter, Instagram) не засягат възприятието на потребителите за психологически контрол върху данните, нито променят значително доверието. Този казус поставя два въпроса, първо, да се разбере дали потребителите правят ефективна разлика между връзки към фен страници и сертификати на официални органи (напр. EDPS, ICO, ISO, NIST) и второ, да се оцени влиянието на фен страниците върху развитието на надеждността на организациите. Следователно, основният пропуск, който беше установен по отношение на подобряването на контрола и надеждността, е ниското ниво на ангажираност на потребителите към условията за поверителност на организациите. И все пак, необходимостта от по-голяма ангажираност и подобряването на информираността за поверителност се счита за висок приоритет за хората. Това показва, че има противоречие между отношението и действителното поведение на потребителите, което подкрепя констатациите на Коколакис при изследването на феномена *парадокс на поверителността* (Kokolakis, 2017, стр. 124).

Валидирането на дихотомията отношение – поведение бе извършено чрез въпроси, които от една страна изискват от потребителите активно да се ангажират с потребителския интерфейс на макет PPC, докато друг набор въпроси бяха насочени към определяне на тяхното отношението. Сравнявайки резултатите от предишни анализи, може да се заключи, че при хипотетични

постановки, т.е. изводи базиращи се на самооценка (отразяващи отношението), а не на наблюдение (отразяващо поведението), потребителите са склонни да бъдат по-оптимистични и да имат по-голяма увереност относно своите способности и отношение към упражняването на потребителските си права, отколкото измерването на действителното им поведение доказва. По отношение на действителните цифри, делтата на дихотомията е 32%, т.е. отношението се оценява с около ⅓ по-високо от действителното поведение.

Достъпът до информация и данни, както и изтриването на данни, показват най-голямо несъответствие със средна делта от 64%. Следователно, приложението на централизирана система за контрол на поверителността от страна на потребителите би намалило значително делтата, произтичаща от дихотомията.

И накрая, само 5% от всички респонденти са предоставили своя имейл адрес, за да участват в томболата. Въпреки това, валидирането на данните с цел оценка на дихотомията на респондентите не показва отклонение от останалите 95% и следователно не се счита за убедителна и значима за това изследване.

В обобщение, главата предоставя подробни доказателства за елементите на факторите изграждащи надеждността. Като допълнение беше подобрено количественото определяне и оценката на характеристиките за подобряване на контрола на данните, както и определянето на надеждността на организациите. Установено е, че поведенческото възприятие силно се отклонява от действителното поведение и че правният, както и технологичният контрол върху данните, процесите и ИТ системите играят второстепенна роля и са силно повлияни от нагласите на участниците в проучването.

4.4. Резюме на Глава Трета

- Обхват:
  - Основният принос в трета глава е методологията използвана при събирането и анализа на лични данни, както и определянето на факторите изграждащи надеждността от гледна точка на потребителите и на организациите.
- Методи:
  - През март и април 2021 г. беше проведено международно уеб базирано проучване с помощта на Qualtrics и Google Forms. Проучването се състои от 25 въпроса с 84 подкатегории, групирани в четири раздела, насочени към установяване на нивото на информираност и експертиза на потребителите относно поверителността, доверието към организациите, оценката на елементите за контрол на поверителността и обратната връзка за качеството на проучването.
- Резултати:
  - По-голямата част от отговорите са събрани чрез Google Forms (90%) а по-малката – чрез Qualtrics (10%). Резултатите имат за цел да измерят средното ниво на информираност по отношение на поверителността, да сравнят предпочитанията за поверителност с действителното поведение, да валидират съществуващите резултати от изследванията и да определят факторите за изграждане на надеждност.
- Принос:
  - Резултатите предоставят представа за информираността и поведението на потребителите относно поверителността и тяхното доверие към организациите, което ще подпомогне разработването на ориентирана към потребителя система за контрол на поверителността.

- Заключение:
    - Глава 3 представя методологията за събиране и анализ на лични данни, използвана в изследването. Резултатите дават представа за информираността и поведението на потребителите относно поверителността и тяхното доверие към организациите, което ще допринесе за разработването на ориентирана към потребителите система за контрол на поверителността.

5. ГЛАВА ЧЕТВЪРТА: „ЕКСПЕРИМЕНТАЛНА ВЕРИФИКАЦИЯ“

5.1. Резултати от изследванията

Сравнението на вероятностите за адаптивност на сходните системи за поверителност (вж. Фиг. 1) е основа да бъде предложена входна стратегия, която намалява техническата тежест при прилагането на предвидената система за контрол на поверителността. Предимството на такава стратегия е повишаването на оперативната реализируемост, осигурено чрез поверителност посредством специализирани мерки, като хостинг на услуги и съхранение на данни, базирани в рамките на ЕС, централизирано разработване и поддръжка на интерфейса и улесняването му чрез приложно-програмен интерфейс (API) . И все пак, по-малките или разполагащи с по-малък технологичен капацитет организации, които са без необходимите компетенции и ресурси, могат да се затруднят при свързването с такава система.

Второ, действителните условия за пълноценна поверителност при организациите не могат да бъдат проверени и това представлява ограничение в изследването, което трябва да бъде критично погледнато. Въпреки оценката на резултатите от външни изследвания, както и цялостните пазарни проучвания по отношение на пълноценното съответствие с GDPR при организациите, истинското състояние не може да бъде напълно отразено. Това обстоятелство е важно да се има предвид, тъй като

то ще повлияе на успеха и функционалността на предложената система за контрол на поверителността. Това допълнително ще засегне надеждността на организациите, тъй като концептуализираната рамка за оценка на надеждността е частично базирана на пълноценността на съответствието с GDPR при организациите. В рамките на това изследване, липсата на точност и сигурност в обстоятелствата може да бъде частично компенсирана чрез външни механизми за сертифициране.

Трето, ограничението в обема на политиката за поверителност се счита от респондентите за необходимост, която подобрява ефективността при спазването на изискванията и допълнително спомага за изграждане на надеждност и за подобряване контрола над данните. Намаляването на съдържанието на правилата обаче може да бъде контрапродуктивно, тъй като ограничава организациите при изпълнението на изискванията за отчетност за своите дейности по обработката на данни. В по-широк смисъл, това води до повече затруднения от страна на организациите да отразяват прозрачно условията за поверителност. Това е особено важно, тъй като тенденцията показва, че въвеждането на нови и допълнителни дейности по обработка на личната информация, т.е. разширяването на случаите на прилагане, води до разширяване на текста на политиката за поверителност. Това обстоятелство поставя пречки пред краткото изложение на съдържанието на политиките, които същевременно трябва изчерпателно да отразяват операциите.

И накрая, според някои организации, безспорна отговорност на лицето е да проучи задълбочено условията за поверителност (Mcdonald & Cranor, 2008, стр.568). Това изследване обаче доказва, че организациите носят голяма отговорност и следователно имат задължението да предоставят удобен за потребителя интерфейс, като подчертаят онези специфики на дизайна, които подобряват ангажираността с условията за поверителност, с цел в крайна сметка да подобрят контрола на данните на потребителите и надеждността на системата. Още по-голямо значение се придава

на въздействието на регулаторите, тъй като те функционират като свързващо звено между организациите и отделните личности. Следователно, критичен фактор за успешното и ефективно спазване на поверителността е скоростта и навременността на регулаторите при приемането на закони.

Ако организациите се противопоставят или дори не успяват да изпълнят изискванията за отчетност по отношение на защитата на данните, регулаторите трябва да се намесят, за да осигурят ефективното им спазване. Изследването на оперативната реализируемост подчертава необходимостта от симбиоза между законови мерки и организационни усилия за да се отговори на изискванията и да се насърчи въвеждането на GDPR, като в крайна сметка се постигне ефективно спазване на поверителността чрез по-добро ангажиране на потребителите. Критични фактори за успех са основните организационни капацитети и ресурси, както и навременното прилагане на мерките. В разработената идея за поверителност, най-малко контролируемият и носещият най-голямо предизвикателство параметър е действителната степен на пълноценност на организациите по отношение на поверителността.

В дисертацията се дават не само правната оценка и съответните изискванията, но и се полагат основите на анализа на техническия контрол. Оценката на правния контрол основно допринася за определянето и очертаването на потребителските права, които могат да бъдат активно и пасивно упражнявани. В този смисъл, правата на потребителите са сегментирани по ниво на важност, което довежда до спецификация на функциите на системата за контрол и спецификации на потребителския интерфейс, т.е. до по-добра прозрачност и по-лесен достъп до права от по-висок ранг.

Техническият контрол се проявява в ефективното инициализиране на правните критерии, включително и по-специално в упражняването на потребителски права от физически лица, както и във възможността на организациите да спазват правните стандарти чрез специално проектирани насоки за

поверителност, които позволяват организационен контрол върху оперативното (свързано с бизнес процеса) и информационно ниво на системата. Следователно анализът предоставя ясни насоки за приложение на системата в съответствие със законовите изисквания.

Оценката на психологическия контрол показва, че възприятието за контрол в различните измерения силно корелира с предоставянето на опростен и удобен за потребителя UI и UX. Съществено откритие е намаляването на разходите за време за прочитане на политиките за поверителност. Съществува изключителна дихотомия между действителното време, изразходвано за прочитане на политиките, т.е. времето, изразходвано за прочитане на условията на поверителността, спрямо времето, необходимо за пълното прочитане на тези политики. Последното не измерва и не включва нивото на разбиране, а само времето, прекарано в четене. Съществуването на разлика между самоотчетените и наблюдаваните поведения, анализирани във външното проучване, се потвърждава в рамките на проучването, проведено за тази дисертация[6].

Следователно, първоначална стъпка в подобряването на контрола и надеждността е намаляването на тежестта на търсенето на информация и свързаното с това време за достъп и обработка на информацията. Оценката подчертава, че опитът на потребителите, т.е. възприемането на условията за поверителност, тяхното представяне, съдържание, дължина, дизайн на интерфейса и навигация съществено влияят върху разходите на време.

Отличителна характеристика на възприятието за психологически контрол е неговото въздействие върху поведението на потребителя. Докато правните и техническите аспекти могат да се разглеждат като външни средства или канали за ефективно

[6] Прилагането на функции за намаляване на времето може да бъде видяно в резултатите от правната и техническата оценка, като в предходния анализ му е отделено необходимото внимание.

прилагане на функциите за контрол, психологическият контрол е преценката на дадено лице с абсолютни права или влияние върху собствената му лична информация, съхранявана във владение на трети лица.

Това от своя страна се отразява на надеждността и на третите страни, тъй като надеждността е степента на сигурност на организациите и респективно склонността на потребителите за споделяне на данни с тези организации. Въпреки че вътрешното възприятие на потребителите за чувствителността на данните е ключов фактор за желанието и честотата на споделянето им, има наблюдения, че доверието и готовността за споделяне на данни се увеличават въз основа на нивото на контрол, което потребителите могат да упражняват, независимо от типа данни.

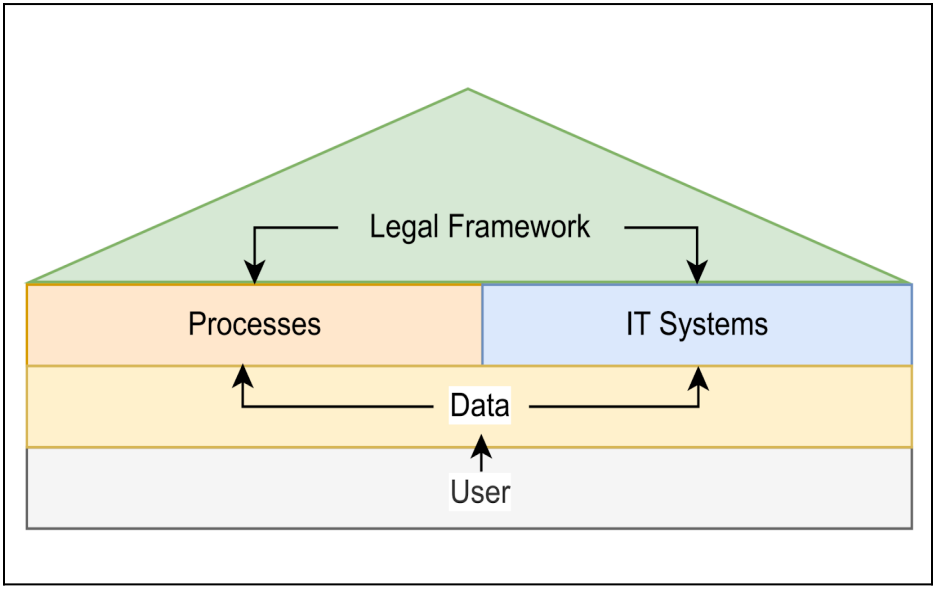
Като допълнение, за по-доброто разбиране на психологическите поведенчески модели на потребителите, беше анализирано влиянието на цветовете върху надеждността. Установено е, че доверието на потребителите в организациите може да бъде по-активно и по-силно повлияно от дадени цветове, отколкото от други. Почти всеки втори участник посочва, че синият цвят има най-силен ефект за изграждане на доверие, следван от зеленият, което се отнася за 25% от участниците. Такива цветове намаляват избягването на риска и пряко влияят върху състоянието на чувствата на потребителите, т.е. насърчават релаксирането и намаляват стреса, като същевременно подобряват надеждността. За да се запази корпоративната идентичност, допълнително беше предложено цветовете, които изграждат доверие да бъдат прилагани единствено към централизираната система за контрол на поверителността. Предвид установеното по-горе, психологическото влияние може да се каже, че придобива по-висока тежест от възприятието на правния и технически контрол за постигане на ефективна надеждност. В крайна сметка, една удобна за потребителя система за контрол, която да намалява сложността и да благоприятства намаляването на изразходвано време, да подобрява възможностите за индивидуална преценка, свързани с ефективното

упражняване на права, съчетана с използването на специфични цветове за интерфейса, проявени в симбиозата на юридически, технически и психологически характеристики води до ефективен контрол и подобряване на надеждността.

5.2. Спецификация на изискванията за системни модули

Модулите на системата за управление са извлечени от куба за поверителност (фиг. 2). Те се отнасят до функциите, на системата за контрол, които имат за цел ефективно да повишат надеждността от гледна точка на потребителя. Въз основа на така оценените характеристики са формулирани атрибути за контрол на поверителността. Този процес улеснява моделирането на верига от зависимости и техните причинно-следствени връзки в под-сегментите и в различните области на кръстосаните таблици. Кубът, създаден като многомерна кръстосана таблица, разделя организацията (ос x), контрола (ос y) и критериите за сегментиране (ос z). Оста x е разбита на данни, процеси и ИТ системи, а оста y на психологически, правни и технологични контролни елементи. Оста z е подразделена на възрастова група, професия и потребител на устройство. Всяка област на кръстосаната таблица се състои от определени параметри за оценка, които са директно представени в проучването. Резултатите от анализа установиха, че правната рамка (фиг. 3) функционира като юридически гръбнак за упражняване на потребителски контрол. Това е интерфейсът между потребители и организации и следователно има най-голямо въздействие, тъй като дори и малки промени в законовите изисквания засягат всички последващи аспекти в куба а оттам и контрола върху данните от гледна точка на потребителя.

С оглед на естеството на бизнес операциите те определят обработката (използването), запазването и изтриването на данните.



Фиг. 3. Опростена структура на симбиозата между основните елементи.

По същество, технологичните ресурси управляващи обработката на данни могат да се осъществят само при предварително определяне на правните граници, упоменати в политиката за поверителност на дадена организация. Правните граници винаги са в строго съответствие с GDPR, докато дейностите по обработване варират в зависимост от естеството на бизнес операциите. Постигането на синхронизация на законовите изисквания и оперативните дейности е най-голямото предизвикателство за организациите според резултатите от това изследване. В допълнение, възприятието за психологически контрол е жизненоважен ключов фактор, който трябва да бъде подкрепен с технологични средства. Триадата на поверителността, представена от трите стълба – правни изисквания, потребител и организация[7] – е необходима за ефективния контрол на поверителността и

[7] Организацията включва данни, процеси и ИТ системи (фиг. 2).

изграждането на организационна надеждност. При липсата на тази основа, упражняването на ефективен контрол в правилната степен не е постижимо.

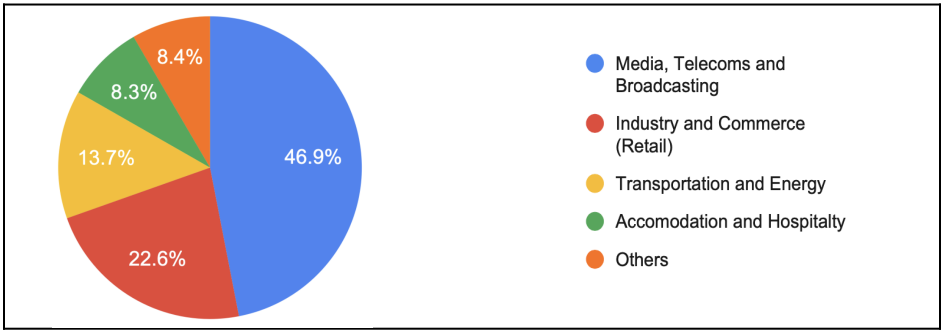
5.3. Приложимост на концепцията на изследването

Предходният синопсис подчертава характеристиките на дизайна за потребителския интерфейс за поверителност. По принцип, системата за контрол изпълнява посредническа функция, тъй като води до увеличаване на ангажираността на потребителите в работата на организациите, което води до повишена готовност за споделяне на лични данни.

В допълнение към определянето на функциите, които насърчават ефективния контрол, агрегирането на контролните модули води до избора на области, и конкретизирането на някои аспекти, които да бъдат подробно описани, както и до изясняване на обхвата на съдържанието. Тези мерки повишават характеристиките на интерфейса на системата за управление. Освен това беше идентифицирана дихотомия между самоотчетеното и наблюдаваното поведение по отношение на ангажираността с практиките за поверителност, които бяха подобрени чрез по-достъпни функции, които улесняват ангажираността на потребителите. Лесният достъп до технически и организационни мерки за сигурност също е допълнителна мярка, която улеснява разбирането от страна на потребителите. В резултат на това беше включено ефективно релевантно съдържание за поверителност и се постигна по-добро разбиране, като по този начин допълнително се потвърди приложимостта на изследователската концепция.

Тази разработка потвърждава резултатите от референтно изследване, което показва, че системата за контрол изгражда и подобрява корпоративната надеждност (Coletti et al., 2005, стр. 479).

Бенефициенти на системата са както физически лица, така и организации. Двете страни са или непосредствено предоставящите ресурса, т.е. потребителите, които предоставят лични данни, или са крайният бенефициент на такива данни, т.е. организациите, които ги използват. В последния случай възникват изисквания за съответствие и отчетност, които ще бъдат изпълнени чрез прилагане на системата за контрол на поверителността. И двете заинтересовани страни споделят резултата, т.е. това е продукт или услуга, използвани или произведени, с характеристики общи за двете страни. Физическите лица са основните бенефициенти, тъй като системата за контрол на поверителността ще бъде на първо място проектирана за детайлен контрол на личната информация. Основните институционални бенефициенти са всички длъжностни лица по защита на данните на Европейския съюз. Те могат да използват тази концепция като план за прилагане на мерки за подобряване на спазването на GDPR. Частният сектор също може да бъде потенциален бенефициент. В този смисъл, най-голям интерес биха имали отраслите, засегнати от глоби за неспазване на GDPR. Фигура 4 по-долу показва натрупаните пропорционални санкции, наложени на отраслите до декември 2020 г.[8]



Фиг. 4. Пропорционално разделение на бизнеса, засегнат от глоби по GDPR (Ider, 2020b).

[8] Видовете бизнес са сегментирани според предварително дефинирани етикети, предоставени от референтния източник.

Стимулът за организациите да използват услугата за контрол на поверителността е нейната повишена прозрачност, което подобрява съответствието ѝ с GDPR чрез ефективно, по-ясно и изчерпателно разкриване на личната информация на лицата. В крайна сметка, използването на подобна услуга следва също да бъде признато и удостоено с внимание от европейските служители по защита на данните и в случай на нарушение, това да води до намалени глоби за участващите организации, тъй като те могат да демонстрират усилията си по изпълнението на задълженията си по отчетността.

5.4. Бъдещи разработки

Един от основните резултати от проведеното изследване е валидация, чрез събиране на доказателства за осъществимостта на концепцията за онлайн система за контрол на поверителността. По-нататъшните изследвания трябва да включват създаване на прототип и тестване на работещ модел. Установените контролни характеристики се коригират съответно в следващ цикъл. Наред с тестването на прототипа, изследователите трябва да измерят дали дихотомията по отношение на самоотчетените и наблюдаваните стойности може да бъде стеснена или дори затворена. Тази процедура подобрява качеството на данните чрез съпоставяне на докладваната от потребителите информация и информацията записана от изследователя, като по този начин се намалява неточността на данните.

Въпреки че разработването и прилагането на закона за GDPR е резултат от съвместни европейски усилия, съществуват значителни разлики между различните надзорни органи при предоставянето на информация за най-добрите практики, насоки и дейности по мониторинга. Проучванията също показват силни различия във фактическото прилагане на глоби или наказателното преследване в случай на нарушения при защитата на личните данни. В резултат на това изглежда, че държавите-членки на ЕС нямат общ консенсус относно своите практики за защита на

личните данни и по-нататъшното сътрудничество с организациите. Следователно, това обстоятелство намалява стимула за прилагане на система за контрол на поверителността на потребителите, където усилията за активен регулаторен надзор чрез налагане на санкции са ниски. Поради това се препоръчва властите да засилят сътрудничеството си с частния и публичния сектор. От друга страна, налагането на санкции трябва да е в съответствие с усилията, които юрисдикциите полагат за насърчаване на спазването на изискванията за защита на личните данни. В крайна сметка, регулаторната система е неразделна част и допринася за успеха на ефективната защита на данните.

Като част от своите ангажименти, надзорните органи следва да сформират работна група за проучване на нуждите на потребителите при взаимодействието им с условията за поверителност. Освен това, към организационните трудности трябва да бъде подходено по подходящ начин чрез публикувани или предоставени от властите ресурси за насърчаване на ефективното прилагане на GDPR. Подобни мерки ще увеличат способността на правителствените агенции да подобрят изпълнението на функцията си като връзка между лица и организации. В крайна сметка това ще бъде от полза и за потребителите, чрез повишен контрол върху техните данни, и за компаниите, чрез подобрена надеждност. Други области на изследване на неприкосновеността на личния живот също трябва да бъдат включени в определянето на рамката за измерване на нивото на съзнание, прозрачност, разбираемост, лесен достъп до информация, както да бъдат включени и насоки за ясен език. Способността за измерване на сложността, съответно, яснотата на езика е определяща за потребителите при изграждане и повишаване на доверието им, както и за по-нататъшния им контрол. Крайната цел на препоръчаното област за изследване ще насърчи силата на отделния потребител да контролира по-активно своите лични данни и да противодейства на нарастващата

тенденция на прехвърляне на контрол към организациите за обработка на данни.

5.5. Резюме на Глава Четвърта

- Въведение:
  - Основна цел на проучването бе да предложи стратегия за въвеждане на система за контрол на поверителността.
  - Насочеността на разработката е към намаляване техническите утежнения с цел повишаване на възможностите за оперативната реализируемост.
- Методология:
  - В анализа са включени също правен, технически и психологически контрол.
- Резултати:
  - Проучването показа силна корелационна връзка между удобния за потребителя UI/UX и неговото въздействие върху потребителското поведение и надеждността.
  - Съкращаването на политиката за поверителност се счита за необходима мярка, но може да доведе до ограничена прозрачност.
  - Подчертани са значението на намаляването на времето за търсене на информация и въздействието на потребителския опит върху поверителността и надеждността → пренареждане и оповестяване на правата за поверителност.
- Принос:
  - Проучването дава представа за нивото на информираност и експертиза на потребителите относно поверителността, доверието към организациите, оценката на елементите за контрол на поверителността, като също така предоставя обратна връзка относно

качеството на проучването (чрез вътрешни и външни методи за валидиране на данни).
    - Представените резултати също така валидират вече съществуващи резултати от изследвания и определят факторите за изграждане на надеждност.
    - Предложената система ще даде възможност на лицата да контролират личните си данни.
    - Противодействие на тенденцията за прехвърляне на контрол към организациите за обработка на данни.

- Ограничения:
    - Валидиране на пълноценността на организационната поверителност чрез оценка на вторични източници.
    - Организации, които са крайно отговорни за предоставянето на удобен за потребителя интерфейс с цел подобряване на контрола на данните и надеждността.

- Бъдещи изследвания:
    - Разработване на прототип за намаляване на дихотомията между самоотчетените и наблюдаваните стойности, както и неговото тестване.
    - Увеличаване на сътрудничеството между надзорните органи, частния и публичния сектор за налагане на уеднаквени санкции за нарушения при защитата на данните.

6. ОЦЕНКА НА РЕЗУЛТАТИТЕ ОТ АПРОБАЦИЯТА

Delivery Hero SE, с основната подкрепа на длъжностното лице по защитата на данни Абдулхамит Чавдар, възнамеряват да възприемат един по-ориентиран към потребителя подход за своята система за контрол на поверителността, за да насърчат доверието и увереността на своите клиенти. За целта, резултатите от изследванията се планира да бъдат имплементирани в бизнес

процесите, като по този начин се опрости спазването на GDPR и се рационализира системата за контрол на поверителността. Прилагайки резултатите от изследването към съществуващата си система, стремежът е да се оцени нейната ефективност и да се идентифицират областите подлежащи на подобрение. В крайна сметка, компанията се стреми да подобри репутацията си и да изгради доверие сред своите клиенти, като гарантира стабилни мерки за поверителност и защита на данните.

7. ЗАКЛЮЧЕНИЕ

В раздела „Заключение“ на дисертационния труд основните констатации от изследването са обобщени и интерпретирани в контекста на изследователските въпроси и хипотези. Определят се значимите тенденции и модели, които допринасят за разбирането на актуалните въпроси в областта. Обсъжда се влиянието на резултатите, включително тяхното значение за разработването на нови теории и практики, и се определят потенциални възможности за бъдещи изследвания. Направени са някои наблюдения върху ограниченията на изследването и методологичния или теоретичния му принос, които могат да предоставят информация за бъдеща работа в тази област.

Конкретно, фокусът на настоящото научно изследване е разработването на ориентирана към потребителя система за контрол на поверителността, която подпомага организациите при спазването на Общия регламент за защита на данните (GDPR), като се отчита въздействието върху обществото, неоднозначните законови разпоредби, както и технологичните аспекти. Проучването подчертава значението от намаляването на техническите утежнения и предоставянето на удобен за потребителя интерфейс, целящ подобряване на надеждността и контрола на данните на потребителите. Предложената система за контрол на неприкосновеността на личния живот дава възможност на лицата да контролират личните си данни, чрез което се

противодействия на тенденцията за прехвърляне на контрола към организациите за обработка на данни. Проучването предполага, че организациите носят голяма част от отговорността и задължението за предоставянето на удобен за потребителя интерфейс и регулатори, за да се гарантира ефективно спазване на изискванията свързани с GDPR.

Методологията на изследването включва анкети, систематичен преглед на литературата и процес на дизайнерско мислене. Също така е проведено международно уеб-базирано проучване, състоящо се от 25 въпроса и 84 подкатегории, групирани в четири раздела, целящо определяне нивото на информираност на потребителите относно поверителността, тяхното доверие към организациите, оценката на елементите за контрол на поверителността и обратната връзка за качеството на проучването. Резултатите от проучването показват силна корелационна връзка между удобния за потребителя UI/UX и въздействието върху потребителското поведение и надеждността. Проучването също така подчертава значението на намаляването на времето за търсене на информация, както и въздействието на потребителския опит върху поверителността и надеждността.

Като възможно ограничение, в проучването се посочва невъзможността да се провери пълноценността на организационната поверителност, като за преодоляването му се предлагат бъдещи разработки, включващи разработване и тестване на прототипи, както и сътрудничество между надзорните органи, частния и публичния сектор и работната група за проучване на нуждите на потребителите по отношение на свързаните с организациите трудности. Целта е да се засили индивидуалният контрол върху личните данни и да се насърчи доверието между лицата и организациите. Посочва се, че намаляването на съдържанието на политиката за поверителност, с цел подобряване на спазването на GDPR и изграждане на надеждност, може да се окаже контрапродуктивно, тъй като ограничава обема, в който организациите могат да изпълнят изискванията за отчетност. Като

цяло, основния принос на проведеното проучване е, че предоставя точни и ясни насоки за прилагането на система за контрол на поверителността, която е в съответствие със законовите изисквания и може да подобри възприемането за контрол и надеждност.

8. ПРИНОСИ ПО ДИСЕРТАЦИОННИЯ ТРУД

Представеното в дисертационния труд изследване носи нов практичен подход към настоящите предизвикателства при спазването на GDPR. Основните научни приноси на които се базира този подход, могат да се изведат като:

1. Представена е нова унифицираща рамка за спазването на GDPR, която спомага за опростяването на процеса на прилагане от страна на организациите и подобрява потребителския контрол върху личните данни чрез система за контрол на поверителността.
2. Разработена е методика за проучване информираността на потребителите относно поверителността, доверието към организациите, оценката на елементите за контрол на поверителността и обратната връзка за качеството на проучването, като се използват вътрешни и външни методи за валидиране на данни.
3. Въз основа на предложената методика са събрани ресурси чрез широкомащабно уеб-базирано допитване до граждани и организации относно практиките при прилагане на GDPR – за оценка на информираността на потребителите относно поверителността, доверието им към организациите, оценка на елементите за контрол на поверителността и обратна връзка за качеството на проучването.
4. Предложена е система даваща възможност на гражданите да контролират личните си данни, като се противодейства на тенденцията за прехвърляне на контрола към организациите обработващи данни.

5. Изведено е заключение за влиянието на контрола на личните данни, процесите и системите върху надеждността. Проучването подчертава значението на въздействието върху обществото, неоднозначните законови регулации и технологиите при оценката на организационната надеждност, като разкрива влиянието на контрола на личните данни, процесите и системите върху надеждността.

9. НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

За нуждите на изследвания са създадени уеб инструменти за събиране и анализ на данни от разнообразни източници, предоставяйки цялостно и нюансирано разбиране на проблемите, свързани със спазването на GDPR:

6. Създадени са он-лайн анкети за нуждите на изследователското проучване чрез използване на две уеб приложения, Qualtrics и Google Forms.
7. Създаден е уеб скрепер за извличане на данни от уебсайтове, което позволява събирането на подходяща информация за изследването. Чрез уеб скрепера е събирана информация за над хиляда глоби, която се анализира и контекстуализира, за да се идентифицират тенденциите в спазването на GDPR.

10. БИБЛИОГРАФИЯ

Alford, S. (2020) GDPR: A Game of Snakes and Ladders: How Small Businesses Can Win at the Compliance Game [Online]. 1st ed. Routledge. Available from: < > [Accessed 1 June 2021].

Andreoni, J. & Miller, J. (2002) Giving According to GARP: An Experimental Test of the Consistency of Preferences for Altruism. Econometrica, 70 (2).

Article 29 Working Party (2014) Opinion 05/2014 on Anonymisation Techniques 0829/14/EN [Online]. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> [Accessed 16 November 2020].

Article 29 Working Party (2016) Guidelines on the Right to Data Portability [Online]. Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35. Available from: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44099>.

Article 29 Working Party (2017) Guidelines on Transparency under Regulation 2016/679 [Online]. Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Available from: <https://ec.europa.eu/newsroom/article29/items/622227>.

Ashraf, N., Bohnet, I. & Piankov, N. (2006) Decomposing Trust and Trustworthiness. Experimental Economics, 9 September, pp. 193–208.

Betti, D., Lacey, J. & Dhoni, I. (2020) 6th GLOBAL SMARTPHONE USER SURVEY [Online]. Mobile Ecosystem Forum Ltd. m, p. 9. Available from: <https://mobileecosystemforum.com/wp-content/uploads/2020/05/MEF_Global_Smartphone_Survey_2020_Summary.pdf>.

Buchanan, E. M. & Scofield, J. E. (2018) Methods to Detect Low Quality Data and Its Implication for Psychological Research. Behavior Research Methods [Online], 50 (6) December, pp. 2586–2596. Available from: <http://link.springer.com/10.3758/s13428-018-1035-6> [Accessed 9 April 2021].

Coletti, A. L., Sedatole, K. L. & Towry, K. L. (2005) The Effect of Control Systems on Trust and Cooperation in Collaborative Environments. The Accounting Review [Online], 80 (2) April, pp. 477–500. Available from: <https://meridian.allenpress.com/accounting-review/article/80/2/477/53536/The-Effect-of-Control-Systems-on-Trust-and> [Accessed 3 January 2022].

Colman, A. M. (2003) A Dictionary of Psychology. Oxford: Oxford University Press.

ContentSquare (2020) Digital Experience Benchmark Report 2020 [Online]. p. 7. Available from: <https://go.contentsquare.com/en/digital-experience-benchmark> [Accessed 18 December 2020].

Council of Europe (1981) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. European Treaty Series No. 108 (108), p. 7.

Dehmel, S. & Kelber, U. (2020) DS-GVO Und Corona – Datenschutzherausforderungen Für Die Wirtschaft (Translation: GDPR and Corona - Data Protection Challenges for Business) [Online]. Bitkom, p. 12. Available from: <https://www.bitkom.org/sites/default/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf> [Accessed 20 December 2020].

Desnoyers, L. (2011) Toward a Taxonomy of Visuals in Science Communication. Technical Communication (Washington), 58 May, pp. 119–134.

DIMITROV, I. (2021) Invasive Apps. The pCloud Blog, 5 March [Online blog]. Available from: <https://blog.pcloud.com/invasive-apps/> [Accessed 6 May 2021].

European Commission (n.d.) Can Individuals Ask to Have Their Data Transferred to Another Organisation? [Online]. European Commission - European Commission. Available from: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en> [Accessed 3 January 2021a].

European Commission (n.d.) What Constitutes Data Processing? [Online]. European Commission - What constitutes data processing? Available from: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en> [Accessed 9 July 2021b].

European Data Protection Board (EDPB) (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default [Online]. Available from: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>.

Eurostat (2020) Annual Enterprise Statistics by Size Class for Special Aggregates of Activities (NACE Rev. 2) [Online]. Available from: <https://ec.europa.eu/eurostat/databrowser/view/sbs_sc_sca_r2/default/bar?lang=en> [Accessed 23 December 2020].

Faustino-Bauer, M. & Ider, K. (2020) Datenschutzmanagement - Ein Erfolgsfaktor bei der digitalen Transformation (Translation: Data protection management - a success factor in digital transformation). 6 / 2020 December, pp. 247–255.

Federal Ministry for Economic Affairs and Energy (BMWi) (2019) Project GAIA-X – A Federated Data Infrastructure as the Cradle of a Vibrant

European Ecosystem [Online]. Federal Ministry for Economic Affairs and Energy Public Relations. Available from: <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4>.

Federal Ministry of Justice and Consumer Protection (2017) Federal Data Protection Act (BDSG) [Online]. p. 43. Available from: <https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf> [Accessed 19 December 2020].

Fish, L. J., Halcoussis, D. & Phillips, G. M. (2017) Statistical Analysis Of A Class: Monte Carlo And Multiple Imputation Spreadsheet Methods For Estimation And Extrapolation. American Journal of Business Education (AJBE) [Online], 10 (2) March, pp. 81–96. Available from: <https://clutejournals.com/index.php/AJBE/article/view/9918> [Accessed 9 April 2021].

Forsa (2018) Forsa Umfrage: Alles unter Kontrolle?! (Translation: Forsa Poll: Everything under control?!) [Online]. Available from: <https://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-2018/forsa-umfrage-alles-unter-kontrolle/> [Accessed 19 December 2020].

General Data Protection Regulation (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

GDPR Enforcement Tracker - List of GDPR Fines (n.d.) [Online]. Available from: <https://www.enforcementtracker.com> [Accessed 29 May 2022b].

Glossary - EUR-Lex (n.d.) [Online]. Available from: <https://eur-lex.europa.eu/eli-register/glossary.html> [Accessed 9 July 2021c].

Grashöfer, J., Degitz, A. & Raabe, O. (2017) User-Centric Secure Data Sharing: Exploration of Concepts and Values. [Online]. Available from: <https://dl.gi.de/handle/20.500.12116/3888> [Accessed 30 September 2020].

Gul, F. A. (1983) A Note on the Relationship between Age, Experience, Cognitive Styles and Accountants' Decision Confidence. Accounting and Business Research, 14 (53) December, pp. 85–88.

Haas, A., Wagner, C., Miyashita, G., Hall, K., Fiorillo, C., Heath, J., Gol, H., McDougal, T., Huggins, K., Laurenza, A., Small, R., Orkin, S., Rayment, S., Byrne, Y., Datwani, H., Campos, F., O'Brien, C. & Emerson, T. (2019) Global Contact Center Survey [Online]. p. 16. Available from: <https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/blog/blog-20190513-2019%20globalcontactcentersurvey.pdf> [Accessed 16 April 2021].

Ider, K. (2020a) Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity. vol. 24. Berlin: Shaker Verlag GmbH, pp. 103–110.

Ider, K. (2020b) based on data from Enforcementtracker.com. (n.d.) GDPR Enforcement Tracker - List Of GDPR Fines. [online] Available from: <https://www.enforcementtracker.com/> [Accessed 12 December 2020].

Jiang, Z., Tolido, R., Jones, S., Hunt, G., BUDOR, I., Bartoli, E., Linden, P. van der, Buvat, J., Theisler, J., Wortmann, A., Cherian, S. & Khemka, Y. (2019) Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century [Online]. Available from: <https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf> [Accessed 18 August 2020].

Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations [Online]. NIST SP 800-53r4. National Institute of Standards and Technology, p. NIST SP 800-53r4. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> [Accessed 14 December 2020].

Kemp, S. (2020) Digital 2020: Global Digital Overview [Online]. DataReportal – Global Digital Insights. Available from: <https://datareportal.com/reports/digital-2020-global-digital-overview> [Accessed 13 November 2020].

Kerkhof, P. & Noort, G. (2010) Third Party Internet Seals: Reviewing the Effects on Online Consumer Trust. Encyclopedia of E-Business Development and Management in the Global Economy, 2 January.

Kissel, R. L. (2013) Glossary of Key Information Security Terms. U.S. Department of Commerce.

Kokolakis, S. (2017) Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. Computers & Security [Online], 64 January, pp. 122–134. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0167404815001017> [Accessed 14 December 2021].

Lintvedt, M. N. (2021) Putting a Price on Data Protection Infringement. International Data Privacy Law [Online], December, pp. 1–15. Available from: <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipab024/6453860> [Accessed 17 January 2022].

Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M. & Barelka, A. J. (2011) Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network. Human Factors [Online], 53 (3) June, pp. 219–229. Available from: <https://doi.org/10.1177/0018720811406726> [Accessed 23 December 2020].

Mcdonald, A. M. & Cranor, L. F. (2008) The Cost of Reading Privacy Policies. I/S: A Journal Of Law And Policy, 4:3, pp. 544–568.

Ministry of Communications and Information (2014) Personal Data Protection Regulations 2014 [Online]. vol. Y03.002.001.EV30/13; AG/LLRD/SL/227A/2012/4 Vol. 2. Ministry of Communications and Information Singapore. Available from: <https://sso.agc.gov.sg/SL/PDPA2012-S362-2014?DocDate=20200528>.

Monteiro, A. F. (2019) First GDPR Fine in Portugal Issued against Hospital for Three Violations. 13 January [Online blog]. Available from: <https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/> [Accessed 17 January 2022].

National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems [Online]. NIST FIPS 200. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST FIPS 200. Available from: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf> [Accessed 19 December 2020].

Osmanoglu, T. E. (2013) Identity and Access Management: Business Performance through Connected Intelligence. Amsterdam, [Netherlands]: Syngress, an imprint of Elsevier.

Pancer, E., McShane, L. & Noseworthy, T. J. (2017) Isolated Environmental Cues and Product Efficacy Penalties: The Color Green and Eco-Labels. Journal of Business Ethics, 143 (1) June, pp. 159–177.

Personal Information Protection Commission (2016) Amended Act on the Protection of Personal Information (Tentative Translation) [Online]. Japan. Available from: <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> [Accessed 26 December 2020].

PricewaterhouseCoopers (2018) Aktueller Stand zur Umsetzung der EU-DSGVO bei Leasinggesellschaften in Deutschland (Translation: Current status on the implementation of the EU GDPR at leasing companies in Germany) [Online]. PwC. Available from: <https://www.pwc.de/de/finanzdienstleistungen/leasing/aktueller-stand-zur-umsetzung-der-eu-dsgvo-bei-leasinggesellschaften-in-deutschland.html> [Accessed 18 August 2020].

Qualtrics.com (n.d.) Response Quality [Online]. Available from: <https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/response-quality/> [Accessed 26 March 2021].

Rotter, J. B. (1980) Interpersonal Trust, Trustworthiness, and Gullibility. American Psychological Association, 35 (1) January, pp. 1–7.

Ruud, T. F. (2003) The Internal Audit Function : An Integral Part of Organizational Governance. In Bailey, Andrew; Gramling, Audrey & Ramamoorti, Sridhar (Ed.): Research Opportunities in Internal Auditing. Altamonte Springs : IIA-The Institute of Internal Auditors, pp. 73–96.

Sambra, A. V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A. & Berners-Lee, T. (n.d.) Solid: A Platform for Decentralized Social Applications Based on Linked Data. p. 16.

Saunders, J. A., Morrow-Howell, N., Spitznagel, E., Dore, P., Proctor, E. K. & Pescarino, R. (2006) Imputing Missing Data: A Comparison of Methods for Social Work Researchers. Social Work Research [Online], 30 (1) March, pp. 19–31. Available from: <https://academic.oup.com/swr/article-lookup/doi/10.1093/swr/30.1.19> [Accessed 9 April 2021].

Sjöberg, M., Chen, H.-H., Floréen, P., Koskela, M., Kuikkaniemi, K., Lehtiniemi, T. & Peltonen, J. (2017) Digital Me: Controlling and Making Sense of My Digital Footprint [Online]. In: Gamberini, L., Spagnolli, A.,

Jacucci, G., Blankertz, B. & Freeman, J. ed., Symbiotic Interaction. vol. 9961. Cham: Springer International Publishing, pp. 155–167. Available from: <http://link.springer.com/10.1007/978-3-319-57753-1_14> [Accessed 1 October 2020].

Skinner, M. (2013) Emotional Control [Online]. In: Gellman, M. D. & Turner, J. R. ed., Encyclopedia of Behavioral Medicine. New York, NY: Springer New York, pp. 671–673. Available from: <https://doi.org/10.1007/978-1-4419-1005-9_950>.

Sobers, R. (2020) How Privacy Policies Have Changed Since GDPR. Inside Out Security, 295T15:07:08-04:00 [Online blog]. Available from: <https://www.varonis.com/blog/gdpr-privacy-policy/> [Accessed 7 May 2021].

Statistisches Bundesamt (Destatis) (2020) Bevölkerung Und Erwerbstätigkeit - Haushalte Und Familien, Ergebnisse Des Mikrozensus (Translation: Population and Employment - Households and Families, Results of the Microcensus) [Online]. Statistisches Bundesamt (Destatis), pp. 43–52. Available from: <https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Haushalte-Familien/Publikationen/Downloads-Haushalte/haushalte-familien-2010300197004.pdf?__blob=publicationFile>.

Su, L., Cui, A. & Walsh, M. (2019) Trustworthy Blue or Untrustworthy Red: The Influence of Colors on Trust. Journal of Marketing Theory and Practice, 27 July, pp. 269–281.

Sutter, M. & Kocher, M. G. (2007) Trust and Trustworthiness across Different Age Groups. Games and Economic Behavior [Online], 59 (2) May, pp. 364–382. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0899825606001199> [Accessed 19 June 2022].

Truong, N. B., Sun, K., Lee, G. M. & Guo, Y. (2020) GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security, 15, pp. 1746–1761.

Ustaran, E. ed. (2019) European Data Protection: Law and Practice. Portsmouth, NH: an IAPP Publication, International Association of Privacy Professionals.

VandenBos, G. R. ed. (2015) APA Dictionary of Psychology (2nd Ed.). Washington: American Psychological Association.

Vaske, H. (2022) European Cloud Project Gaia-X Is Stuck in the Concept Stage [Online]. CIO. Available from: <https://www.cio.com/article/308818/european-cloud-project-gaia-x-is-stuck-in-the-concept-stage.html> [Accessed 1 May 2022].

Voigt, P. & Bussche, A. von dem (2017) The EU General Data Protection Regulation (GDPR). Cham: Springer International Publishing.

Wasaya, A., Saleem, M. A., Ahmad, J., Nazam, M., Khan, M. M. A. & Ishfaq, M. (2021) Impact of Green Trust and Green Perceived Quality on Green Purchase Intentions: A Moderation Study. Environment, Development and Sustainability: A Multidisciplinary Approach to the Theory and Practice of Sustainable Development, 23 (9) September, pp. 13418–13435.

Werliin, R. & Kokholm, M. (2020) Insights 2020 - Device Usage [Online]. AudienceProject. Available from: <https://www.audienceproject.com/wp-content/uploads/audienceproject_study_device_usage_2020.pdf?x56703> [Accessed 18 December 2020].

White, H. & Carvalho, S. (2005) Combining the Quantitative and Qualitative Approaches to Poverty Measurement and Analysis. EconWPA, Development and Comp Systems, January.