An exploration of whether current Privacy by Design models meet the need to gain Informed Consent.

by

Nicholas Williams

May 2023

A thesis submitted in partial fulfilment of the requirements of the University of Brighton for the degree of Master in Philosophy

Abstract

In 2018 the UK implemented the European Union's (EU) General Data Protection Regulations (GDPR) into law as the Data Protection Act 2018. This significantly increased the personal data requirements organisations needed to meet to be compliant.

One of these requirements is that organisations now need to gain informed consent from data subjects to use their personal data. I wanted to explore if current privacy by design models can keep up with the change in data protection regulations. If they do not seem to be able to do so, I wanted to explore if they could be extended to gain informed consent.

The thesis looks at several privacy by design models, and then presents a model that can provide a foundation for future privacy by design frameworks can to be extended to gain informed consent from data subjects. The thesis also compares the new framework against an existing privacy by design framework, to show how it provides additional functionality.

"I'd take the awe of understanding over the awe of ignorance any day."

Douglas Adams, The Salmon of Doubt

Table of Contents

List of Tables

List of Figures

Definitions and Acronyms

Several key terms are used throughout this document and are defined here:

Abbreviation	Long Form
GDPR	General Data Protection Regulations
EU	European Union
DPA	Data Protection Act 2018
CNIL	Commission nationale de l'informatique et des Libertés
ICO	Information Commissioner's Office
HMRC	His Majesty's Revenue and Customs
CMS	Consent Management System
gICS	generic Informed Consent Service
SMS	Short Message Service
Pbd	Privacy by design
Pbdf	Privacy by default
DA	Data Auditor
DS	Data Subject
DC	Data Controller
DP	Data Processor
DAL	Data Audit Logs
PD	Personal data
DO	Data Owner
SO	Service Owner

DSG Data Subject Guardian

NHS National Health Service

DEFeND Data govErnance For supportiNg gDpr

ICBDF Informed Consent by Design Framework

ICBDL Informed Consent by Design Language

ICBDM Informed Consent by Design Model

Acknowledgements

To everyone that has supported me in my studies. I would not have been able to do it without you.

Declaration

Declaration I declare that the research contained in this thesis, unless otherwise formally indicated within the text, is the original work of the author. The thesis has not been previously submitted to this or any other university for a degree and does not incorporate any material already submitted for a degree.

Signed N Williams

Dated 22/05/2023

1 Introduction

1.1 Current situation and background.

The UK's Data Protection Act 2018 (DPA) introduced a robust set of controls relating to how organisations can use personal data. Each of the member states of the EU were and continue to be required to implement the GDPR into their own laws. Meaning that the EU member states, as well as the UK, all have the same regulatory framework regarding data protection. The DPA is the UK's implementation of the European Union's (EU) General Data Protection Regulations (GDPR). When the UK left the EU the DPA was been updated in January 2021, to enable it to work effectively in a UK context. This means that an organisation holding personal information may need to ensure that they are complying with the DPA for UK citizens and GDPR for EU citizens. For this thesis it is assumed that the requirement of gaining *informed consent* is required for both sets of legislation.

The DPA includes a more substantial need for organisations to be able to show that they have gained informed consent from data subjects[1] (their customers) to be able to use and process their personal data. This is especially true when comparing the current legislation with the previous data protection act, enacted in 1998. The fines that can now be levied on organisations for breaching the DPA are now noticeably more severe than they used to be. In addition, the requirements of the DPA are now more strongly worded. The wording is now typically "Must be …" as opposed to "Shall be …" (Practical Law Employment, Employment and Practical Law Employment, 2020).

In line with the updates in the law regarding data protection, in the world of creating computer systems the concept of Information Security has been moving from a post post-launch add on to being considered while the system is first being created. In recent years the concept of privacy by design (Pbd) (Wuyts, Scandariato and Joosen, 2014) has appeared. Additionally, privacy by default (PbdF) and the implementation of privacy and security are taking place at the earliest stages of a systems' lifecycle.

[1] Is "… [a] living individual on whom personal data is held"(ICO, 2020b)

This work will focus on looking at Pbd models because article 25 paragraph 2 of the GDPR states that "The controller shall implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed." (European Union, 2016)[emphasis is that of the author]. This is taken to mean that Pbd methods need to be used.

In addition to the increasing legal requirements, there has been a growth in interest in the protection of personal information from the media. Examples of this include coverage of:

- The UK's NHS Covid-19 mobile application coverage in 2020 (Channel 4 news, 2020) by Channel 4 news.
- Cambridge Analytica/Facebook coverage in 2018 by Channel 4 news (Channel 4 news, 2018) and the Guardian newspaper in the UK (Wong, 2019).
- The Pegasus Project coverage in 2021 by the Guardian newspaper in the UK (McKernan, 2021).

Since the introduction of the DPA in 2018, the ICO[2] has fined, or otherwise punished, a number of organisations for data breaches that have also been covered by the media including:

- EasyJet (Guardian, 2020), when a hack into their systems led to email addresses, travel details and payment card details being stolen.
- Amazon, Apple, and Google (BBC, 2019) accused of not fully complying with data subject requests to see their own data.
- Google fined €50000000 (CNIL, 2019) for the use of personalised adverts that they did not have clear and valid consent for.
- A Portuguese Hospital given a €400000 fine (Meneszes, 2019), for violations including a lack of implementation of measures to prevent unlawful access to personal data.
- The UK's HMRC (ICO, 2019b) for not giving data subjects sufficient information about how recordings of their voice would be used in identifying them when they called the HMRC.
- British Airways fined £118,390,000 (ICO, 2019c) due to an incident in which some traffic intended to go to the British Airways website was diverted to a fraudulent website. That led to around 500000 data subjects' personal data being breached.

[2] ICO or its counterparts in other EU member states.

- The Marriot Hotel chain fined $99,000,000 (ICO, 2019d) for an incident that exposed personal data of around 339,000,000 guest records globally.
- Amazon fined $886,600,000 (BBC, 2021) for processing personal data in a way that did not comply with EU law.[3]

Across the countries that have implemented GDPR there have been 518 fines issued relating to not gaining the full consent of a data subject with the fines totalling €465,992,081(CMS Law, no date). The categories used in these numbers are "Insufficient Data Processing Agreement", "Insufficient Fulfilment of data subjects" rights" and "Insufficient legal basis for data processing".

Organisations also need to consider the actions of third parties. A third parties' actions can tarnish the reputation of the Organisation. For example, a private provider of student accommodation used by students of the University of Brighton was found to have put into general waste students' belongings including passports and other documentation that could be used to identify students (BBC, 2020a). While the University of Brighton had no part of this, the University's name was used in media headlines reporting this incident, potentially damaging the reputation of the university.

It's not just organisations that have fallen foul of the DPA. It has been reported that a grandmother has been ordered to delete pictures of her grandchildren from Facebook as she did not have permission from the children's parents (BBC, 2020b).

The high levels of continuing media interest in how personal data is being used and misused by organisations within the UK have likely resulted in closer attention by the public as to *whom* can access their personal data.

The ability to use personal data to target consumers directly has significant financial considerations for organisations. In 2009, $149.3 billion was spent on targeted advertising, which resulted in $1,783 trillion in sales (Wicker and Schrader, 2011). This has many important implications for organisations. Handled incorrectly there can be damaging negative media attention and, in the case of a data breach massive fines.

[3] It is reported that (at the time of writing) Amazon has won an appeal against this ruling.

An additional but significant issue that has had some media attention is how many websites ask users to give their consent to cookies. Mainstream podcasts have covered this issue from an end-user point of view, such as the podcast "Skeptics with a K" (Hall, Marshall and Howarth, 2020). The episode of Skeptics with a K criticised how some sites implemented the way they asked for consent. This podcast identified that websites often prevented users from reading a webpage until they have consented for the use of their personal data. In addition, some websites, make it difficult for users to choose the cookies they want to consent to by giving the explanations in inaccessible language, or hidden behind a Settings option, for example the Smooth Radio website.(Smooth Radio, no date)

A study examining how consumers interact with different cookie consent pop-ups suggests that consumers are confused about how cookies function (Lomas, 2019). Research indicates that consumers expect that if they do not click to consent to the use of cookies, that data is not collected about them, although this is not often the case (Utz *et al.,* 2019). It has also been shown that many consumers would engage with consent notices, but the notices do not currently offer a meaningful choice to the consumer (Utz *et al.,* 2019). If cookie consent notices were GDPR compliant, only about 0.1% of users would actually consent to the use of third-party cookies (Utz *et al.*, 2019).

How can organisations gain and importantly maintain the trust of the people whose information they hold and process?

94% of people (The Open Data Institute, 2018)[4] stated that *trust* was essential to them when deciding to share personal data with an organisation. Just 36% (The Open data Institute, 2018) said that they would share their data with an organisation, they do not know. Compliance with the current data protection regulations may be able to assist in this regard. Organisations may need a change of perspective to see privacy as a benefit as opposed to a burden. Some organisations have already started to grasp this. Apple took the step to protect users' data by encrypting all data on their devices from 2014(Allison, 2019). DuckDuckGo, a search engine, in an unusual step, diverging from most search engines, does not use personal data to provide personalised adverts. It only uses general advertising. Both Apple and DuckDuckGo offer popular services (DuckDuckGo exceeding 1 billion

[4] The survey was carried out by YouGov PLC, sample size of 2,023 adults between 28-29 November 2017. Figures were weighted and are representative of all GB adults.

search requests in January 2019 (Allison, 2019) and Apple recording quarterly sales of $58.3bn in March 2020, an increase of $3.8bn from the same time in 2019). This very much contrasts with what happened to Cambridge Analytica, who did not appear to see privacy as a benefit and is no longer operating. (House, 2020)

1.2 Changes in the legal requirements

As previously mentioned, in 1.1 “Current situation and background”, we have seen an increase in the legal requirements that organisations need to be compliant with.

For example, organisations now need to report data breaches within 72 hours of becoming aware of them (European Parliament, 2016). This means that an organisation needs to have a system of recording when a breach occurs so that the organisation’s data controller can report it to the appropriate authorities. The data controller also needs to report the violation to the data subjects clearly and plainly (European Parliament, 2016).

In addition to the above, the definition of personal data has changed. It now includes information from the online world, such as cookies and IP addresses, as well as information that has traditionally been considered personal data (e.g., name and address).

The fines that can be levied on an organisation are significantly higher than they once were. There are now two tiers of penalties that can be imposed on organisations. The first is the standard maximum fine (ICO, 2019e) which is €10 million (or sterling equivalent) or 2% of the total annual worldwide turnover of the previous year, whichever is higher (ICO, 2019e).

The second, the higher maximum is €20 million (or sterling equivalent) or 4% of the total annual worldwide turnover for the previous year, whichever is higher (ICO, 2019e).

The territorial scope of the new regulations has also been defined. If a “Controller” or “Processor” are not established within the EU and are processing personal data of EU data subjects, then the data protection regulations apply to them (European Parliament, 2016). This effectively means that EU data subjects are protected by EU law regardless of where the organisation holding and processing their personal data is based. This is relevant to UK organisations post Brexit.

Notably, the Data Protection Act 2018 defines what is meant by the "consent" of a data subject, concerning the storing and processing of their personal data. Organisations must now do much more to ensure they have real, informed consent from the data subjects. However, while the regulations state what is required, this is done in legal language [(European Parliament, 2016), Article 7], which needs considerable thought about how the requirements can be implemented into a useable system. When it comes to implementing the requirements of the regulation, the requirements need to be in a language that can be understood by those who are implementing it.

The need for privacy and consent to use data subjects' personal data also has to be balanced with the availability of being able to use that data in times of need (Robol *et al.*, 2018). An example is when a data subject is taken to a hospital. In that case, the medical staff will need to have access to the data subject's personal data before they are able to carry out appropriate care. The data subject may not be able to give consent at that time, and waiting for the data subject to give consent may be life-threatening.

The DPA, (in Part 3, Chapter 4, Section 57) sets out the implementation of data protection by design and default. This has been stated by the Information Commissioners Office to include privacy by default.(ICO, 2019a) Privacy by design concepts need to be included to help ensure compliance with this requirement (ICO, 2020a).

While in this work I am looking at how frameworks can assist computer systems in gaining informed consent from data subjects, the nature of "informed consent" will need the input from other research fields such as Education, Law, Psychology and Ethics.

Other parts of the world have introduced, or are looking to introduce, data protection laws. The US State of California has introduced the California Consumer Privacy Act of 2018 (CCPA) (State of Callifornia Department of Justice; Office of the Attorney General, 2021), which brings into force similar protections to the EU's GDPR for Californian citizens. It has also been reported that China has implemented similar data protection laws on 1st November 2021 with the Personal Information Protection Law (Ashurst, 2021) "…recalls Europe's GDPR in setting a framework to ensure user privacy" (Horwitz, 2021). Several other countries outside of the EU have started updating (or implementing) data protection legislations in response to GDPR, such as Argentina, Bahrain and Panama (Lexology, 2021)

For an organisation, the cost of completely re-engineering their current way of working to ensure they are compliant with current DPA legislation, may be prohibitively expensive. A framework that can be used to complement and improve their existing way of working is likely to be of considerable value and easier to develop and integrate into current working practices. The framework will extend existing ways of working to gain compliance with the new regulations.

1.3 Research Aims, Questions and Objectives.

1.3.1 Aim

It is the aim of this thesis to look at Pbd models, that are available for organisations to use, to see if they are able to gain consent or informed consent from data subjects. It also aims to suggest improvements and to set out the foundations of an "Informed Consent by Design" (ICBDF) framework. The aim of the ICBDF is to ensure that business's systems have a greater chance of being compliant without excluding customers.

If the models can only gain consent, what extensions can be added to them that would enable them to gain informed consent?

1.3.2 Research Questions

i) Do Pbd frameworks and their concepts help design computer systems to store and process personal data that are compliant with the informed consent requirements of DPA legislation?

ii) If existing Pbd frameworks are not fully compliant, can they be extended to set out the foundations of an "Informed Consent by Design Framework" using metamodeling that is appropriate for computer systems?

   a. This should include a method to gain understanding of the data subject, but also help the organisation monitor its compliance.

1.4 Motivations:

i) Consent vs Informed consent is a critical part of being able to be compliant with the legal requirements. This is discussed further in section 2.4
ii) What are the consequences of failure to comply with the requirements of the DPA/GDPR? We have considered this in sections 1.1 and 1.2.

1.5 Research Methodology

The methodology chosen is one based on Design Science Research (DSR) for information systems. DSR is a method of research aimed at developing an artifact to enable the improvement of the artifact's functionality. "DSR allows for the creation of a conceptual model for how researchers can carry out Design Science Research … to recognise and evaluate it"(Peffers *et al.*, 2006). It is also a methodology that "…aims to solve known problems or design something that does not yet exist"(Goecks *et al.*, 2021, p. 2)

Steps of the DSR are:

1) Problem identification and motivation
2) Objectives of a solution
3) Design and Development
4) Demonstration.
5) Evaluation
6) Communication

The thesis is limited in its ability to fully develop and demonstrate an informed consent framework. That said we will design a framework and demonstrate how it is envisioned to work with a worked example that highlights what it is able to do that other framework don't.

It is recognised that for an informed consent framework to reach its full potential, research from other disciplines will need to be drawn upon. The DSR is not likely to be helpful in these arears. Research frameworks such as the Functional-Cognitive framework, which offers a conceptual basis for greater co-operation between behavioural and cognitive psychology research, would be more appropriate for research in Psychology. (Barnes-Holmes and Hussey, 2016) Due to its focus on psychology it is not going to be helpful in a thesis focussing in Computer Science.

Research frameworks such as the one put forward by Anton N Isaacs in "An overview of qualitative research methodology for public health researchers" has an approach that requires data collected from people who use a health care provision. This information would typically be sensitive medical information (Isaacs, 2014). If interviews were going to be done for this thesis, the information we are asking for would not be sensitive personal information, so the use of this research methodology would have limited applicability.

A drawback of using the DSR research method is that it is one that does not take in external inputs (e.g. interviews) to improve the artifact being created. Thus would be a significant drawback if it was being used for a PhD thesis, which requires a higher level of review of the created article. However I believe that it is a good fit for an MPhil thesis.

1.6 Thesis Outline.

The first research question (section 1.3.2) will be addressed in steps 1 and 2 of the DSR, while the second research question will be addressed in steps 3,4 and 5 of the DSR.

1.6.1 Step 1: Problem identification and motivation.

This chapter (chapter 1 Introduction), as well as chapter 2 "Literature review", will identify the problem, as well as the motivation for this research. Chapter 1 has laid out why organisations may need or want to look at their current systems that deal with processing and storing personal data, and how informed consent is gained. We have already seen in this chapter how the penalties the DPA introduces are at a level that can make a significant dent in the finances of even the largest companies. We noticed that, how the reporting of how companies are using personal data has made prime time news programmes and newspaper front pages. So, organisations not only face high fines, but also reputational damage from the association with failing to protect personal data.

Chapter 2 will look into the differences between how consent is currently gained, and how consent *needs* to be gained under the current legal framework. It will also look into the

current Pbd models and look at how they implement the gaining of consent. Are they able to help gain informed consent from data subjects?

1.6.2 Step 2: Objectives of the solution.

Chapter 2 will also be highlighting the issues found when reviewing current Pbd models. It will help define the requirements of the ICBDF. We will also look into if the current models do not appear to take into account the needs of the data subjects, and they do not offer an explanation to the data subjects of what they are consenting to in a way that is accessible to them.

The focus of this thesis is to look at ***what*** the data subject is being asked, rather than ***how*** it is being asked. The consent request that the data subject is given needs to state what personal information is being collected, and why. Who is going to have access to that personal information, what they are going to use that personal information for, and why they have access to the personal information?
It is outside of the scope of this thesis to look in detail at how the consent request is presented to the data subject, as it is believed that this is an area that is best researched by other disciplines. That said, any requirements that come out of research into this area needs to be included in the requirements of a computer system gaining a data subjects informed consent. In Chapters 3 and 4 we do consider how consent requests are understood by the data subject as that is relevant in considering what the request asks of them.

1.6.3 Step 3: Design and Development

In Chapter 3 we will look into what a solution will need to contain to try and improve on the current state of play, and to design and develop a possible solution. The solution will also be targeted to an appropriate audience. The audience that is expected to use this solution would include developers, project managers, and Data Protection Officers.

The introduction of a consent request explanation is an example of how the framework could be made to reflect the data subject's needs.

1.6.4 Step 4: Demonstration

Chapter four will look at demonstrating how the possible solution would work in a case study. By adding an "consent request explanation" into the ICBDF, written in a way that is targeting the needs of the data subject, it is thought that this will assist the data subject in understanding what is being asked of them so that they will be able to give informed consent.

In this chapter we aim to demonstrate via a case study how the ICBDF can take into account the requirements of the data subject, as well as the requirements of the service, to form ***what*** the data subject is being asked. This may also have an effect on ***how*** the data subject is asked.

1.6.5 Step 5: Evaluation

Chapter five will look at how the possible solution could be evaluated against a current model with a case study or comparison.

The ICBDF will be compared against another Pbd framework (Orange Consent Management System) to show how the ICBDF helps to gain informed consent from the data subjects, where this is lacking in the Orange Consent Management System. Comparisons will include areas such as: the use of explanations for the data subject; what methods are used to gain informed consent; auditability of the records.

1.6.6 Step 6: Communication

Given that this thesis on submission will be added to the University of Brighton's repository PURE, it will be able to be found by researchers so that it can be built on. Thus this thesis is the main avenue for communication for this work.

1.6.7 Intended audience of the new framework

It is envisaged that the framework would be used by several types of users within a business. This would include users responsible for Information/Cyber Security, Privacy/Data Protection, business analysts, system development, and Project Managers.

The framework will be able to be used by the project manager to help describe the system to multiple different departments (e.g., software engineers, data controllers etc.) within the organisation in a way that gives them a better understanding as to how the system works. It is envisaged that the framework will also be able to aid in the defining and gathering of the requirements of the framework to be able to build the system.

Aside from the project manager, when implementing a new system, it is envisioned that an organisations' Data Protection Officer would use the framework to aid in ensuring that the current systems used to provide services are in line with the requirements of Data Protection Laws.

1.7 Chapter Summary

In this chapter we have shown that the current legal landscape regarding data protection is considerably more stringent than previously. Organisations need to be able to demonstrate that they have gained informed consent from data subjects with regards to the storing and processing of personal data.

Chapter 2 will look into current Pbd models to identify if they are able to assist organisations in gaining informed consent, and if not, then identify the requirements that are needed to be able to gain informed consent.

Chapter 3 will look into what a solution will need to contain to try and improve on the current state of play, and design and develop a possible solution. For example, can the solution provide a way to gain informed consent.

Chapter 4 will look to demonstrate how the possible solution would work using a case study. In addition, we will evaluate the possible solution against a current model using a case study or comparison.

Chapter 5 will summarise the findings of this research and highlight areas of future work, as well as the limitations of the solution detailed in this research.

It is recognised that while this thesis is focused on computer science, for the work to be able to achieve its full potential it will need the input from a number of other disciplines, such as psychology, education, IT, ethics, and law.

2 Literature Review

2.1 Background

Organisations can be fined significant amounts by the Information Commissioner's Office (ICO). There is increased public and press interest in privacy and personal data. Organisations therefore are now under much more pressure than before to ensure that privacy is built into their systems. It is no longer good enough to have privacy and security bolted onto an existing data processing system. Systems now need to be designed with privacy, security and consent in mind from the start. The approach is known as "privacy-by-design" has started to emerge as a useful tool (Wuyts, Scandariato and Joosen, 2014). This approach places privacy within the life cycle of the development of a system, often at the "requirements gathering" phase, to ensure that privacy requirements needed for a system are included from the beginning of the systems' lifecycle.

In order to build security, privacy and consent management into systems, a model that lays out the legal and system requirements is needed. Additionally, the model will need to present these requirements in language that software engineers can understand (Zarrabi *et al.*, 2012). This is so that the system can accurately reflect the requirements.

Making sure the developers have a set of requirements they understand is of importance. This is because developers do not typically have the experience to interpret legal documentation (Islam, Mouratidis and Jürjens, 2011). Legal texts are not always clear about what is required, or provide examples for specific situations that may arise within a systems lifecycle. The way that legal texts are phrased is so that they are helpful for lawmakers and the court system. However, the legal language used is not helpful to a system developer who typically would find technical writing more helpful to understand what is required. Also, with GDPR in particular, but Information Security in general, the legislation is still recent and not always fully understood (Islam, Mouratidis and Jürjens, 2011). This may be exacerbated as legislators are not used to the rapid change in technology and are trying to make legislation relevant to a fast-changing landscape.
In light of this, having a framework that can help develop requirements that help software engineers understand the legal requirements of a system, then the system is likely to be

compliant with the law. The framework should have an element where the legal requirements are set out in the same kind of language as all other system requirements, and the legal requirements are considered alongside other requirements as the system is being designed

For the constraints of this work, I will be considering consent management systems (CMS) to be included within the term Privacy by Design model. This is because both attempt to build privacy (and consent) into a system at the beginning of the "systems lifecycle".

2.2 Methodology

The methodology that is to be used is based on the one presented in "Understanding Frameworks: A commentary to assist us in Moving Our Field forward by analysing our past" by Schwarz et al. (Schwarz *et al.*, 2007).

The first step that was taken was the selection of articles that were going to be reviewed. To do this, I identified the following repositories that had the types of articles that I needed for the literature review. The journal repositories identified are: IEEE; Westlaw; Wiley online library; the University of Brighton library's One Search and Scopus. Specific journals in which articles were found include: Proceedings - International Conference on Research Challenges in Information Science; Software and Systems Modelling; Computer Law and Security Review; Communications of the Association for Information Systems; Journal of Internet Law; IEEE Pervasive Computing; Journal of Universal Computer Science; European Journal of Operational Research; Proceedings of the IEEE International Conference on Requirements Engineering; Technology Science and Frontiers in Artificial Intelligence and Applications. These were chosen as they publish papers that are related to computer science topics.

While within the medical field, there appears to be significant work done regarding consent and informed consent, other fields have started to look into what informed consent is since the introduction of GDPR so that they can be legally compliant. We will use Google Scholar as a method of confirming that relevant articles have been found as it can search an

extensive range of subject areas and is not limited to articles in journals by a single publisher.

The two main subjects looked for: -

- Systems that can record when a data subject has given their consent and can assist in managing data subjects' information. Consent Management Systems (CMS), Privacy (by design and default), and how they can be modelled. This will be with a slant towards compliance with GDPR.
- The second is understanding how informed consent can reliably be given by the data subjects. I will identify what consent is.

These areas have been chosen so that the current consent management frameworks can be compared. Having an understanding of what consent *is* will enable us to look into how current frameworks cater to differences in data subjects understanding to give informed consent.
The time range that has been chosen to look at when searching the journals is 2010 and later for the first area, and from 1990 for the second area. These time frames have been chosen so that for the first area that they are compliant with the requirements of the GDPR. For the second area, a broader understanding of what consent is and then a definition of consent for this thesis can be formed.

The following search terms that have been used are: GDPR; consent management systems; consent; informed consent; explicit consent; privacy; Privacy by Design; Privacy by Default; modelling and conceptual methods; methodologies for security; methodologies for privacy. Areas such as privacy by design have be looked into as they may be able to assist in defining how a framework for consent by design can be created. The area of Pbd and Pbdf has been of research interest for some time, so the initial timeframe started at 2010 to the present to get an initial understanding of the research that has been done in this area.

The time frames above are a general guideline, should there be relevant and useful articles found outside of them they will be included, with a note if they were published prior to the final version of GDPR.
When reviewing the literature found for Consent Management Systems, we will filter to ensure that they are fully relevant for the literature review. Articles regarding Consent Management Systems will be checked to ensure that they describe the system in enough detail that they can be compared with other systems. Also, they will need to have enough

detail to be able to confirm how, or if, they conform to the requirements set down in the GDPR. Around 250 articles were found and considered through this process. Of this around 90 were used.

Once the articles have been filtered, they will then be compared to each other against the research questions outlined in 1.1.2 Research Questions. This should also highlight aspects that the existing models do not capture.

The articles concerning consent have been reviewed in a similar way to the above. However, this section will have more of a narrative tone. We will investigate what informed consent is with respect for GDPR and Privacy. From this, bringing in what the regulations require, we have then formulated a definition of what consent is for the purpose of this literature review

2.3 Methodology justification

The choice of using the methodology set out in "Understanding Frameworks: A Commentary To Assist Us In Moving Our Field Forward By Analysing Our Past" by Schwarz et al. (Schwarz *et al.*, 2007) was made because of its academic standing in reviewing literature that proposes frameworks, and because it gives a repeatable and structured method for doing this.
Other methodologies have been looked at, including Patterns of business intelligence systems use in organisations by Arnott et al. (Arnott, Lizama and Song, 2017); Schryen (Schryen, 2015) vom Brocke et al. (vom Brocke *et al.*, 2015) and Jetu et al. (Jetu and Riedl, 2012). It is worth noting that these methodologies have similarities to the chosen methodology, in their repeatability and structured methodology.

2.4 Consent

Consent as a concept is one that has changed over time, such as after the Nuremburg trials at the end of World War 2 (Hammer, 2016). The kind of consent needed can be different depending on the nature of the situation. For example requiring informed consent before a

medical procedure may be appropriate, but requiring informed consent for purchasing a train ticket may be overkill (O'Neil, 2003).

The concept of informed consent can be traced back to the 16th century, [Selek 2010 cited in (Hammer, 2016)] and its use has particularly been used in the medical field, such as medical research and medical treatment. The first recorded use of the term "informed consent" was used by a Paul G. Gebhard in a medical malpractice case in 1957 (Pace, 1997).

The DPA definition of consent "… means a freely given, specific, informed and unambiguous indication…" (HMSO, 2018) that the data subject approves of the processing of their personal data for the purpose that it has been requested. For a data subject to be able to give their consent to an organisation, they must be able to understand what it is that is being asked of them. The ICO has given guidance on the rules around consent requests, and has gone on to say that the way the explanation is given needs to be ***easily understood*** (ICO, 2020c). In addition if a request is "… vague, sweeping, or difficult to understand, then it will be invalid" (ICO, 2020c).

In the creation of a system, the organisation needs to be clear ***what*** it is that they are needing to ask the data subject, rather than ***how*** the data subject is going to interpret the question. If there is a lack of clarity in what is actually being asked for, and that it is not understood by the data subject, then the system will not collect the necessary permissions. It is relevant therefore to consider how can an organisation be sure that all data subjects they asked for consent to understand the explanation that is provide.

There are several factors that may affect a data subject's understanding of an explanation. Information overload is a factor. This may be a factor that is difficult to overcome as how is an organisation to know how much information is too much for any given data subject? It has been found that organisations' explanations are becoming more complex, and also the amount of information given is increasing (Shore and Steinman, 2015). It has also been found that the more information that is given to a data subject, the more likely it is for them not to be able to process and fully understand it (Shore and Steinman, 2015). It has been argued that in some cases, particularly medical procedures, that overburdening a data subject with all the risks involved may not lead to the best outcome for them (Shore and Steinman, 2015).

The second issue that hinders a data subjects' ability to give informed consent is the complexity of the information that data subjects are presented. A data subject is likely not an expert in the field, but they are often presented information in a way that expects the reader to be proficient in the area.

The third issue might be the state of mind of the data subject. For example if they are about to undergo a medical procedure the data subject might be scared (Hammer, 2016), and not able to process the information given. Or a data subject wants to check a news story on a web site might just click "Accept" on the Cookie consent notice without even reading what they agree to.

The above issues can perhaps have their roots in a *data subjects understanding*, and their *engagement* (or interest) in the explanation that they are being presented.

It is difficult to ensure a data subject understands the explanation presented to them. One difficulty in this is what is termed as the "explanatory gap" (Loughlin *et al.*, 2013), which is the apparent gap between the understanding of a subject, and the way something has been explained. An example given by an organisation may be well written, but that does not mean that a subject is automatically going to be able to understand it. Although if an explanation is able to harness a context that a data subject knows or has experienced, then this is likely to be helpful in their understanding of the explanation (White and Gunstone, 2014).

For the purpose of this thesis the definition of *understanding* that is going to be used is: "How an individual can make meaning of facts, and being able to transfer them to other areas" (Wiggins and McTighe, 2005).

So, to summarise: A data subject needs to consent to the explanation given to them by the data controller on why, what and how, personal data is needed to be stored and processed. The consent also needs to be given freely, and with the data subject being able to decide if they want to give consent without pressure from the organisation requesting the informed consent (Robol *et al.*, 2018).

To be able to consent to the explanation, the data subject needs to be able to understand it. To allow a data subject to understand the explanation, the data controller needs to give the explanation in an appropriate and understandable way. This is key to the thesis. The quality of the explanation given to the data subject needs to be in a method that the data subject can give informed consent to.

Although in this thesis we are not concerned with the *how* of gaining consent, it is relevant for the person framing the explanations to consider if they want *what* they are asking to be clear. The use of guidance from the Plain English Campaign to aid in the creating of clear and jargon-free explanations may be helpful. Along with this, there is the "readability" aspect of the explanation. Readability takes in a number of layout factors, such as how the text is laid out on the page (text size, colour, font etc.), and also the density of the text on the page (Cronin, 2009). Readability takes into account the use of vocabulary and grammar. Research has shown that several rules help with the written word; these include:

- Use short, simple, familiar words
- Use correct grammar, punctuation, and spelling.
- Use simple graphic elements such as bulleted lists…." (DuBay, 2004).

It has been found that if texts are too complex for the reader, then the reader is likely to stop reading (DuBay, 2004), so there needs to be care taken to ensure the level of complexity of an explanation is of an appropriate level.

For this thesis, we have chosen the definition of consent to be the following:
Consent: is a permission given by a data subject to a data processor/controller to process personal information to provide a service. For the permission to be given, the data processor/controller needs to inform the data subject what personal information they require and how they are going to process it. The permission is only for the processing that is required for the specific service and must be given freely.
Although we have touched on *how* the consent request is presented to the data subject, that is not the focus, but assists us in considering the requirements of a computer system.
The focus of this research is to look at what the data subject is being asked for rather than how it is being asked. This means that the consent request that the data subject is given needs to state what personal information is being collected, and why. Who is going to have access to that personal information? Why they have access to the personal information?

2.5 Consent Management Systems in Literature

In this section we will look at a selection of currently available systems that can be used to manage consent. These were chosen for their focus on gaining consent from data subjects, and how this could be implemented in a computer system. These systems are similar to the

Pbd frameworks considered later in this work, but the focus of the CMSs is how consent is managed, rather than looking at a system in which consent management is a part of.

The system that is described within MAGIC: Once Upon A Time In Consent Management (Bialke *et al.*, 2018) was designed to replace a thesis -based system with a more robust computer-based and GDPR compliant CMS.

The first step in the proposed system was the use of a generic informed consent service (gICS) that could automatically produce printed consent documents for the user to sign. Once signed, the module needs to be able to import it into the digital system. This is illustrated in figure 1

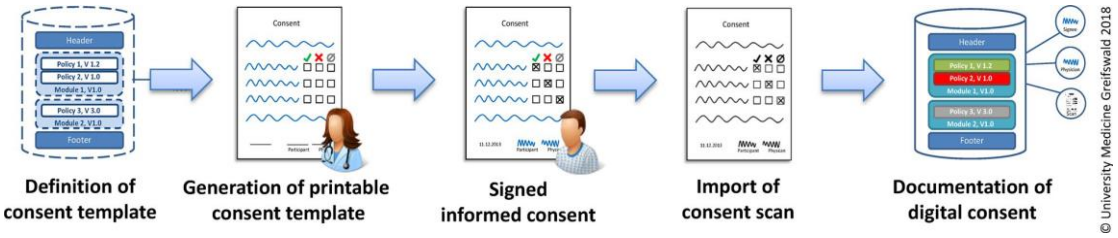


Figure 1: A structured exchange format for informed consent templates fosters the convergence of paper-based and digital informed consent management with generic informed consent service (gICS) (Bialke *et al.*, 2018).

The gICS is described fully in "May I? Challenges to a generic, automated electronic administration of consent" by L. Geidel et al. (Geidel, Bahls and Hoffmann, 2014)[5]. This is a very useful system, as it enables the easy management of the consent templates when they need to be updated.

As the consent templates are printed out when required, the need to recall batches of pre-printed forms is removed. It also requires little to no change in the working practices of the staff who are gaining the consent of a user. As the printed and signed form is then digitised, the user's consent is more easily managed on the digital system than it is on a paper-based system. It should be mentioned that this gICS was developed prior to the

[5] The paper was originally in German, Google translate was used to translate into English.

finalisation of the GDPR. That said, however, it was intentionally developed to be modular and be able to be updated as requirements (regulatory and business) change with time.

The Magic system then able to take the consent form (either electronically or paper-based) depending on the modules that have been assigned to the consent form template. Depending on if consent has been given or declined, the appropriate policies can be applied. The Magic system collates the requirements for the system from published legal requirements along with the requirements of current systems, so that it is able to produce a system that is able to automate the consent management within an organisation. This includes technical standards use in the organisations it is being designed for, so that it could be inter operable with existing systems.

There is, however, a drawback to this proposed CMS. While the use of the gICS does help in the modelling of creating an automatic system to create consent forms, as it ensures that the consent templates collect the legal and system requirements, it does not however take into account any requirements that the data subject may have, e.g., large font. Thus it does not collect *all* of the requirements for the consent forms. While the authors of the document state that it is a "work in progress" (Bialke *et al.*, 2018) it is still worth considering even if the implemented system has been modified.

In "Blockchain For Consent Management In The eHealth Environment: A Nugget For Privacy and Security Challenges" (Genestier, 2017) it is proposed that for current content management systems, consent is an all or nothing choice. The end-user is unable to control who is able to make use of their data. They also propose that each application has its own pool of data that is not shared between applications.

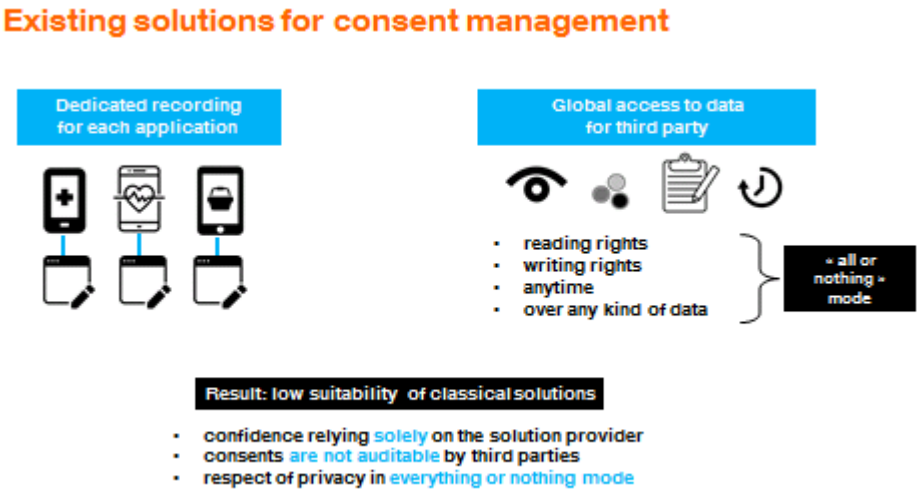


Figure 2: Existing Solutions for Consent Management (Genestier, 2017).

They go on to propose what they call the “Orange Consent Management Service". This solution uses block-chain technology, and as such, it is able to share consent management across a number of applications.

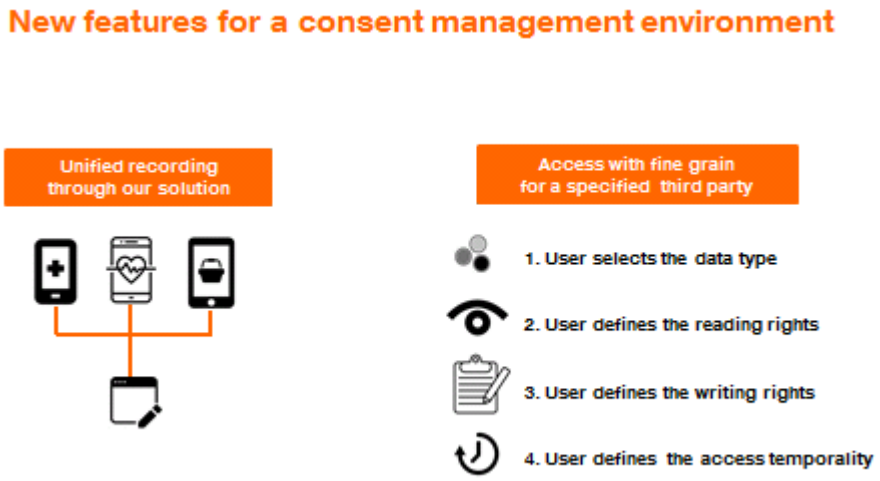


Figure 3: New features for a Consent Management Enviroment (Genestier, 2017).

This solution can help improve trust, as the consent is distributed across several systems, and there is no one single point of failure. In addition, as the solution is using block-chain technology and the ledgers are duplicated, it becomes very difficult (if not impossible) to falsify the records. Trust is further increased as it is possible to audit the ledgers by third parties.

For the Orange Consent Management service, the authors chose Hyperledger as the block-chain. This is because Hyperledger is a private block-chain which limits access to the block-chain system to authorised users. This is different from public block-chains such as Bitcoin that anyone can join.

The system has four main steps in its working. Firstly, it records the consent given by the data owner (user) and this is recorded in the Block-chain via the consent management server. Then in the second step, the user’s data is recorded,

and stored on the data server. Thirdly, third parties access the data that the user has granted them authorisation to access. This is done by the data management server checking with the consent management server. The consent management server also updates the block-

chain. Finally, third parties are able to review the block-chain to audit the organisations compliance. Figure 4 shows this.

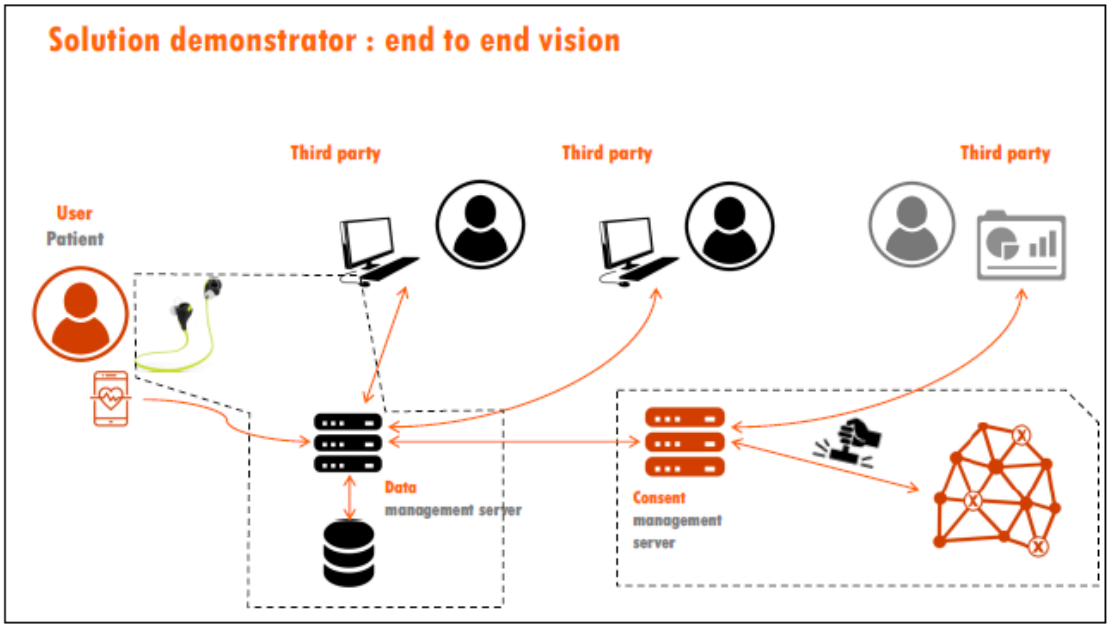


Figure 4: Solution Demonstrator: End to End Vision (Genestier, 2017).

There are some drawbacks of the Orange Consent Management Service as described. Firstly, at the time of the publication of the literature, the Hyperledger block-chain system was in Beta. Second, it is also not known if the service as described can be scaled up and thus able to support a large organisations CMS'. Thirdly, the authors also raise the challenge of whether enough organisations can agree to be a part of a consortium that would allow the benefits of the Hyperledger block-chain system.

Blockchain for Student Data Privacy and Consent uses the Hyperledger system that was used in the Orange Consent Management Service. The Hyperledger, is a Blockchain implementation that is an open-source blockchain technology to aid them in creating a consent management system for the education environment. This could lead to advantages such as limiting the ongoing costs of using the system (i.e., no re-occurring licencing fees) and that it can be fully customisable for the needs of the users (as it is open source). However, there are some disadvantages, such as needing the in-house expertise to be able to maintain the blockchain system, and that as because Hyperledger is not backed by a large company (e.g., IBM or Microsoft) educational institutions may be nervous in adopting it.

It appears that the Orange Consent Management Service has lately implemented Hyperledger V1 and is working with several projects to implement demonstrator implementations with several organisations. (Orange, 2022)

In this system rather than looking for the consent of the data subjects (who are children), they are looking for consent from their parents. For the purposes of GDPR it would need to be able to gain the consent of both the children *and* their parents.

In their system, they have entities of a Data Manager (DM) who maintains the database of personal data, a Data User (DU) who is an entity that needs consent to use the data (in this case, a school). They also have an Authorised Agent (AA) who administrates the creation of other AA's or DU's who need to get the consent of an Associated Entity (AE). The AEs are the owners of the data, in the case of this system they are the child's parents.

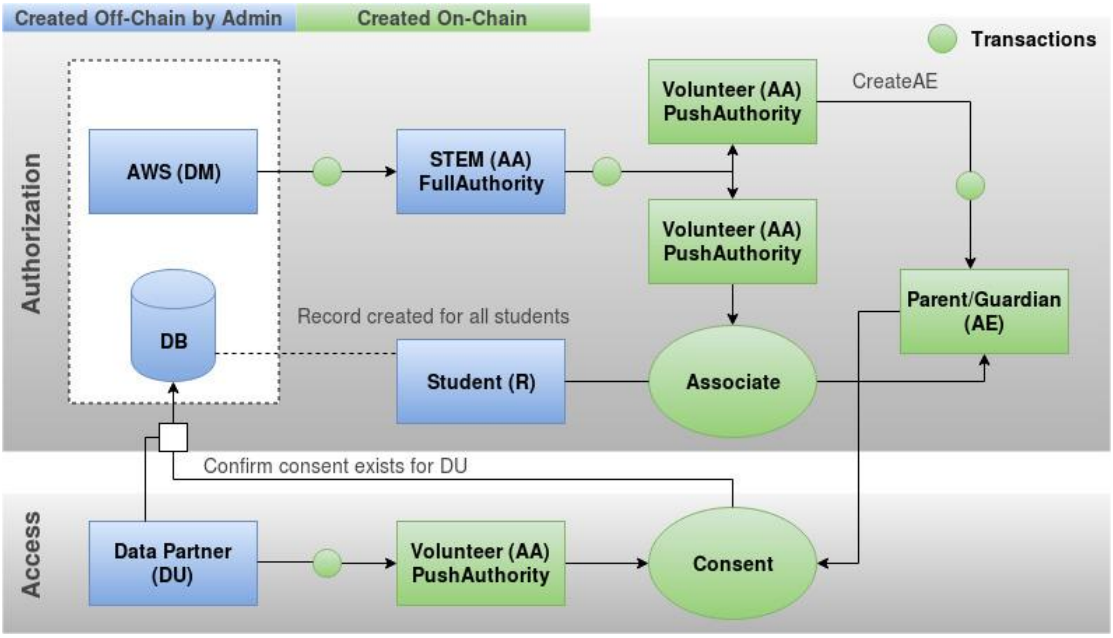


Figure 5: A visualisation of the STEM India data Authorization and Access System (Gilda and Mehrotra, 2018).

Figure 5 shows how the DM has the authority to associate parents with their child's record and the child's record can move between the educational institution's workers, and how educational institutes are able to manage who in their organisation has access to the records. It also shows how a DU can request consent from the parents using this system. The system also has a permissions structure built-in, and limited access is enforced by a permissions file within the Hyperledger Composer part of the Hyperledger ecosystem. Access to the resources can be limited depending on the role that an entity has.
There are three functional algorithms used in the system to ensure the privacy and security

of the data stored. Each function adds to the system update to guarantee that all updates, changes or other work has been completed.

The three functional algorithms are:

- General Authorisation: this is to ensure that the current user has the credentials to be able to initiate this function, and also has the same authorisation root as the transaction. This is to prevent the initiator from giving authorisation to another user that they do not already have. So, an AA from one educational institution cannot give access to their data to an AA from a different educational institution.
- Associations: This process confirms that the person starting a transaction has the correct associations to the data e.g., the parent is associated with the student record. This also confirms that the associations are not out of date. e.g., when a student has moved to a different educational institution.
- Consent: This function uses the previous two functions to ensure that consent has been gained from the correct parent and is stored by the correct educational institution.

The authors of this paper did highlight three main areas when they evaluated the security of the system. The first being “nosy parents", or parents who want to compare their child with other students in their class. They got around this by only giving parents “read” access to the records of their child only. The second being “nosy volunteers" or staff/volunteers who have the privileges to be able to create accounts and use this to give themselves accounts that can see student records that they should not see. The authors think that this is a moderate risk, but by limiting the time that a volunteer has access to the system could minimise this risk. (E.g., a volunteer can only access the system in working hours and for no more than 20 minutes per log in). The third are “Hacktavists” or people who are outside the system who would gain access to the system by subversive means. The authors have mitigated this risk by having a single trusted database admin (the Data Manager). There are some areas where this system could improve however. The first is that with GDPR in the UK, children of 13 and up are considered to be able to give consent for themselves (ICO, 2018). In addition the child has the right (like adults) to request the data to be updated and to remove consent (ICO, 2018). This proposed system also does not appear to have a mechanism to be able to ensure that the explanation for consent is understandable. Like

the Orange Consent Management System, questions around how scalable the system is are present in this system as well. There appears to be a single point of failure in this system as well, if the database that the DM is in charge of is not available for any reason this would cause issues for the use of the whole system.

Compliance through informed consent: Semantic-Based Consent Permission and Data Management Model (Fatema *et al.*, 2017) puts forward a consent and data management model for recording and management of consent. In this model, there are several parts that have separate but related tasks. The Consent Manager (CM) keeps the current consent (and by extension, the permissions) that are relevant for the current processing of the data. The Context Handler (CH) is responsible for managing the current context and detecting changes to the context and alerting the CM and Data Manager (DM). The Data Manager is responsible for managing and protecting the data, including enforcing permissions to the data. The final part is the Provenance Manager (PM). This provides a log of all activities that have affected the data; it also tracks the consent and data through its life in the system. It is able to provide an audit trail so that in the event of a data breach or an audit, it is possible to find out when an event occurred.

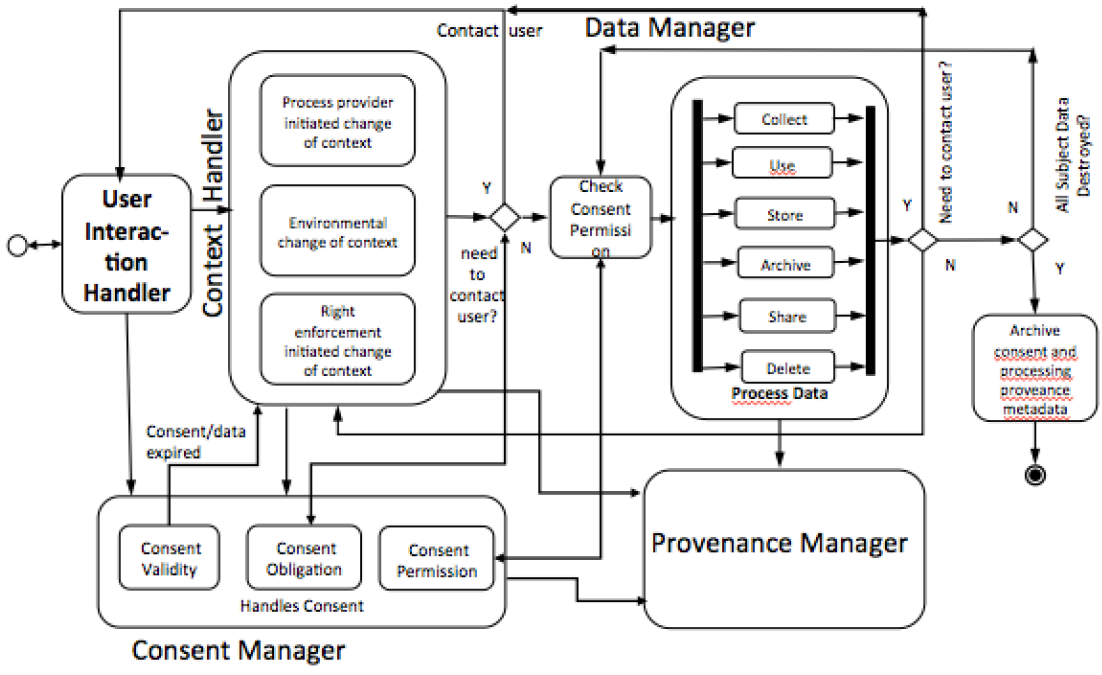


Figure 6: Consent and data Management Model (Fatema *et al.*, 2017).

The flow of interaction within the model is as follows:

- The User Interaction Handler gains consent the first time a user registers or logs in to the system. This is then passed for validation by the CM, which logs this and passes providence related data to the PM.
- The CH generates the context of a new sign up, and informs the DM.
- The DM ensures that the appropriate permissions are assigned to the data, regarding the intended use of the data, as specified by the consent that has been given.
- The CH records changes in context and consent and passes this to the CM and DM. The CM identifies the change, and updates itself and the PM. The DM halts processing of the data and checks the new consent before processing it further.
- When consent is revoked, this is detected by the CH and passed to the CM and the DM. The CM records the revocation of consent. The DM stops processing of the data, and adjusts accordingly, which may include the deletion of the data stored.
- The PM records in a log, all changes involved the data and the consent. This includes how consent was gained, and how the data was stored including if the data was shared and how and where it was stored.

The authors of this paper do note that (at the time of writing their paper) they are working on using this model in real-life situations. So, this model has yet to be tested so it may see changes in the future once it has been used within an organisation. In addition, while it puts forward a model for managing and auditing consent, it does not cover how to ensure that the end-users' consent has been given with their full understanding of what is being asked of them.

2.6 Privacy By Design

Privacy by Design (Pbd) is an approach that when creating a new system, the Privacy of sensitive information is considered from the very beginning of scoping the requirements for the system (ICO, 2019a).

The concept of Pbd is not a new one; it was coined in the 1990s (Morales-Trujillo *et al.*, 2018). However, with the introduction of GDPR in the EU, it has now become a legal requirement (European Parliament, 2016).

Pbd research has been carried out in several areas. This includes Internet of Things (IoT), (Perera *et al.*, 2020); Big data (Cavoukian and Jonas, 2012); Smart Healthcare (O'Connor *et al.*, 2017); Smart Homes (Perera *et al.*, 2016); as well as in the area of the European Union's (EU) General data protection Regulations (GDPR) (Morales-Trujillo *et al.*, 2018).

A. Cavounkian also mentions other areas that work has been done in regards to Pbd include: Surveillance; Biometrics, Smart Meters; Mobile devices; Near Field Communication (Cavoukian, 2012). She goes further to lay out 7 foundational privacy by design principles:

1. Proactive, not Reactive; Preventative not

   Remedial;

2. Privacy as the Default Setting;

3. Privacy Embedded into Design;

4. Full functionality – positive sum, not zero sum;

5. End to end Security – Full lifecycle protection;

6. Visibility and Transparency – Keep it open;

7. Respect for user privacy – Keep it user-centric. (Cavoukian, 2009).

It has been suggested that some of these principles are easier for a software developer to use in the design of a system. Principle 2 could easily be defined such as where there is an option for a user to choose their privacy settings; the default should be that their privacy is retained. Principle 3 is essentially telling us that privacy should be included in every step of the design of a system (Schartum, 2016). However, the other principles are useful as they give us what the final system needs to include, but they do not give an idea as to how they are going to be achieved.

Having a framework containing clear guidelines about how privacy can be implemented to aid developers in creating applications that contain improved privacy (Perera *et al.*, 2020). This would lend support to the idea that having a framework for privacy will improve the privacy of a system. It may also support the idea that embedding appropriate privacy education/advice throughout an organisation would aid in improving how privacy can be managed within an organisations system.

While a focus has been placed on how to implement Pbd within the area of system development, a significant problem has the possibility to undermine an organisation's attempt to implement Pbd. This is getting an organisation's management involved in a meaningful way in the creation and implementation of a privacy policy. The need for management to be fully engaged is important, as personal data can be vital for the organisation's bottom line (Spiekermann, 2012). This could be from being limited in strategic opportunities, but also from media backlash and legal cases.

As mentioned above, when talking about foundational Privacy by Design principles, privacy is a concept that is difficult to define. And as such, it may lead to difficulties in understanding for developers and managers, as to what it is they need to protect along with the risks and benefits of protecting it (Spiekermann, 2012). Having a framework that allows an organisation to identify what personal data they have, and how to identify the risks to the personal data could be very helpful to influence an organisations' privacy policy and Pbd framework. An example of a framework that could assist with this is the privacy and data protection Impact Assessment Framework for RFID Applications (European Commission, 2011). This is something that could be used in conjunction with the ICBDF to help organisations implement appropriate security measures.

2.6.1 Pbd frameworks: How do they manage consent?

In this section, we are going to investigate how Pbd frameworks manage the collection of consent from data subjects. In the frameworks that collect consent, do they provide a framework compliant with the informed consent requirements of the DPA legislation?

The methodology for finding literature can be found in section 2.3.

I filtered the results of my search for duplicates. For this, I would discard a summary paper if I already had the full version of the paper.

For this investigation, I am only looking at Pbd frameworks that have a consent recording function in them. The reasoning for this is I am looking at how consent is managed in them, so they need to have a consent function in them.

I looked to answer the research questions:

i) How they implement the gaining of consent, and if current models are able to help gain informed consent from data subjects.

ii) If they do not help gain informed consent, what requirements would be needed to be implemented in a framework that does help gain informed consent?

The DEFeND project has been developed a Pbd framework build around the requirements of the GDPR, and as such, has included functions to record the consent of data subjects. In the DEFeND Architecture: a Privacy By Design Platform for GDPR Compliance, they acknowledge that "…obtaining user consent is difficult" (Piras et al., 2019).

It also has functions to ensure that the information held is just what is required, as well as being able to offer differing levels of data security based on the sensitivity of the personal data that is being held. The framework goes a long way to covering the foundations laid out by A. Cavounkian's work (Cavoukian, 2009).

However, it is not clear in the referenced document as to how it goes about gaining the informed consent of data subjects, or data subject guardians. While the actual methods that the DEFeND project use to gain informed consent are confidential to the project, the DEFeND project has advised that these methods are based on current tools and advice from the French data protection agency CNIL.

The paper: Modelling[6] and Reasoning about privacy-consent requirements (Robol et al., 2018), looks into a model that is being used within the Trentino Health-care provider. Like the DEFeND project, it looks into how consent can be gained, and how the personal data is used within the organisation.

[6] This is the spelling that is used in the title of the paper.

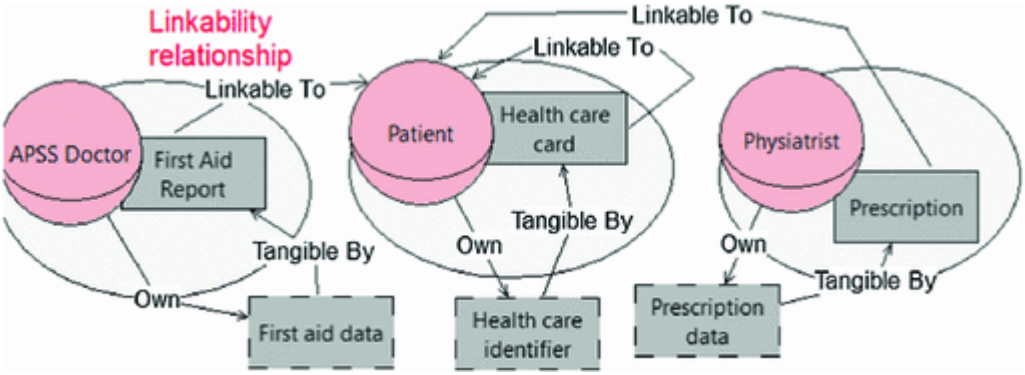


Figure 7: APSS information view modified (Robol et al., 2018). [7]

In Figure 7 we can see in an informational view, how the patient's information can be linkable to them via the first aid report that is passed to the Doctor, or prescription that the psychiatrist has access to.

In the model, the patient is asked for consent by the First Aider to be able to pass on the personal data to the professionals (Doctor, Pharmacist, etc.) that need to see it to be able to provide care.

This model is one that has been developed and tested in a "live" system, and in its evaluation, it was reported that participants were positive regarding the model. Although of the groups that were mentioned within the document that participated, the data subjects (in this case, the patients) were not mentioned.

An additional concern regarding the model is that in the paper there is no mention regarding the understandability of the explanations given to the patients, particularly as when they are asked for consent, they are being given first aid. Depending on the situation, the person giving the first aid may not know what personal data is going to be needed, or who is going to need to have access to it. In addition, the person receiving first aid may not be in a condition to be able to give consent, let alone understand what is being asked of them.

The paper, An Agent-Based Framework for informed consent in the Internet of Things (Neisse et al., 2015) puts forward an interesting consent framework. In this framework, it uses the model-based Security Toolkit (SecKit) to apply rules around

[7] This is the spelling that is used in the paper.

events that occur on an IoT network. The system uses an Event-Condition-Action (ECA) ruleset in which should an Event occur (e.g., connecting to a new network), it applies a Condition. This Condition could be things such as time of day or location where the Event is happening. The Action part is what enforcement action should take place, e.g., Allow, or Deny. The enforcement action is based on the policies that the data subject has selected in a secure gateway. The secure gateway is a user-centric system that allows them to choose the policies that they want to apply to their personal data.

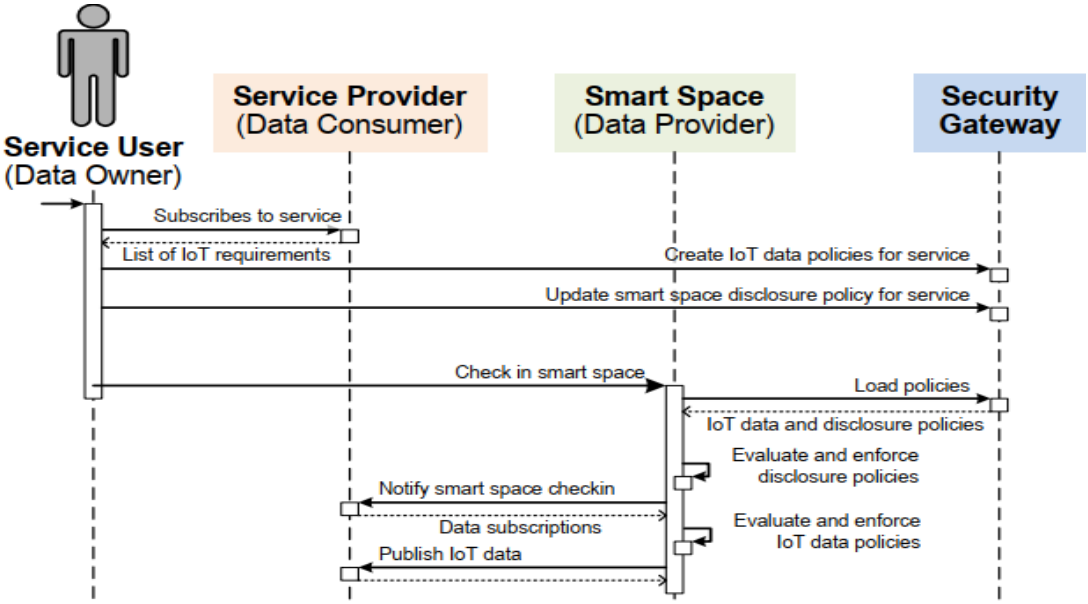


Figure 8 Sequence diagram showing the interaction between domains (Neisse et al., 2015).

In Figure 8 shows how the gaining of consent works within this framework. The data subject subscribes to a service provider (e.g., the heating controls of their home). They accept the requirements for that service (e.g., communication with the heating system). Once the data subject has done that, they are able to specify what policies they wish to add to their information. From then on, whenever the data subject connects to a service provider, the policies that they have applied to their account are used to govern the Action taken in the ECA process.

This is a very interesting and novel way in which consent can be managed over several IoT systems. However, as with the other two frameworks described, it does not consider the requirements of the data subject.

What we have seen above is not unusual in Pbd frameworks. Whilst there are frameworks that are able to record if consent has been given, and manage the personal data in an appropriate way, they do not look at how consent is given, and if the data subject actually is in a position to be able to give informed consent (Morales-Trujillo et al., 2018) (Perera et al., 2016) (Sing, 2018). There are, however, Pbd frameworks that appear to be made for use in systems that do not deal with personal data, and thus do not have a component for requesting data subject consent (Le Métayer, 2013) (Kung, Freytag and Kargl, 2011).

It appears that the areas of:

- How informed consent is reliably collected
- How the amount of personal data that is collected is only what is needed (data minimisation).
- How the processing and access to the personal data is minimized.

Do not appear to be explicitly covered within current Pbd frameworks.

2.7 Conclusions of Literature Review

In this chapter we have looked at several Pbd and CMS models. They all have a method of collecting consent, however with regards to gaining *informed consent* they are none of them have a method of doing this. Below is a bullet point summery of the framework's limitations and strengths:

Strengths:

- Frameworks have a method of collecting data subject's consent.
- The frameworks looked at do appear to manage the personal data in a secure and appropriate way.
- The use of Hyperledger (blockchain) technology to store the subjects' choices in Orange Consent Management Service appears to be a secure method of keeping it secure. Ensuring the integrity and availability of this data.

Limitations

- The frameworks while collecting consent do not take into account *how* consent is given. Typically, this is a “check box” to say that consent has been given.
- Gaining *informed consent* is something that is not considered in the frameworks looked at.
- The frameworks seem only to be made for people working within an organisations’ computing department, to assist the creation of a computing system.
- To gain *informed consent* other professions need to be consulted.

So, it can be said that there will need to be some extensions that would need to be implemented to allow my framework to gain informed consent.

We have looked at Pbd frameworks in this chapter, and it becomes clear that the frameworks looked at in this section do not have a way to confirm if the consent they are gaining is informed consent or not.

There are several requirements for the extensions we are now going to introduce. These include a method of identifying ***what*** it is that needs to be asked of the data subject. And framing the consent explanation to take into account the requirements of the system and the data subjects.

How the requirements of the data subjects are identified are outside of the scope of this research.

3 Proposed Model

3.1 Introduction

To bridge the gaps identified in the last chapter (Chapter 2) we looked to develop a model that can assist in the creation of a system that:

1. Includes concepts that help gain informed consent that can help design a computer system to store and process personal data in a way that is compliant with DPA legislation

In the model, there are several concepts that have been sourced from the UK's ICO. The choice of using the ICO as a basis of the definitions is that they are the UK's regulatory body for data protection. The Information Commissioner is the person appointed by the UK Government who has the power to investigate any data breaches and apply corrective actions such as issuing reprimands and, if needed, fines to organisations operating as either data controllers or data processors. The ICO also produced definitions on their website for the use of individuals and organisations in a manner that does not include legal jargon to aid in the understanding of the Data Protection Act 2018.

Other definitions are based on the text within the Data Protection Act 2018 itself, as this is the statue that implements GDPR in the UK. Differences between the text in the Data Protection Act 2018 and the text of the GDPR should be minimal, as the DPA 2018 has been implemented to bring GDPR into law in the UK.

Some of the concepts are not explicitly named in the DPA 2018, but the concept is implied by its role. For example, the data subject guardian is not mentioned by name in the act, however, the role is talked about in relation to children up to 16 (in the UK 13) (HMSO, 2018) and for those over 16 who are not likely to be able to give informed consent. For those over the age of 16, there is the assumption that they are able to give informed consent, unless it is shown otherwise, such as having Power of Attorney in place (ICO, 2020c).

I have added several other concepts into the model, while they are not mentioned in the DPA, these concepts would typically be used by organisations. For example, the data

acquirer. This is the entity that gets the consent from a data subject. This, in a larger organisation, is likely to be a website or a salesperson. The data acquirer would be authorised by the data controller to gain consent from a data subject. A data acquirer might also be a third-party employee in situations where a third-party organisation has been authorised to sell the service on behalf of the data controller.

In the papers that we covered in the Literature Review (Chapter 2) the concepts mentioned so far, either do not have a direct equivalent or are not mentioned.

I have added the new concept of Consent Request Explanations, this concept is critical to the ICBDF as this is the method that should increase the likelihood of informed consent being obtained by this framework.

The Consent Request Explanations are aimed to give the data subject an explanation that is full and clearly tailored to the data subject, this will allow them to be able to give informed consent. The explanations should include what information is required to provide a service, and how that information is going to be used and processed. It should also include if the information is going to be shared with third parties (e.g., banks to process payments, delivery companies so that physical items required for the service can be delivered). The explanations should also take into account requirements of the data subject.

An example of this might be where an introduction is given one to one by the data acquirer, then the explanation is given in a short video which uses visuals/audio/subtitles followed by a print out of the salient points and an enquiry from the data acquirer if there is anything else the data subject needs to clarify the explanation.

In this proposed model, we include the ability for an organisation to be able to provide multiple explanations of how they are going to use personal data. This allows the data subjects to be able to choose the explanation that they can most easily understand.[8] The choice will be recorded so that the organisation can demonstrate if asked, how it is attempting to gain informed consent.
The identification of the data subject's requirements is not part of this proposed framework. The proposed framework is showing that this needs to be considered when using the proposed model to create a system.

[8] The creation of consent request explanations may need the input of non-technical staff to help ensure they can be understood by members of the public

3.2 Proposed Framework

See next page

ICBDF

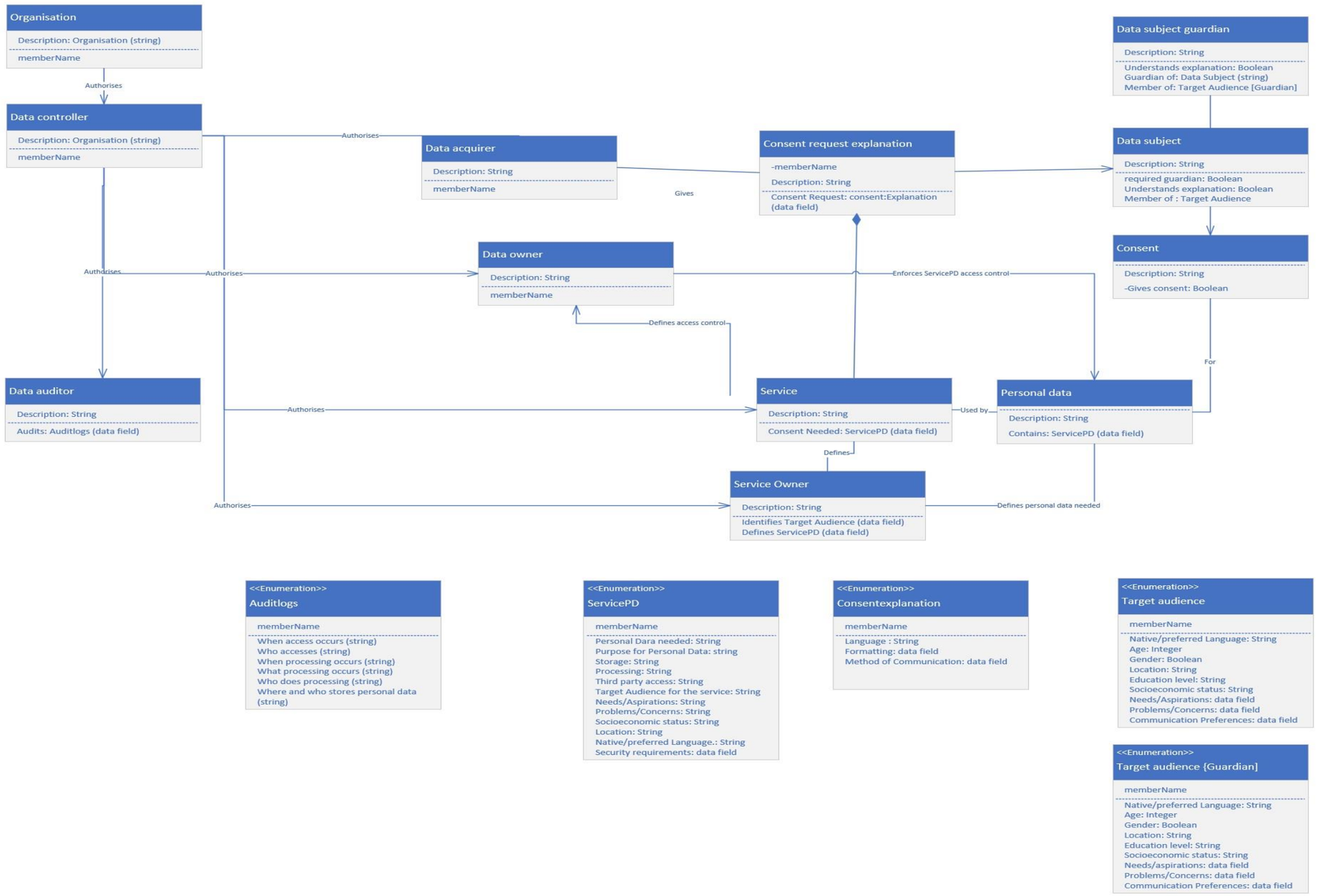

Organisation
Description: Organisation (string)
memberName
Authorises
Data controller
Description: Organisation (string)
memberName
Authorises
Data acquirer
Description: String
memberName
Gives
Consent request explanation
-memberName
Description: String
Consent Request: consent:Explanation (data field)
Data subject guardian
Description: String
Understands explanation: Boolean
Guardian of: Data Subject (string)
Member of: Target Audience [Guardian]
Data subject
Description: String
required guardian: Boolean
Understands explanation: Boolean
Member of : Target Audience
Consent
Description: String
-Gives consent: Boolean
For
Authorises
Authorises
Data owner
Description: String
memberName
Defines access control
Enforces ServicePD access control
Data auditor
Description: String
Audits: Auditlogs (data field)
Authorises
Service
Description: String
Consent Needed: ServicePD (data field)
Used by
Personal data
Description: String
Contains: ServicePD (data field)
Defines
Service Owner
Description: String
Identifies Target Audience (data field)
Defines ServicePD (data field)
Authorises
Defines personal data needed
<<Enumeration>>
Auditlogs
memberName
When access occurs (string)
Who accesses (string)
When processing occurs (string)
What processing occurs (string)
Who does processing (string)
Where and who stores personal data (string)
<<Enumeration>>
ServicePD
memberName
Personal Dara needed: String
Purpose for Personal Data: string
Storage: String
Processing: String
Third party access: String
Target Audience for the service: String
Needs/Aspirations: String
Problems/Concerns: String
Socioeconomic status: String
Location: String
Native/preferred Language.: String
Security requirements: data field
<<Enumeration>>
Consentexplanation
memberName
Language : String
Formatting: data field
Method of Communication: data field
<<Enumeration>>
Target audience
memberName
Native/preferred Language: String
Age: Integer
Gender: Boolean
Location: String
Education level: String
Socioeconomic status: String
Needs/Aspirations: data field
Problems/Concerns: data field
Communication Preferences: data field
<<Enumeration>>
Target audience {Guardian]
memberName
Native/preferred Language: String
Age: Integer
Gender: Boolean
Location: String
Education level: String
Socioeconomic status: String
Needs/aspirations: data field
Problems/Concerns: data field
Communication Preferences: data field

Figure 9: ICBDF

Figure 9: ICBDF shows the ICBDF, the concepts and how they are related. It is possible that there could be multiple instances of each of the entities within the ICBDF (e.g., more than one data subject or data processor). It is not envisaged that the Framework would be limited solely to one-to-one relationships. It shows that it would be possible to have a one-to-many relationship within the framework (e.g., one data controller with many data subjects or data processors).

The ICBDF uses strings in many cases to allow for data to be entered in a variety of formats, such as 1/10/10 or First of October 2010 for a date. Integer ranges are not set to allow for them to be configured in implementation as needed by an organization. It is recognised that in the case of gender (in target audience) is a Boolean value, although this can be changed to an integer or string to allow for non-binary genders as needed.

It is possible that a data subject may understand a consent request explanation, while their data subject guardian may not, (or the other way round). It is also possible that a data subject guardian may understand the explanation and give their consent but the data subject does not give their consent. In this case the data subject and data subject guardian need to understand the consent request explanation and give their consent for the personal data to be used by the organisation.

Below are definitions of the concepts of the Language used in the ICBDF:

1. **Informed Consent:**
   Is the permission that a data subject gives an organisation to use their personal data in a specific way. Based on (ICO, 2021a)**.**
   The informed consent is always owned by the data subject and can be modified or rescinded by the data subject at any time. The informed consent is given for the reasons the organisation has asked for to be able to provide a service. The data subject needs to understand what it is they are giving consent to.

2. **Data Subject**
   Is "… [a] living individual on whom personal data is held."(ICO, 2020b).

The data subject has the attributes of Target Audience. This gives the data subject a number of values (such as language) that they may acquire. This includes (but is not limited to) the data subject language, or age.

3. **Data Subject Guardian**

This is a person who has responsibility for the data subject.

This can be either because of their age (European Commission, 2018) (ICO, 2018), or if they are not likely to be able to give informed consent.

The data subject guardian has the enumeration of Target Audience Guardian. This gives the data subject guardian a number of values (such as language) that it may acquire. This includes (but is not limited to) the data subject guardian's language, age and needs.

4. **Consent Request Explanations:**

This is a collection of explanations that the organisation has created to give to the data subject.

The explanations would be provided to aid the data subject in understanding what giving consent for. The collection should be in appropriate formats for the data subject's requirements. Each of the explanations should detail what personal data is required, how and by whom it is going to be stored and processed, and the reasons for its storage and processing.

5. **Data Acquirer:**

The data acquirer is an entity that directly interacts with the data subject to gain consent.

This may be an employee of the organisation, the organisations' website, or a person not directly employed by the organisation but who has been authorised to work on behalf of the organisation.

The data acquirer does not perform any further actions with the personal data collected. This entity could be considered to be equivalent to a service user within the ITIL 4 framework (Brahmachary, 2019).

6. **Organisation**

"An organized group of people with a particular purpose, such as a business or government department."(Lexico Dictionaries, no date)[9]**.**

Within the ICBDF an organisation is the entity providing a service either directly to a data subject (this acting as a data controller) or to another organisation (thus acting as a data processor).

7. **Service**

"A government system or private organization that is responsible for a particular type of activity, or for providing a particular thing that people need."(Cambridge English Dictionary, no date c)**.**

Examples include: mobile phone services, education, online shopping, banking.

8. **Personal data**

Any information relating to a data subject

This could include information such as an individual's name, address, phone number. This could include additional attributes that could be included at a later time, or attributes that are not known. Subsets include:

a) **Sensitive data:**
A subset of personal data that requires additional protections.
This could include information such as sexuality, race, or genetic data.

b) **Identifiable data:**
Information that you can identify a data subject from.
This could be an Identity Number, or a combination of information that allows identification. (E.g., name, address and phone number)
Information that is in one of the Subsets may be identifiable via the definitions within the DPA, and thus steps to ensure the correct level of security are taken at the time of collection (e.g., asking for sensitive data in a private location).

9. **Data Controller**

"An organisation that determines the purpose and means of the processing of personal data" (HMSO, 2018)**.**

[9] English spelling can be with an S or a Z. US English is only with a Z.

This would be a person or persons who are the authorising authority within an organisation who have overall control over the purposes and means of using personal data (ICO, 2021b).

10. Service Owner

Entity within an organisation who has day to day ownership of the service and identifies what personal data is required to provide the service.

This entity does not have a formal definition within GDPR law, however the service owner would have the responsibilities of the service owner and service design manager within the ITIL 4 framework (Brahmachary, 2019). It is the service owner who identifies what personal data is required to be able to offer the service, how the personal data is to be stored and processed. The service owner also needs to specify if a third party is going to have access to some or all of the personal data collected and why they need to have access to it. The service owner also needs to ensure that the minimum amount of personal data is collected for the provision of the service.

Additionally, the service owner is responsible for identifying the "target audience" for the service. For the purpose of this thesis target audience is defined as "… a group of people having common interests, demographics, and behaviour"(Question pro, 2020).

11. Data Owner

Entity within an organisation who has day to day ownership of the security of the personal data held by the organisation.

This entity does not have a formal definition within the GDPR, however the actions carried out by the data owner are. The person (or team) is given responsibility by the data controller for ensuring that personal data is only used for the purpose(s) that the organisation has consent from the data subject to use it for. In addition, they have the responsibility of restricting access to only those people who need the data consented to in order to provide the service.

12. Data Audit Logs:

Record of all transactions that occur to the personal data within the organisation.

GDPR requires that an organisation keeps records of the processing and storage processing that takes place with personal data (ICO, no date).

13. **Data Auditor:**

This is the person (or persons) who is (are) responsible for auditing the consent within the system, and that the personal information needed for the service is as minimal as possible.

The team also investigate any data breaches. This function may be carried out by an internal team (e.g., Internal Audit) or a third party (e.g., the ICO, KPMG etc).

Relationships:

14. **Guardian of**

The data subject guardian is the guardian of a data subject if the data subject is not able to make informed consent.

15. **Ward of**

The data subject when not able to make informed consent is a ward of a data subject guardian.

The relationship between the data subject and data subject guardian modifies the "Gives" relationship, where if the data subject has a data subject guardian, both have to "Give" their consent.

A data subject may have a guardian for a time (while a child) then no longer have one (when they are over 13). Or they need a guardian when they have not previously needed one (e.g., due to illness). The data subject may not know that they are a ward of a data subject guardian in the case of illness.

A data subject guardian may be responsible for several data subject, such as a parent with more than one child.

16. **Owns**

Consent is always the property of the data subject.

17. **Gives**

The data subject "Gives" their consent for their personal data to be used. The data subject can always modify/change or rescind their permission they have "Given" to an organisation.

If the data subject has a guardian, then the organisation needs to be "Given" permission to use the personal data by both the data subject and the data subject guardian. In this case the data subject continues to enjoy the same protections regarding "Ownership" of their consent.

18. **Offers**

This is where one party offers another party something.

The organisation offers a service that a data subject wants to use.

A data acquirer offers the data subject a consent request explanation.

19. **Reports any breach to**

The data controller is responsible for keeping the data subject informed of any data breaches.

The data controller is also responsible for the compliance to the regulations by the organisation and any third parties used.

20. **Authorises**

The data controller authorises other entities to perform tasks on their behalf.

This includes when the data acquirer is authorised to gain consent from data subjects. The data controller also authorises the service owner, data owner, and the data processor(s). In addition, the data controller authorises and ensures the quality of the consent request explanations.

21. **Responsible for**

The data controller is responsible for the personal data held by the organisation.

This includes who has access to the personal data, and who can process the personal data.

22. **To use**

The relationship between one entity who wants to be able to use something that is provided by another entity.

For example: consent given by the data subject gives permission of the organisation to be able to use the personal data for providing the service.

The data subject would also want to use a service provided by an organisation.

23. **Requires some/Required to be able to provide**

To be able to provide a service, some personal data is required. The service needs to be able to store, access and process the personal data in some way.

24. **Defines personal data needed**

The service owner defines the personal data that is needed to provide the service. This needs to include what personal data is required; who needs to be able to access it: how it is stored; what processing is needed to be carried out on it; along with who does this processing.

It is important to ensure that the minimum amount of personal data is required, and if the personal data needed includes sensitive data, then additional protections need to be in place.

25. **Authorises Access To**

The data owner authorises who can access the personal data held. The data owner updates who is able to access the personal data as needed.

26. **Maintains**

The service owner maintains the service, as well as what personal data is required and what storage and processing is required on the personal data to enable the provision of the service.

27. **Logs All Transactions**

All Transactions on the personal data are recorded within the data audit logs.

This includes details of:

When consent is given, modified or rescinded.

Who has given consent?

What consent has been given for.

Who has accessed the personal data?

Who has processed the personal data?

Any breaches of security measures in place to protect the personal data.

The data audit logs will need a high level of integrity toensure that the information it contains are not corrupted. The data audit logs only contain data about personal data, and not the personal data itself.

28. **Uses for investigations and reporting**

Data auditors use the data audit logs to ensure that the personal data is being used in accordance to the consent that has been given.

Data auditors will also use the data audit logs to investigate any real or suspected breaches of security of the personal data.

29. **Request reports investigation of breaches**

The data controller will request investigations and or reports into any breaches of information from the data auditor

30. **Reports results to**

The data auditors report results of and investigations that have been carried out to the data controller.

31. **Is About**

Personal data is About a data subject.

32. Provides

A service that an organisation offers to give to a data subject.

For example, an organisation offers to provide a data subject a mobile phone service.

33. To

Is who the service is intended to be used by.

34. Defines

The organisation sets out the content and the format of the data consent explanations (Cambridge English Dictionary, no date a)**.**

The organisation needs to ensure that they are able to provide explanations that can be understood by the target audience of the service that they provide.

35. To Gain

The organisation needs to have the consent of the data subject to be able to use their personal data (Cambridge English Dictionary, no date b)**.**

36. Uses

The Data Audit Logs provide the information needed by the data Auditors to be able to report on any breaches of Personal data held by the organisation (Cambridge English Dictionary, no date d)**.**

37. About Usage of

The data Audit logs record how the personal data is being used within the organisation.

3.3 Guide for implementing the ICBDF

It is expected that an organisation is able to identify the people or teams that will responsible for each role outlined within the ICBDF. This is particularly important given the explanations of the responsibilities given above.

In this section we shall how the additional concepts detailed in the ICBDF can be implemented. We use UML2.0 as a modelling language which was chosen to demonstrate the ICBDF. This is for two reasons, firstly as I have chosen it because it has become the "…de facto modelling language for software development" (Lange and Chaudron, 2006) and is "… is rapidly becoming the standard for object-oriented systems development" (Grossman, Aronson and McCarthy, 2005). The second reason is that because of its popularity, it is likely to be one of the most accessible modelling languages in common use.

It is expected that other modelling languages (e.g., Secure Tropos) will be able to be used to model the additional concepts that the framework adds.

3.4 Use of the ICBDF in an opticians

In the diagram found in Appendix B there is a decision point - is the consent request understood?

The introduction of the concept of understanding the consent request explanation to existing models is linked to the existing concept of consent. This is because if a data subject does not understand what is being asked of them, then they are unable to give informed consent. Thus, it is important for an organisation to be able to communicate what they are asking of the data subject in a way that they are able to understand. In addition, the data subject needs to be able to agree to giving their consent. The data subjects understanding of the consent request explanation, and their agreement to give consent need to be recorded.

The attribute *explanation understood confirmation* is needed within the consent concept. Without the understanding of the explanation consent cannot be given. [10]

The consent request explanations are the main way that the organisation is able to ensure that the data subject is able to understand what is asked of them. Thus, there are attributes to the *consent request explanation* that will aid in their understandability. These include:

The Text Used: This includes things such as the language used, how long the sentences are, the use of technical or legal language, and is the language suitable for the target audience?

The Design and Layout: This would cover things such as the font and font size, if the text is easy to read, and if there is a clear layout.

Usefulness: Is the tone appropriate? Has the *consent Request Explanation* actually covered what it is intended to cover, this included the requirements of the service as well as the data subject.

This is showed in Figure 10: Consent Request Explanations.

[10] While it is difficult to be 100% sure if a customer actually understands the explanation, asking the customer if they understand is still an important step and allows them to say that they do not understand. How to ensure an explanation is understood is outside of the scope of this thesis

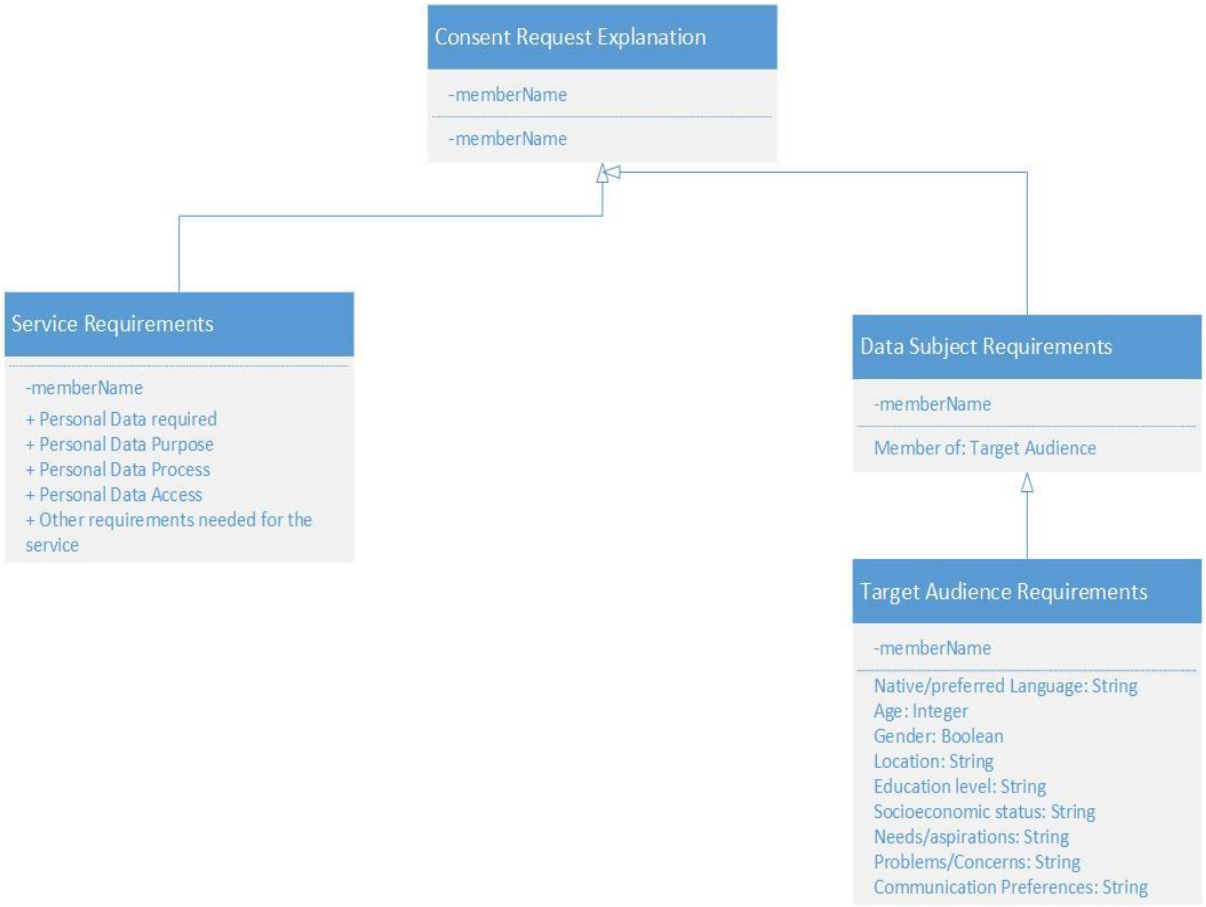


Figure 9: Consent Request Explanations.

Figure 10 shows that the Consent Request Explanation needs to include two sets of requirements. The first is the requirements of the system (e.g. what information is required). The second is the requirements of the Data Subject. The requirements of the Data Subject are gained from the requirements of the Target Audience that they are part of. The use of the Target Audience Requirements is *not* a method for discriminating any kind of disability or other factor (e.g. age, gender, or gender). Its use is to help the organisation tailor the consent request explanations to better serve the customer.

The above is inspired by (Plain English Campaign and Campaign, 2020).

3.5 Worked example: Example of the Use of The ICBDF When Visiting an Opticians

The diagram that is referenced in this worked example is found in Appendix B

A customer [data subject] enters the store and is approached by a member of staff [data acquirer]. The reason for the visit is identified (e.g., eye test, purchase of a new pair of glasses/contact lenses, collection of glasses/contact lenses).

The member of staff then checks the in-store system to confirm the information that is required from the data subject to be able to provide the service.

If consent has already been given [for example from a previous appointment] and the information has already been gathered, the member of staff will then confirm that the information is correct with the data subject.

If the required information has not previously been gathered. The staff member will request this from the customer by providing the data subject /data subject guardian with a consent request explanation.

The consent request explanation will need to meet the requirements of the data subject /data subject guardian, and detail what information/processing is needed to provide the service.

Identifying the requirements of the data subjects would be done via the identification of the target audience the service is being aimed at, and ensuring that the consent request explanations meet the requirements of the data subject /data subject guardian, as well as the requirements of the service. As mentioned in the previous section, the identification of the requirements for the target audience is to ensure that all customers regardless of ability or background are included. [Identifying the requirements of the data subjects is outside the scope of this work, however it is important that these requirements are included within the scope of producing the consent request explanations]. So the consent request explanations will need to ensure that they are accessible to the data subject /data subject guardian visiting the opticians.

The consent request explanation offered to the data subject /data subject guardian, needs to meet the requirements of the data subject /data subject guardian. If the request explanation offered to the data subject /data subject guardian is not understood, then they need to be offered another request explanation that they understand. It is envisioned that there would be several different consent request explainations' that are appropriate for the customer's needs.

If there isn't an appropriate request explanation, then this gap sould be highlighted within the system so that an appropriate request explanation can be created.

If the customer has a guardian [data subject guardian] then consent needs to be gained from both the customer and their guardian. Appropriate consent request explanations need to be available for the guardian.

The system then records that the customer has understood the explanation given to them and also that they have given consent.

The personal data is stored in the system in line with the access and security requirements of the system. Medical information (eg medications taken, medical history) are considered, by the DPA, to be sensitive personal data and should be stored to a higher standard than other personal data.

Payment information is shared with a third-party payment provider (i.e., the organisation's bank) for the payment of the eye test and or glasses. [In the case of NHS funded eye tests and glasses, the relevant information is passed to the NHS.]

Prescription information and measurements are shared with the glasses' manufacturer for the provision of the glasses ordered by the customer. [Note this only occurs if the customer orders a new pair of glasses. If the customer orders a non-prescription pair of glasses, only the measurements are shared.]

If the eye test has highlighted a previously undiagnosed medical condition, then this will be shared with the NHS (e.g., GP/Hospital) for treatment. [11]

[11] However, it is my understanding is that this can be passed to a medical professional under the provision of health care of the data subject.

The data audit log records what information has been passed to third parties and the reason for which it has been passed to them. It also logs where the personal data is held on the system.

The data owner has an ongoing responsibility to ensure that access to and use of personal data is restricted to entities that are approved to access it.

The service owner has an ongoing responsibility to ensure that only the minimum amount of personal data is recorded.

3.6 Example of the use of the ICBDF when creating a new system.

The following example is a way that the framework can be used when a telecoms company wants to launch a new service. This example is illustrated Appendix C use of the ICBDF when creating a new service.

The data controller would first authorise a service owner to define the service that is going to be offered. In the ICBDF the data controller is specific role, with specific actions.

In terms of GDPR the service owner will need to specify what personal data is required for the service, along with details such as how the personal data is going to be stored, who has access to the personal data, and what processing is going to be carried out on the personal data. If third parties require access to or need to process the personal data then this is to be documented, along with the reasons why the third-party needs access. For example, a bank will need to have access to the payment details for the reason of processing ongoing payments for the service. The service should not ask for additional personal data over and above what is needed for the provision of the service. If the ICBDF was not being used, then the data protection requirements may not be considered at this early stage of the development of the new system. Along with specifying how the personal data is needed and used, the service owner also needs to identify the target audience for the service. They will need to identify attributes about the target audience that have an effect on how the organisation is going to communicate with the data subject.

These attributes are also typically used by advertisers and marketing teams so that products can be advertised to a particular demographic audience.[12]

The data controller approves the personal data requirements of a service. The data controller will also appoint a data owner. The data owner is responsible for ensuring that only authorised entities can access the personal data stored by the organisation. The role of the data owner is one that has been introduced by the ICBDF so that there is a person/group that has specific responsibility to ensure that the data is protected.

The service owner, along with the data controller will develop the consent request explanations so that the explanations are accessible to the target audience of the service. The explanations should include enough detail so that a data subject is aware of how the personal data is being used, and by whom, to provide the service. The consent request explanations should be approved by the data controller to ensure the quality and understandability of the explanations. This is to ensure that the intended audience is included by the explanations. Without this step, the creation of appropriate consent request explanations would not be created. For example, presenting a consent form in small font for someone to sign, that refers the person to a website for details of what they are consenting to.

Data audit logs will be kept regarding the personal data. The data audit logs should contain enough information to allow for investigations to be carried out if the security of the personal data has been breached. This should include, when personal data has been accessed, who has accessed the personal data, when consent has been changed, when personal data has been updated (e.g., a data subject has let the organisation know of a change of their personal details).

The data auditors (which could be an organisations' internal auditors, or a third party such as the ICO) will use the data audit logs in the event of a breach being reported, or as a part of a regular auditing program to ensure that the systems are working.

The example demonstrates that using the ICBDF can help to ensure that there are auditable records of data subjects giving their informed consent, and that should there be a breach it can be fully investigated.

[12] The marketing of the service and the identification of the target audience's requirements is not in the scope of this paper

4 Evaluation.

4.1 Evaluation of the ICBDF

In this chapter we are going to look into how the ICBDF answers the research questions highlighted in section 1.3.2 Research Questions.

The Research Questions are repeated here for clarity.

i) Do Pbd frameworks and their concepts help design computer systems to store and process personal data that are compliant with the informed consent requirements of DPA legislation?

ii) If existing Pbd frameworks are not fully compliant, can they be extended to set out the foundations of an "Informed Consent by Design Framework" using metamodeling that is appropriate for computer systems?

   a. This should include a method to gain understanding of the data subject, but also help the organisation monitor its compliance.

For this evaluation, we are going to use the Orange Consent Management System as an example of an existing Pbd model to compare with the ICBDF as described in chapter 3.

We have already looked into the Orange Consent Management Service in Section 2.5 Consent Management Systems in Literature. This model was chosen for comparison with the ICBSF because it can help improve trust, as the consent is distributed across several systems, and there is no one single point of failure.

How does the Orange Consent Management Service help design computer systems store and process personal data that is compliant with the informed consent requirements of the DPA legislations?

The Orange Consent Management Service does assist in helping a system that is compliant with many of the requirements of the DPA legislation. For example, it helps create consent forms. It additionally allows for data subjects to be able to give more of a fine-grained control over what they are consenting to. Interestingly the Orange Consent Management Service leverages block chain technology, which is a technology that records transactions

(in this case a data subjects' choices) in a block of data and adds it to a chain (IBM, no date). The chain is not stored centrally, but is distributed. The way this is done means that it is very difficult for the choices made by the data subject to be changed by an outside party.

However, regarding the requirements of informed consent that have been set out by the DPA legislation, the Orange Consent Management Service does *not* have a method of gaining informed consent from the data subjects. The consent forms built by systems using this framework are more focused on asking for generic consent for the data to be stored and processed, rather than presenting the request that is likely for the data subject to understand enough to enable them to give informed consent.

Can we extend existing Pbd frameworks to set out the foundations of an "Informed Consent by Design Framework" using metamodeling that is appropriate for computer systems?

In this document we have shown that a framework can be set out that includes a way to attempt to gain informed consent from data subject. In the previous chapter we saw that the ICBDF, offers a method that can expand what can be done in regards to gaining informed consent. This has been done by the inclusion of the concept of the Consent Request Explanation to gain informed consent, which includes requirements from both the organisation, *and* the data subject. This is able to present an explanation of what the data subjects are being asked to consent to in a way that is more accessible. The ICBDF framework enables the data subject to be better able to give informed consent, as unlike other models it attempts to include the needs of the data subject as well as the needs of the system, whereas other models do not include the needs of the data subject.

5 Conclusions

5.1 Answering the research questions.

In relation to the research questions, we set out at the beginning of the research, we have shown in chapters 2 and 4 that current Pbd models, while they can help in managing an organisations Data Protection responsibility, do not attempt to tackle how an organisation would meet the requirements of Informed Consent set out in the Data Protection Act.

We have shown in chapters 3 and 4 that by extending existing Pbd frameworks it is possible to include steps to assist gaining informed consent from data subjects. This framework adds the requirements of the data subject along side the requirements of the system, when asking for informed consent, which can be added to other frameworks without affecting the rest of the framework.

5.2 Comments regarding the work

The ICBDF presented in this thesis is a foundation of a Pbd model that allows computer systems to gain informed consent from data subjects. A limitation is that it has not yet been used to create a system. It does however provide a framework that allows organisations to create a system that is easy to use without having to redesign the systems already in place.

The framework is a step forward in how organisations will be able to create computer systems that actually take steps in gaining *informed* consent. When implementing the ICBDF an organisation will need to spent time and effort in understanding what the target market for their services is, and this will help them ensure that they are requesting informed consent in a method better tailored for their target audience. In doing this, an organisation will be able to demonstrate that they are addressing their legal duties regarding the DPA.

It should also be noted that this work has only provided a way that a computing system can help gain informed consent from a data subject. It has not looked at the *how* informed consent is gained. This will need research not just from the computer science field, but also

other fields of research including psychology, ethics, education, and law. To fill gaps such as the “best” way to ask for consent, and how to ensure that updates in the law are considered, a multi-disciplinary team would ideally work together to aid in filling these gaps.

In addition, future work on the ICBDF should include using it in a real-life situation, so that it can be tested to ensure that it meets expectations in a live system. There are likely to be gaps that will be found when it is used for real, that are not envisioned when creating it in a theoretical way.

5.3 Final thoughts and areas of future research

The ICBDF model presented in this thesis is a starting point for future work to assist Pbd models to take into account how gaining informed consent from data subjects can be included in creating computer systems.

As mentioned previously in this thesis, the gaining of informed consent from a data subject is a difficult task. There are many fields of research that have looked into this, including psychology, law, education. The ICBDF is proposing a method of being able to include the work of these fields into a computer system, that improves the likelihood of meeting the requirements of the DPA.

Areas of future research found, as a result of researching this thesis, include:

1. How informed consent can actually be gained.
2. How to identify the requirements of the data subject and integrate them into a computer system.
3. How can an organisation know that they have gained *informed* consent?

Presented in this thesis, is one possible way to be able to gain informed consent in a computer system. This is a foundation rather than a complete solution to the questions we set out to answer, which it is hoped will help further research into this area.

6 References

Allison, P.R. (2019) ‘Data protection: How privacy can be a benefit, not a burden’, *Computer Weekly* [Preprint]. Available at: https://www.computerweekly.com/feature/Data-protection-How-privacy-can-be-a-benefit-not-a-burden.

Arnott, D., Lizama, F. and Song, Y. (2017) ‘Patterns of business intelligence systems use in organizations’, *Decision Support Systems*, 97, pp. 58–68. Available at: https://doi.org/10.1016/j.dss.2017.03.005.

Ashurst (2021) *China’s new data privacy law - what does it mean for you?*, *Website*. Available at: https://www.ashurst.com/en/news-and-insights/legal-updates/chinas-new-data-privacy-law-what-does-it-mean-for-you (Accessed: 21 January 2022).

BBC (2020a) ‘Brighton University students’ belongings binned by halls’, *BBC Website* [Preprint]. Available at: https://www.bbc.co.uk/news/uk-england-sussex-53860029.

BBC (2020b) ‘Grandmother ordered to delete Facebook photos under GDPR’, *Website* [Preprint]. Available at: https://www.bbc.co.uk/news/technology-52758787.

BBC (2021) *Amazon hit with $886m fine for alleged data law breach*, *Website*. Available at: https://www.bbc.co.uk/news/business-58024116 (Accessed: 31 August 2021).

Bialke, M. *et al.* (2018) ‘MAGIC: Once upon a time in consent management - A FHIR®tale’, *Journal of Translational Medicine*, 16(1), pp. 1–12. Available at: https://doi.org/10.1186/s12967-018-1631-3.

Brahmachary, A. (2019) *ITIL Roles and Responsibilities – Process Wise | ITSM Roles*, *Certguidance website*. Available at: https://www.certguidance.com/processes-wise-itil-roles-itsm/ (Accessed: 13 July 2021).

vom Brocke, J. *et al.* (2015) ‘Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research’, *Communications of the Association for Information Systems*, 37(August), pp. 205–224. Available at: https://doi.org/10.17705/1CAIS.03709.

Cambridge English Dictionary (no date a) *Defines Cambridge English Dictionary*, *Website*. Available at: https://dictionary.cambridge.org/dictionary/english/define?q=Define

(Accessed: 14 July 2021).

Cambridge English Dictionary (no date b) *Gain Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/gain?q=Gain (Accessed: 14 July 2021).

Cambridge English Dictionary (no date c) *SERVICE meaning in the Cambridge English Dictionary., Online*. Available at: https://dictionary.cambridge.org/dictionary/english/require (Accessed: 9 July 2021).

Cambridge English Dictionary (no date d) *Use Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/use.

Cavoukian, A. (2009) 'Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices', *Information and Privacy Commissioner of Ontario, Canada*, p. 5. Available at: https://doi.org/10.1007/s12394-010-0062-y.

Cavoukian, A. (2012) *Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices*. 1st edn. Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. and Jonas, J. (2012) 'Privacy by Design in the Age of Big Data', *Information and Privacy Commisioner*, (June), pp. 1–17. Available at: https://doi.org/10.1126/science.aaa5945.

Channel 4 news (2018) 'Data, Democracy and Dirty Tricks – Channel 4 News.', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Channel 4 news (2020) '"Are people going to be excluded from workplace if they don't go with contact tracing app?" - Newcastle University's Lilian Edwards', *Online* [Preprint]. Available at: https://www.channel4.com/news/are-people-going-to-be-excluded-from-workplace-if-they-dont-go-with-contact-tracing-app-newcastle-universitys-lilian-edwards.

CMS Law (no date) *GDPR Enforcement Tracker, Website*. Available at: view-source:https://www.enforcementtracker.com/ (Accessed: 3 July 2022).

CNIL (2019) *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, Online*. Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

Cronin, M. (2009) ‘10 Principles Of Readability And Web Typography’, *Website* [Preprint]. Available at: https://www.smashingmagazine.com/2009/03/10-principles-for-readable-web-typography/.

DuBay, W.H. (2004) ‘The principles of readability: A brief introduction to readability research’, *Impact Information*, (949), pp. 1–72. Available at: https://doi.org/10.1.1.91.4042.

European Commission (2011) ‘Privacy and Data Protection Impact Assessment Framework for RFID Applications’, (January), pp. 1–24.

European Commission (2018) *Regulation (EU) 2016/679*.

European Parliament (2016) ‘General Data Protection Regulations’, *Official journal of the European Union* [Preprint]. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

European Union (2016) ‘Regulation 2016/679’, *Official Journal of the European Communities*, 2014(March 2014), pp. 1–88. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

Fatema, K. *et al.* (2017) ‘Compliance through informed consent: Semantic based consent permission and data management model’, *CEUR Workshop Proceedings*, 1951.

Geidel, L., Bahls, T. and Hoffmann, W. (2014) *May I? - Challenges to a generic, automated electronic administration of consent*, *GMDS 2014. 59th Annual Meeting of the German Society for Medical Informatics, Biometry and Epidemiology (GMDS)*. 4 September 2014. Available at: https://www.egms.de/static/en/meetings/gmds2014/14gmds131.shtml.

Genestier, J.O.T.I.S.F.T.A.. (2017) ‘BLOCKCHAIN FOR CONSENT MANAGEMENT IN THE EHEALTH ENVIRONMENT: A NUGGET FOR PRIVACY AND SECURITY CHALLENGES Introduction and Use Case’, *J Int Soc Telemed eHealth*, 5, pp. 24–25.

Gilda, S. and Mehrotra, M. (2018) ‘Blockchain for Student Data Privacy and Consent’, *2018 International Conference on Computer Communication and Informatics, ICCCI 2018*, pp. 1–5. Available at: https://doi.org/10.3897/zookeys.788.30148.

Goecks, L.S. *et al.* (2021) ‘Design Science Research in practice: Review of applications in Industrial Engineering’, *Gestao e Producao*, 28(4), pp. 1–19. Available at:

https://doi.org/10.1590/1806-9649-2021v28e5811.

Grossman, M., Aronson, J.E. and McCarthy, R. V. (2005) 'Does UML make the grade? Insights from the software development community', *Information and Software Technology*, 47(6), pp. 383–397. Available at: https://doi.org/10.1016/j.infsof.2004.09.005.

Guardian, T. (2020) 'EasyJet reveals cyber-attack exposed 9m customers' details', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Hall, M., Marshall, M. and Howarth, A. (2020) *Skeptics with a K*. UK: Merseyside Skeptics Society.

Hammer, M.J. (2016) 'Informed consent in the changing landscape of research', *Oncology Nursing Forum*, 43(5), pp. 558–560. Available at: https://doi.org/10.1188/16.ONF.558-560.

HMSO (2018) *Data Protection Act 2018, HMSO*. Available at: https://doi.org/10.1016/S1067-2516(00)80076-9.

Horwitz, J. (2021) *China passes new personal data privacy law, to take effect Nov. 1, Reuters*. Available at: https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/ (Accessed: 20 August 2021).

House, C. (2020) 'CAMBRIDGE ANALYTICA(UK) LIMITED', *Website* [Preprint]. Available at: https://beta.companieshouse.gov.uk/company/09375920.

IBM (no date) *Blockchain success starts here, Website*. Available at: https://www.ibm.com/uk-en/topics/what-is-blockchain (Accessed: 26 June 2022).

ICO (2018) *Children, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/ (Accessed: 25 May 2019).

ICO (2019a) 'Data protection by design and default', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (2019b) *ICO says that voice data collected unlawfully by HMRC should be deleted, ICO website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-

blogs/2019/05/ico-says-that-voice-data-collected-unlawfully-by-hmrc-should-be-deleted/.

ICO (2019c) *Intention to fine British Airways £183.39m under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/.

ICO (2019d) *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

ICO (2019e) 'Penalties', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/.

ICO (2020a) 'Data protection by design and default', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (2020b) *Definitions, Website*. Available at: https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/ (Accessed: 4 July 2021).

ICO (2020c) 'What is valid consent?', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

ICO (2021a) *Consent, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (Accessed: 13 July 2021).

ICO (2021b) *Controllers and processors, Websire*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/. (Accessed: 9 July 2021).

ICO (no date) *Documentation, Webpage*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (Accessed: 13 July 2021).

Isaacs, A. (2014) 'An overview of qualitative research methodology for public health researchers', *International Journal of Medicine and Public Health*, 4(4), p. 318. Available

at: https://doi.org/10.4103/2230-8598.144055.

Islam, S., Mouratidis, H. and Jürjens, J. (2011) ‘A framework to support alignment of secure software engineering with legal regulations’, *Software and Systems Modeling*, 10(3), pp. 369–394. Available at: https://doi.org/10.1007/s10270-010-0154-z.

Jetu, F.T. and Riedl, R. (2012) ‘Determinants of Information Systems and Information Technology Project Team Success: A Literature Review and a Conceptual Model’, *Communications of the Association for Information Systems*, 30(1). Available at: https://doi.org/10.17705/1cais.03027.

Kung, A., Freytag, J.C. and Kargl, F. (2011) ‘Privacy-by-design in ITS applications’, *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings*, pp. 1–6. Available at: https://doi.org/10.1109/WoWMoM.2011.5986166.

Lange, C.F.J. and Chaudron, M.R. V (2006) ‘In Practice: UML Software Architecture and Design Description’, *Ieee Software* [Preprint].

Lexico Dictionaries (no date) *ORGANIZATION | Definition of ORGANIZATION by Oxford Dictionary, Lexico Dictionaries Online English*. Available at: https://www.lexico.com/definition/organization (Accessed: 7 July 2021).

Lexology (2021) *The impact of the GDPR outside the EU - Lexology. [ONLINE], Website*. Available at: https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f (Accessed: 25 August 2021).

Lomas, N. (2019) ‘Most EU cookie “consent” notices are meaningless or manipulative, study finds’, *Tech Crunch* [Preprint]. Available at: https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGT0n55tXVP0W5OHBZPDib2wxg5MZQRNy4q_FvRvLeY2G2HHGTAm3NW4bnyN7OVg.

Loughlin, M. *et al.* (2013) ‘Explanation , understanding , objectivity and experience’, 19, pp. 415–421. Available at: https://doi.org/10.1111/jep.12060.

McKernan, B. (2021) *Israeli authorities inspect NSO Group offices after Pegasus*

revelations, The Guardian website. Available at: https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations (Accessed: 29 July 2021).

Meneszes, A. (2019) *First GDPR fine in Portugal issued against hospital for three violations, The Privacy Advisor*. Available at: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

Le Métayer, D. (2013) 'Privacy by design: Formal framework for the analysis of architectural choices', *CODASPY 2013 - Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, pp. 95–104. Available at: https://doi.org/10.1145/2435349.2435361.

Morales-Trujillo, M.E. *et al.* (2018) 'Privacy by design in software engineering: A systematic mapping study', *Avances en Ingenieria de Software a Nivel Iberoamericano, CIbSE 2018*, 22(1), pp. 107–120.

Neisse, R. *et al.* (2015) 'An agent-based framework for Informed Consent in the internet of things', *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, (3), pp. 789–794. Available at: https://doi.org/10.1109/WF-IoT.2015.7389154.

O'Connor, Y. *et al.* (2017) 'Privacy by Design: Informed Consent and Internet of Things for Smart Health', *Procedia Computer Science*, 113, pp. 653–658. Available at: https://doi.org/10.1016/j.procs.2017.08.329.

O'Neil, O. (2003) 'Some limits of informed consent', *Journal of Medical Ethics*, 29(1), pp. 4–7. Available at: https://doi.org/10.1136/jme.29.1.4.

Orange (2022) *Blockchain for consent management: improved privacy and user control, Website*.

Pace, E. (1997) 'P. G. Gebhard, 69, Developer Of the Term "Informed Consent"', *The New York Times*, p. Section D Page 21. Available at: https://www.nytimes.com/1997/08/26/us/p-g-gebhard-69-developer-of-the-term-informed-consent.html.

Peffers, K. *et al.* (2006) 'THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH', *1st International Conference, DESRIST 2006 Proceedings. (pp. 83-106). Claremont Graduate*

University., 18, pp. 583–594.

Perera, C. *et al.* (2016) 'Privacy-by-design framework for assessing internet of things applications and platforms', *ACM International Conference Proceeding Series*, 07-09-Nove, pp. 83–92. Available at: https://doi.org/10.1145/2991561.2991566.

Perera, C. *et al.* (2020) 'Designing privacy-aware internet of things applications', *Information Sciences*, 512, pp. 238–257. Available at: https://doi.org/10.1016/j.ins.2019.09.061.

Piras, L. *et al.* (2019) 'DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance', pp. 78–93. Available at: https://doi.org/10.1007/978-3-030-27813-7_6.

Plain English Campaign and Campaign, P.E. (2020) *Plain English Campaign, Website*. Available at: http://www.plainenglish.co.uk/.

Practical Law Employment, Employment, P.L. and Practical Law Employment (2020) *Comparisons: DPA 1998 v GDPR and DPA 2018, Website*. Available at: https://uk.practicallaw.thomsonreuters.com/w-011-6935?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (Accessed: 21 May 2020).

Question pro (2020) *Target Audience: What is and how to define it, Website*. Available at: https://www.questionpro.com/blog/what-is-a-target-audience/.

Robol, M. *et al.* (2018) 'Modeling and reasoning about privacy-consent requirements', *Lecture Notes in Business Information Processing*, 335(May), pp. 238–254. Available at: https://doi.org/10.1007/978-3-030-02302-7_15.

Schartum, D.W. (2016) 'Making privacy by design operative', *International Journal of Law and Information Technology*, 24(2), pp. 151–175. Available at: https://doi.org/10.1093/ijlit/eaw002.

Schryen, G. (2015) 'Writing qualitative is literature reviews -Guidelines for synthesis, interpretation, and guidance of research association for nformation ystems writing qualitative is literature reviews - guidelines for Synthesis, Interpretation, and Guidance of Research', *Communications of the Association for Information Systems*, 37(12), pp. 286–325. Available at: http://aisel.aisnet.org/cais.

Schwarz, A. *et al.* (2007) 'Understanding Frameworks and Reviews : A Commentary to

Assist us in Moving Our Field Forward by Analyzing Our Past', *The DATA BASE for Advances in Information Systems*, 38(3), pp. 29–50. Available at: https://doi.org/http://doi.acm.org/10.1145/1278253.1278259.

Shore, J. and Steinman, J. (2015) 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy', *Technology Science*, pp. 1–37. Available at: http://techscience.org/a/2015081102/.

Sing, E. (2018) 'A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR'.

Smooth Radio (no date) *Smooth Chil - Music To Chill To, Webpage*. Available at: https://www.smoothradio.com/chill/ (Accessed: 4 September 2022).

Spiekermann, S. (2012) 'The challenges of privacy by design', *Communications of the ACM*, 55(7), pp. 38–40. Available at: https://doi.org/10.1145/2209249.2209263.

State of Callifornia Department of Justice; Office of the Attorney General (2021) *California Consumer Privacy Act (CCPA), Website*. Available at: https://www.oag.ca.gov/privacy/ccpa (Accessed: 25 August 2021).

The Open Data Institute (2018) 'ODI survey reveals British consumer attitudes to sharing personal data', *Website* [Preprint]. Available at: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/.

Utz, C. *et al.* (2019) '(Un)informed Consent: Studying GDPR consent notices in the field', *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 973–990. Available at: https://doi.org/10.1145/3319535.3354212.

White, R. and Gunstone, R. (2014) *Probing Understanding, Journal of Chemical Information and Modeling*. Available at: https://doi.org/10.1017/CBO9781107415324.004.

Wicker, S.B. and Schrader, D.E. (2011) 'Privacy-aware design principles for information networks', *Proceedings of the IEEE*, 99(2), pp. 330–350. Available at: https://doi.org/10.1109/JPROC.2010.2073670.

Wiggins, G. and McTighe, J. (2005) *Understanding by Design, Association for Supervision and Curriculum Development*.

Wong, J.C. (2019) 'The Cambridge Analytica scandal changed the world – but it didn't

change Facebook', *The Guardian* [Preprint]. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

Wuyts, K., Scandariato, R. and Joosen, W. (2014) 'Empirical evaluation of a privacy-focused threat modeling methodology', *Journal of Systems and Software,* 96, pp. 122–138. Available at: https://doi.org/10.1016/j.jss.2014.05.075.

Zarrabi, F. *et al.* (2012) 'A Meta-model for Legal Compliance and Trustworthiness of Information Systems', *CAiSE 2012 Workshops LNBIP,* (112), pp. 46–60.

Allison, P.R. (2019) 'Data protection: How privacy can be a benefit, not a burden', *Computer Weekly* [Preprint]. Available at: https://www.computerweekly.com/feature/Data-protection-How-privacy-can-be-a-benefit-not-a-burden.

Arnott, D., Lizama, F. and Song, Y. (2017) 'Patterns of business intelligence systems use in organizations', *Decision Support Systems,* 97, pp. 58–68. Available at: https://doi.org/10.1016/j.dss.2017.03.005.

Ashurst (2021) *China's new data privacy law - what does it mean for you?, Website*. Available at: https://www.ashurst.com/en/news-and-insights/legal-updates/chinas-new-data-privacy-law-what-does-it-mean-for-you (Accessed: 21 January 2022).

BBC (2020a) 'Brighton University students' belongings binned by halls', *BBC Website* [Preprint]. Available at: https://www.bbc.co.uk/news/uk-england-sussex-53860029.

BBC (2020b) 'Grandmother ordered to delete Facebook photos under GDPR', *Website* [Preprint]. Available at: https://www.bbc.co.uk/news/technology-52758787.

BBC (2021) *Amazon hit with $886m fine for alleged data law breach, Website*. Available at: https://www.bbc.co.uk/news/business-58024116 (Accessed: 31 August 2021).

Bialke, M. *et al.* (2018) 'MAGIC: Once upon a time in consent management - A FHIR®tale', *Journal of Translational Medicine,* 16(1), pp. 1–12. Available at: https://doi.org/10.1186/s12967-018-1631-3.

Brahmachary, A. (2019) *ITIL Roles and Responsibilities – Process Wise | ITSM Roles, Certguidance website*. Available at: https://www.certguidance.com/processes-wise-itil-roles-itsm/ (Accessed: 13 July 2021).

vom Brocke, J. *et al.* (2015) ‘Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research’, *Communications of the Association for Information Systems*, 37(August), pp. 205–224. Available at: https://doi.org/10.17705/1CAIS.03709.

Cambridge English Dictionary (no date a) *Defines Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/define?q=Define (Accessed: 14 July 2021).

Cambridge English Dictionary (no date b) *Gain Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/gain?q=Gain (Accessed: 14 July 2021).

Cambridge English Dictionary (no date c) *SERVICE meaning in the Cambridge English Dictionary., Online*. Available at: https://dictionary.cambridge.org/dictionary/english/require (Accessed: 9 July 2021).

Cambridge English Dictionary (no date d) *Use Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/use.

Cavoukian, A. (2009) ‘Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices’, *Information and Privacy Commissioner of Ontario, Canada*, p. 5. Available at: https://doi.org/10.1007/s12394-010-0062-y.

Cavoukian, A. (2012) *Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices*. 1st edn. Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. and Jonas, J. (2012) ‘Privacy by Design in the Age of Big Data’, *Information and Privacy Commisioner*, (June), pp. 1–17. Available at: https://doi.org/10.1126/science.aaa5945.

Channel 4 news (2018) ‘Data, Democracy and Dirty Tricks – Channel 4 News.’, *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Channel 4 news (2020) ‘“Are people going to be excluded from workplace if they don’t go with contact tracing app?” - Newcastle University’s Lilian Edwards’, *Online* [Preprint]. Available at: https://www.channel4.com/news/are-people-going-to-be-excluded-from-

workplace-if-they-dont-go-with-contact-tracing-app-newcastle-universitys-lilian-edwards.

CMS Law (no date) *GDPR Enforcement Tracker*, *Website*. Available at: view-source:https://www.enforcementtracker.com/ (Accessed: 3 July 2022).

CNIL (2019) *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, *Online*. Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

Cronin, M. (2009) '10 Principles Of Readability And Web Typography', *Website* [Preprint]. Available at: https://www.smashingmagazine.com/2009/03/10-principles-for-readable-web-typography/.

DuBay, W.H. (2004) 'The principles of readability: A brief introduction to readability research', *Impact Information*, (949), pp. 1–72. Available at: https://doi.org/10.1.1.91.4042.

European Commission (2011) 'Privacy and Data Protection Impact Assessment Framework for RFID Applications', (January), pp. 1–24.

European Commission (2018) *Regulation (EU) 2016/679*.

European Parliament (2016) 'General Data Protection Regulations', *Official journal of the European Union* [Preprint]. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

European Union (2016) 'Regulation 2016/679', *Official Journal of the European Communities*, 2014(March 2014), pp. 1–88. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

Fatema, K. *et al.* (2017) 'Compliance through informed consent: Semantic based consent permission and data management model', *CEUR Workshop Proceedings*, 1951.

Geidel, L., Bahls, T. and Hoffmann, W. (2014) *May I? - Challenges to a generic, automated electronic administration of consent, GMDS 2014. 59th Annual Meeting of the German Society for Medical Informatics, Biometry and Epidemiology (GMDS)*. 4 September 2014. Available at: https://www.egms.de/static/en/meetings/gmds2014/14gmds131.shtml.

Genestier, J.O.T.I.S.F.T.A.. (2017) 'BLOCKCHAIN FOR CONSENT MANAGEMENT

IN THE EHEALTH ENVIRONMENT: A NUGGET FOR PRIVACY AND SECURITY CHALLENGES Introduction and Use Case', *J Int Soc Telemed eHealth*, 5, pp. 24–25.

Gilda, S. and Mehrotra, M. (2018) 'Blockchain for Student Data Privacy and Consent', *2018 International Conference on Computer Communication and Informatics, ICCCI 2018*, pp. 1–5. Available at: https://doi.org/10.3897/zookeys.788.30148.

Goecks, L.S. *et al.* (2021) 'Design Science Research in practice: Review of applications in Industrial Engineering', *Gestao e Producao*, 28(4), pp. 1–19. Available at: https://doi.org/10.1590/1806-9649-2021v28e5811.

Grossman, M., Aronson, J.E. and McCarthy, R. V. (2005) 'Does UML make the grade? Insights from the software development community', *Information and Software Technology*, 47(6), pp. 383–397. Available at: https://doi.org/10.1016/j.infsof.2004.09.005.

Guardian, T. (2020) 'EasyJet reveals cyber-attack exposed 9m customers' details', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Hall, M., Marshall, M. and Howarth, A. (2020) *Skeptics with a K*. UK: Merseyside Skeptics Society.

Hammer, M.J. (2016) 'Informed consent in the changing landscape of research', *Oncology Nursing Forum*, 43(5), pp. 558–560. Available at: https://doi.org/10.1188/16.ONF.558-560.

HMSO (2018) *Data Protection Act 2018, HMSO*. Available at: https://doi.org/10.1016/S1067-2516(00)80076-9.

Horwitz, J. (2021) *China passes new personal data privacy law, to take effect Nov. 1, Reuters*. Available at: https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/ (Accessed: 20 August 2021).

House, C. (2020) 'CAMBRIDGE ANALYTICA(UK) LIMITED', *Website* [Preprint]. Available at: https://beta.companieshouse.gov.uk/company/09375920.

IBM (no date) *Blockchain success starts here, Website*. Available at: https://www.ibm.com/uk-en/topics/what-is-blockchain (Accessed: 26 June 2022).

ICO (2018) *Children, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-

data-protection/key-data-protection-themes/children/ (Accessed: 25 May 2019).

ICO (2019a) ‘Data protection by design and default’, *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (2019b) *ICO says that voice data collected unlawfully by HMRC should be deleted, ICO website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/ico-says-that-voice-data-collected-unlawfully-by-hmrc-should-be-deleted/.

ICO (2019c) *Intention to fine British Airways £183.39m under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/.

ICO (2019d) *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

ICO (2019e) ‘Penalties’, *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/.

ICO (2020a) ‘Data protection by design and default’, *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (2020b) *Definitions, Website*. Available at: https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/ (Accessed: 4 July 2021).

ICO (2020c) ‘What is valid consent?’, *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

ICO (2021a) *Consent, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (Accessed: 13 July 2021).

ICO (2021b) *Controllers and processors, Websire*. Available at: https://ico.org.uk/for-

organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/. (Accessed: 9 July 2021).

ICO (no date) *Documentation, Webpage*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (Accessed: 13 July 2021).

Isaacs, A. (2014) 'An overview of qualitative research methodology for public health researchers', *International Journal of Medicine and Public Health*, 4(4), p. 318. Available at: https://doi.org/10.4103/2230-8598.144055.

Islam, S., Mouratidis, H. and Jürjens, J. (2011) 'A framework to support alignment of secure software engineering with legal regulations', *Software and Systems Modeling*, 10(3), pp. 369–394. Available at: https://doi.org/10.1007/s10270-010-0154-z.

Jetu, F.T. and Riedl, R. (2012) 'Determinants of Information Systems and Information Technology Project Team Success: A Literature Review and a Conceptual Model', *Communications of the Association for Information Systems*, 30(1). Available at: https://doi.org/10.17705/1cais.03027.

Kung, A., Freytag, J.C. and Kargl, F. (2011) 'Privacy-by-design in ITS applications', *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings*, pp. 1–6. Available at: https://doi.org/10.1109/WoWMoM.2011.5986166.

Lange, C.F.J. and Chaudron, M.R. V (2006) 'In Practice: UML Software Architecture and Design Description', *Ieee Software* [Preprint].

Lexico Dictionaries (no date) *ORGANIZATION | Definition of ORGANIZATION by Oxford Dictionary, Lexico Dictionaries Online English*. Available at: https://www.lexico.com/definition/organization (Accessed: 7 July 2021).

Lexology (2021) *The impact of the GDPR outside the EU - Lexology. [ONLINE], Website*. Available at: https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f (Accessed: 25 August 2021).

Lomas, N. (2019) 'Most EU cookie "consent" notices are meaningless or manipulative, study finds', *Tech Crunch* [Preprint]. Available at: https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-

manipulative-study-finds/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGT0n55tXVP0W5OHBZPDib2wxg5MZQRNy4q_FvRvLeY2G2HHGTAm3NW4bnyN7OVg.

Loughlin, M. *et al.* (2013) 'Explanation , understanding , objectivity and experience', 19, pp. 415–421. Available at: https://doi.org/10.1111/jep.12060.

McKernan, B. (2021) *Israeli authorities inspect NSO Group offices after Pegasus revelations, The Guardian website*. Available at: https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations (Accessed: 29 July 2021).

Meneszes, A. (2019) *First GDPR fine in Portugal issued against hospital for three violations, The Privacy Advisor*. Available at: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

Le Métayer, D. (2013) 'Privacy by design: Formal framework for the analysis of architectural choices', *CODASPY 2013 - Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, pp. 95–104. Available at: https://doi.org/10.1145/2435349.2435361.

Morales-Trujillo, M.E. *et al.* (2018) 'Privacy by design in software engineering: A systematic mapping study', *Avances en Ingenieria de Software a Nivel Iberoamericano, CIbSE 2018*, 22(1), pp. 107–120.

Neisse, R. *et al.* (2015) 'An agent-based framework for Informed Consent in the internet of things', *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, (3), pp. 789–794. Available at: https://doi.org/10.1109/WF-IoT.2015.7389154.

O'Connor, Y. *et al.* (2017) 'Privacy by Design: Informed Consent and Internet of Things for Smart Health', *Procedia Computer Science*, 113, pp. 653–658. Available at: https://doi.org/10.1016/j.procs.2017.08.329.

O'Neil, O. (2003) 'Some limits of informed consent', *Journal of Medical Ethics*, 29(1), pp. 4–7. Available at: https://doi.org/10.1136/jme.29.1.4.

Orange (2022) *Blockchain for consent management: improved privacy and user control, Website*.

Pace, E. (1997) ‘P. G. Gebhard, 69, Developer Of the Term “Informed Consent”’, *The New York Times*, p. Section D Page 21. Available at: https://www.nytimes.com/1997/08/26/us/p-g-gebhard-69-developer-of-the-term-informed-consent.html.

Peffers, K. *et al.* (2006) ‘THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH’, *1st International Conference, DESRIST 2006 Proceedings. (pp. 83-106). Claremont Graduate University.*, 18, pp. 583–594.

Perera, C. *et al.* (2016) ‘Privacy-by-design framework for assessing internet of things applications and platforms’, *ACM International Conference Proceeding Series*, 07-09-Nove, pp. 83–92. Available at: https://doi.org/10.1145/2991561.2991566.

Perera, C. *et al.* (2020) ‘Designing privacy-aware internet of things applications’, *Information Sciences*, 512, pp. 238–257. Available at: https://doi.org/10.1016/j.ins.2019.09.061.

Piras, L. *et al.* (2019) ‘DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance’, pp. 78–93. Available at: https://doi.org/10.1007/978-3-030-27813-7_6.

Plain English Campaign and Campaign, P.E. (2020) *Plain English Campaign, Website*. Available at: http://www.plainenglish.co.uk/.

Practical Law Employment, Employment, P.L. and Practical Law Employment (2020) *Comparisons: DPA 1998 v GDPR and DPA 2018, Website*. Available at: https://uk.practicallaw.thomsonreuters.com/w-011-6935?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (Accessed: 21 May 2020).

Question pro (2020) *Target Audience: What is and how to define it, Website*. Available at: https://www.questionpro.com/blog/what-is-a-target-audience/.

Robol, M. *et al.* (2018) ‘Modeling and reasoning about privacy-consent requirements’, *Lecture Notes in Business Information Processing*, 335(May), pp. 238–254. Available at: https://doi.org/10.1007/978-3-030-02302-7_15.

Schartum, D.W. (2016) ‘Making privacy by design operative’, *International Journal of Law and Information Technology*, 24(2), pp. 151–175. Available at:

https://doi.org/10.1093/ijlit/eaw002.

Schryen, G. (2015) ‘Writing qualitative is literature reviews -Guidelines for synthesis, interpretation, and guidance of research association for nformation ystems writing qualitative is literature reviews - guidelines for Synthesis, Interpretation, and Guidance of Research’, *Communications of the Association for Information Systems*, 37(12), pp. 286–325. Available at: http://aisel.aisnet.org/cais.

Schwarz, A. *et al.* (2007) ‘Understanding Frameworks and Reviews : A Commentary to Assist us in Moving Our Field Forward by Analyzing Our Past’, *The DATA BASE for Advances in Information Systems*, 38(3), pp. 29–50. Available at: https://doi.org/http://doi.acm.org/10.1145/1278253.1278259.

Shore, J. and Steinman, J. (2015) ‘Did You Really Agree to That? The Evolution of Facebook’s Privacy Policy’, *Technology Science*, pp. 1–37. Available at: http://techscience.org/a/2015081102/.

Sing, E. (2018) ‘A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR’.

Smooth Radio (no date) *Smooth Chil - Music To Chill To, Webpage*. Available at: https://www.smoothradio.com/chill/ (Accessed: 4 September 2022).

Spiekermann, S. (2012) ‘The challenges of privacy by design’, *Communications of the ACM*, 55(7), pp. 38–40. Available at: https://doi.org/10.1145/2209249.2209263.

State of Callifornia Department of Justice; Office of the Attorney General (2021) *California Consumer Privacy Act (CCPA), Website*. Available at: https://www.oag.ca.gov/privacy/ccpa (Accessed: 25 August 2021).

The Open Data Institute (2018) ‘ODI survey reveals British consumer attitudes to sharing personal data’, *Website* [Preprint]. Available at: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/.

Utz, C. *et al.* (2019) ‘(Un)informed Consent: Studying GDPR consent notices in the field’, *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 973–990. Available at: https://doi.org/10.1145/3319535.3354212.

White, R. and Gunstone, R. (2014) *Probing Understanding*, *Journal of Chemical Information and Modeling*. Available at: https://doi.org/10.1017/CBO9781107415324.004.

Wicker, S.B. and Schrader, D.E. (2011) ‘Privacy-aware design principles for information networks’, *Proceedings of the IEEE*, 99(2), pp. 330–350. Available at: https://doi.org/10.1109/JPROC.2010.2073670.

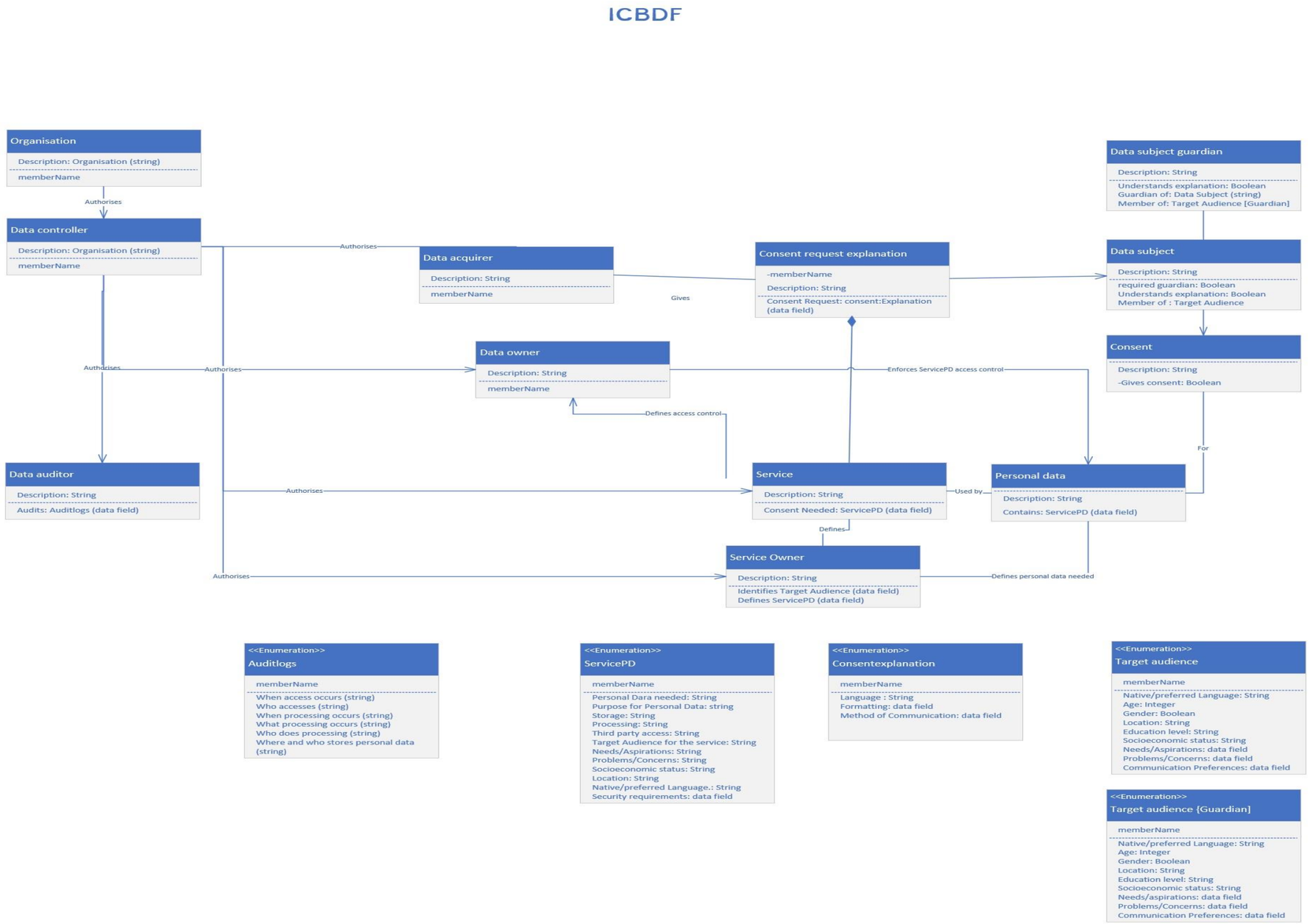
Wiggins, G. and McTighe, J. (2005) *Understanding by Design*, *Association for Supervision and Curriculum Development*.

Wong, J.C. (2019) ‘The Cambridge Analytica scandal changed the world – but it didn’t change Facebook’, *The Guardian* [Preprint]. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

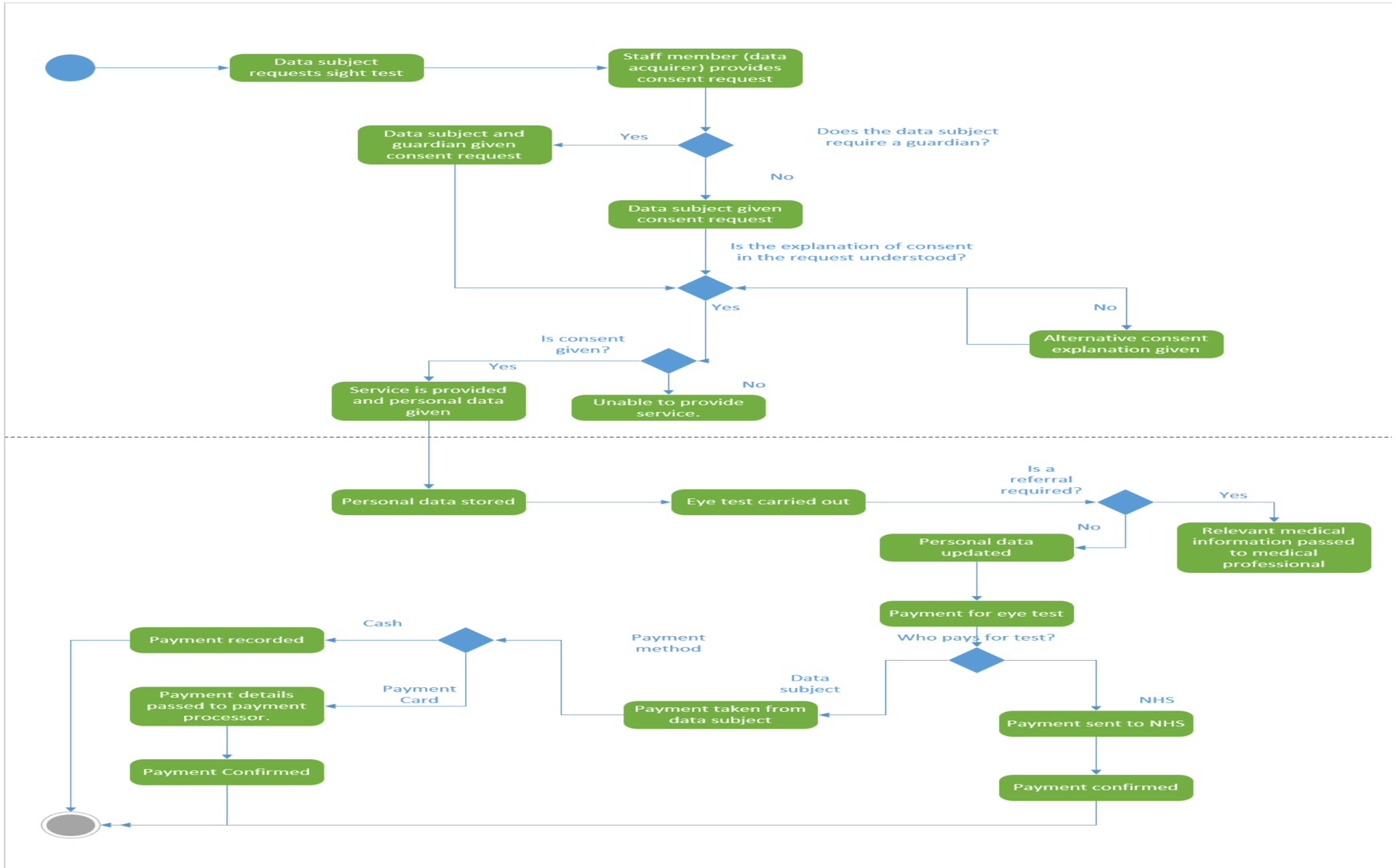
Wuyts, K., Scandariato, R. and Joosen, W. (2014) ‘Empirical evaluation of a privacy-focused threat modeling methodology’, *Journal of Systems and Software*, 96, pp. 122–138. Available at: https://doi.org/10.1016/j.jss.2014.05.075.

Zarrabi, F. *et al.* (2012) ‘A Meta-model for Legal Compliance and Trustworthiness of Information Systems’, *CAiSE 2012 Workshops LNBIP*, (112), pp. 46–60.

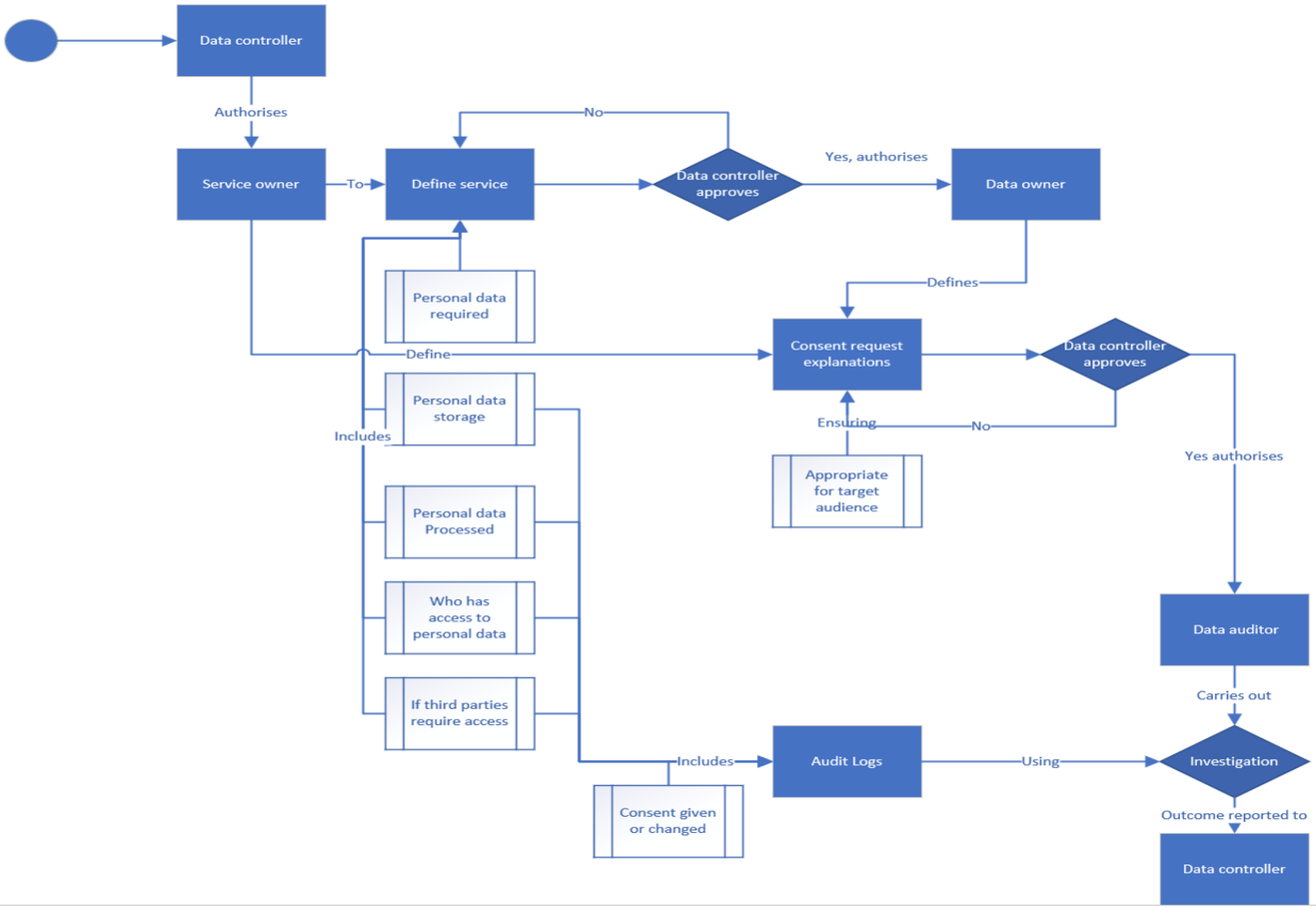
Appendix A: ICBDF



Appendix B Activity Diagram When a Customer Visits an Opticians.



Appendix C: Use of the ICBDF when creating a new service.



Page left intentionally blank to preserve formatting

Appendix D: Additional case study.

The following example is based on the framework presented in "An agent-based framework for Informed Consent in the Internet of Things" (Neisse et al., 2015)

Using this framework, a system of Internet of Things (IoT) has been installed across a smart city. This can monitor data such as how busy the roads are, or for targeting adverts. Smart meters installed in homes to help monitor energy consumption of a household. Environmental sensors would monitor various environmental variabilities e.g. temperature, to help ensure that heating is used when it is needed. Residents may also wear smart devices that can monitor their health conditions.

The system would be able to analyse data about the residents, for example the preference of temperature when at work, or lifestyle choices from the data collected by the IoT sensors. This would mean that when a resident visits a public place, such as a shopping centre, the system would be able to alert the resident with specific offers, and also alert them should there be a change in the environment, for example a sudden change of weather.

A number of organisations that could use the IoT system. Examples would include:

- The emergency services using the system so that they can avoid heavy traffic when responding to an emergency.
- Health providers, using the data gathered from wearable IoT devices to be able monitor the health of their patients.
- Advertisers use the data collected to be able deliver adverts relevant to the residents depending on the situation.
- Local government using the data to be able to make better decisions when planning infrastructure developments.

The "An agent-based framework for Informed Consent in the Internet of Things" framework provides a privacy preserving authentication method, where the system

controllers make digital identities for each citizen. For example a company will generate a digital identity for each of its employees. This way only the issuer of the identity knows who the digital identity is.

This framework also uses “informed consent policy rules”, which allows residents to specify what they consent to, and this is enforced by an Event – Condition – Action structure. This structure activates when an Event occurs. The Condition of the Event is applied, such as when a resident comes home (event) at lunchtime on a hot day (condition) then an Action trigger (such as turning on the air conditioning).

The framework also employs a User Centric Policy Manager, which the resident can store the permissions they choose into. Using this, the IoT devices can recognise what information they can and cannot collect about the residents within the area. For example if resident A goes to a shopping centre, the IoT devices in the shopping centre can apply resident A’s permissions to the data that they collect about them. This allows for the IoT system to be able to apply specific rules to each resident that that are collecting data about.

While the “An agent-based framework for Informed Consent in the Internet of Things” framework does all of this, it does not however consider if the “informed consent” that it tracks is actually “informed”. It does not have a method of giving the resident an explanation as to what data they are collecting, who can access it and how it is going to be used for.

If the ICBDF was used in this case study, at the point where the resident is being asked to give their consent, they would be provided with a Consent Request Explanation. This would be written by the organisation that is wanting to use the resident’s data (e.g. the local government, an employer, owner of a shopping centre). This explanation should be provided in a format that is accessible by the resident (e.g. digitally, printed etc) and should be written in a style that is understandable by the resident. Avoiding technical or legal jargon, and with clear explanations.

The resident should also know who is going to have access to their information and if an organization is going to share it with anyone for any reason. The resident should also be able to contact the organisation to be able to assert their rights under the Data Protection Act, such as being able to see the data that is held on them, or changing their consent. As each organisation is giving the resident a Consent Request

Explanation, it should be clear as to which organisation is requesting the residents consent.

The Consent Request Explanation should also state in what cases they would provide personal data to the emergency services. For example if the resident has consented to the processing of their health data, it should be made clear that emergency services will be given data should it be detected that the resident is having a medical emergency (e.g. heart attack).

From the above we have demonstrated that in the case of "An agent-based framework for Informed Consent in the Internet of Things" provides a good framework. However with the addition of using the ICBDF it is able to improve the way that it gains the informed consent of the residents. In doing so it also provides the residents a record of who has asked them for their consent, and the ability for them to be able to contact the organisations that have their data if they want to change their consent.

Bibliography

Aboud, S.J., Al Fayoumi, M. and Alnuaimi, M. (2009) 'Verification and validation of simulation models', *Handbook of Research on Discrete Event Simulation Environments: Technologies and Applications*, pp. 58–74. Available at: https://doi.org/10.4018/978-1-60566-774-4.ch004.

Act, S.O., Victims, T. and Context, C. (2003) 'What is consent ? Key issues for investigators and prosecutors'.

Ade Bilau, A., Witt, E. and Lill, I. (2018) 'Research methodology for the development of a framework for managing post-disaster housing reconstruction', *Procedia Engineering*, 212(2017), pp. 598–605. Available at: https://doi.org/10.1016/j.proeng.2018.01.077.

Agre, P. and Rapkin, B. (2019) 'Improving Informed Consent: A Comparison of Four Consent Tools', *IRB: Ethics and Human Research*, 25(6), pp. 1–7. Available at: https://doi.org/10.1007/978-1-349-95810-8_562.

Ahmadian, A.S. *et al.* (2018) 'Supporting Privacy Impact Assessment by Model-Based Privacy Analysis', *Proceedings of the ACM Symposium on Applied Computing*, pp. 1467–1474. Available at: https://doi.org/10.1145/3167132.3167288.

Alaboodi, S.S. (2013) 'Model-based Evaluation : from Dependability Theory to Security', 1(1), pp. 48–65. Available at: https://doi.org/10.1109/TDSC.2004.11.

Albrecht, J.P.P.P. (2016) 'How the GDPR Will Change the World', *European Data Protection Law Review*, 2(3), pp. 287–289. Available at: https://doi.org/10.21552/EDPL/2016/3/4.

Alhogail, A. (2015) 'Design and validation of information security culture framework', *Computers in Human Behavior*, 49, pp. 567–575. Available at: https://doi.org/10.1016/j.chb.2015.03.054.

Alismaili, S. *et al.* (2015) 'A multi perspective approach for understanding the determinants of cloud computing adoption among Australian SMEs', *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems* [Preprint].

ALKUBAISY, D. *et al.* (2021) 'ConfIs: a tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design', in *Proceedings of 16th Evaluation of novel approaches to software engineering international conference 2021 (ENASE 2021)*. SCITEPRESS - Science and Technology Publications, pp. 80–91. Available at: https://doi.org/10.5220/0010406100800091.

Allen, D.W.E. *et al.* (no date) 'Volume 39 , Issue 2 Some economic consequences of the GDPR', 39(2), pp. 785–797.

Allison, P.R. (2019) 'Data protection: How privacy can be a benefit, not a burden', *Computer Weekly* [Preprint]. Available at: https://www.computerweekly.com/feature/Data-protection-How-privacy-can-be-a-benefit-not-a-burden.

Almeida Teixeira, G., Mira da Silva, M. and Pereira, R. (2019) 'The critical success factors of GDPR implementation: a systematic literature review', *Digital Policy, Regulation and Governance* . Emerald Group Holdings Ltd., pp. 402–418. Available at:

https://doi.org/10.1108/DPRG-01-2019-0007.

Alnemr, R. *et al.* (2015) *A Data Protection Impact Assesment Methodology for Cloud*.

Alnemr, R. *et al.* (2016) 'A data protection impact assessment methodology for cloud', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9484, pp. 60–92. Available at: https://doi.org/10.1007/978-3-319-31456-3_4.

Alshammari, M. and Simpson, A. (2018a) 'Privacy architectural strategies: An approach for achieving various levels of privacy protection', in *Proceedings of the ACM Conference on Computer and Communications Security*. Association for Computing Machinery, pp. 143–154. Available at: https://doi.org/10.1145/3267323.3268957.

Alshammari, M. and Simpson, A. (2018b) 'Privacy Architectural Strategies', pp. 143–154. Available at: https://doi.org/10.1145/3267323.3268957.

Amis, F. (1978) 'Relational understanding and instrumental understanding', *The Arithmetic Teacher*, pp. 20–26. Available at: http://eledu.net/rrcusrn_data/Skemp article.pdf.

'AN202109September2021.pdf' (no date).

Anikeev, M., Shulman, H. and Simo, H. (2021) 'Privacy Policies of Mobile Apps - A Usability Study', in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, pp. 1–2. Available at: https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484434.

Annas, G.J. (2017) 'Informed consent: Charade or choice?', *Journal of Law, Medicine and Ethics*, 45(1), pp. 10–11. Available at: https://doi.org/10.1177/1073110517703096.

Antkiewicz, M. (2008) 'Framework-specific modeling languages | Generative Software Development Lab'. Available at: http://gsd.uwaterloo.ca/node/97.

Antkiewicz, M.L. (no date) *Framework-Specific Modeling Languages*.

Argyropoulos, N. *et al.* (2016) 'Incorporating Privacy Patterns into Semi-Automatic Business Process Derivation', *2016 Ieee Tenth International Conference on Research Challenges in Information Science*, 2016-Augus, pp. 529–540. Available at: https://doi.org/10.1109/RCIS.2016.7549305.

Argyropoulos, N. *et al.* (2017) 'A Semi-Automatic Approach for Eliciting Cloud Security and Privacy Requirements', *HICSS-50 2017 Hawaii International Conference on System Sciences*, pp. 4827–4836. Available at: https://doi.org/10.24251/hicss.2017.587.

Arnott, D., Lizama, F. and Song, Y. (2017) 'Patterns of business intelligence systems use in organizations', *Decision Support Systems*, 97, pp. 58–68. Available at: https://doi.org/10.1016/j.dss.2017.03.005.

Article 29 Data Protection Working Party and Party, A. 29 D.P.W. (2017) 'Wp29 Guidelines on Consent', *Ssrn*, pp. 1–31.

Article 29 Working Group and Group, A. 29 W. (2017) *Guidelines on consent under Regulation 2016/679, 17/EN WP259, SSRN*. Available at: https://doi.org/10.2139/ssrn.2972855.

Ashraf, S. (2021) 'GDPR Implementation Framework for SMEs', (March).

Ashurst (2021) *China's new data privacy law - what does it mean for you?, Website*.

Available at: https://www.ashurst.com/en/news-and-insights/legal-updates/chinas-new-data-privacy-law-what-does-it-mean-for-you (Accessed: 21 January 2022).

Badillo-Urquiola, K. *et al.* (2018) 'Privacy in context: Critically engaging with theory to guide privacy research and design', *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, pp. 425–431. Available at: https://doi.org/10.1145/3272973.3273012.

Baloyi, N. and Kotzé, P. (2019) 'Guidelines for data privacy compliance: A focus on cyber-physical systems and internet of things', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3351108.3351143.

Barnes-Holmes, D. and Hussey, I. (2016) 'The functional-cognitive meta-theoretical framework: Reflections, possible clarifications and how to move forward', *International Journal of Psychology*, 51(1), pp. 50–57. Available at: https://doi.org/10.1002/ijop.12166.

Baron, J. (2018) 'Forms of explanation and why they may matter', *Cognitive Research: Principles and Implications*, 2(1). Available at: https://doi.org/10.1186/s41235-018-0143-2.

Bartolini, C., Calabró, A. and Marchetti, E. (2019) 'GDPR and business processes: An effective solution', in *ACM International Conference Proceeding Series*. Association for Computing Machinery. Available at: https://doi.org/10.1145/3309772.3309779.

Bau, Jason; Mitchell, J.C. *et al.* (2011) 'Security Modeling and Analysis with UMLsec(ppt)', *IEEE Security and Privacy*, 9(June), pp. 18–25. Available at: https://doi.org/10.1109/MSP.2011.2.

Bauer, J. (2013) 'Význam průkazu RAS mutací pro anti-EGFR protilátky v léčbě 1. linie metastazujícího kolorektálního karcinomu', *Onkologie (Switzerland)*, 7(5), pp. 260–261.

Bayarri, M.J. *et al.* (2007) 'A framework for validation of computer models', *Technometrics*, 49(2), pp. 138–154. Available at: https://doi.org/10.1198/004017007000000092.

BBC (2019) *Amazon, Apple and Google face data complaints*. Available at: https://www.bbc.co.uk/news/technology-46944694.

BBC (2020a) 'Brighton University students' belongings binned by halls', *BBC Website* [Preprint]. Available at: https://www.bbc.co.uk/news/uk-england-sussex-53860029.

BBC (2020b) 'Grandmother ordered to delete Facebook photos under GDPR', *Website* [Preprint]. Available at: https://www.bbc.co.uk/news/technology-52758787.

BBC (2021) *Amazon hit with $886m fine for alleged data law breach, Website*. Available at: https://www.bbc.co.uk/news/business-58024116 (Accessed: 31 August 2021).

Beckett, P. (2017) 'GDPR compliance: your tech department's next big opportunity', *Computer Fraud and Security*, 2017(5), pp. 9–13. Available at: https://doi.org/10.1016/S1361-3723(17)30041-6.

Bialke, M. *et al.* (2018) 'MAGIC: Once upon a time in consent management - A FHIR®tale', *Journal of Translational Medicine*, 16(1), pp. 1–12. Available at: https://doi.org/10.1186/s12967-018-1631-3.

Bitto, A. *et al.* (2019) 'ePub WU Institutional Repository framework', *Journal of Systems and Software*, (September), p. 85. Available at: https://www.sciencedirect.com/science/article/pii/S0164121212000040.

Black, V. and Hadskis, M. (2015) ‘INFORMED CONSENT COMES TO BRITAIN Thejudgment earlier this year of the Supreme Court of the United Kingdom in Montgomery v . Lanarkshire Health Board ’ has been described by British commentators as a " landmark decision " 2 and " the most important clinic’, *The Advocates’ Quarterly*, 44(4), pp. 403–410.

Blackmer, W.S. (2018) ‘EU general data protection regulation’, *American Fuel and Petrochemical Manufacturers, AFPM - Labor Relations/Human Resources Conference 2018*, 2014(October 1995), pp. 45–62. Available at: https://doi.org/10.1308/rcsfdj.2018.54.

Blix, F., Addin Elshekeil, S. and Laoyookhong, S. (no date) *Data Protection by Design in Systems Development From legal requirements to technical solutions*.

Blix, F., Elshekeil, S.A. and Laoyookhong, S. (2017) ‘Data Protection by Design in Systems Development’, *12th International Conference for Internet Technology and Secured Transactions (ICITST-2017)*, pp. 98–103.

Bock, K. *et al.* (2020) ‘Data Protection Impact Assessment for the Corona App’, *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.3588172.

Bothun, L.S., Feeder, S.E. and Poland, G.A. (2021) ‘Poor Readability of COVID-19 Vaccine Information for the General Public: A Lost Opportunity’, *medRxiv*, 6(51809007), p. 2021.06.11.21258778. Available at: https://doi.org/10.1101/2021.06.11.21258778.

Bouabidi, A. *et al.* (2010) ‘Critical analysis of several analytical method validation strategies in the framework of the fit for purpose concept’, *Journal of Chromatography A*, 1217(19), pp. 3180–3192. Available at: https://doi.org/10.1016/j.chroma.2009.08.051.

Bourdiew, P., Bourdieu, P. and Bourdiew, P. (1996) ‘Understanding’, *Theory, Culture & Society*, 13(2), pp. 17–37.

Brahmachary, A. (2019) *ITIL Roles and Responsibilities – Process Wise | ITSM Roles, Certguidance website*. Available at: https://www.certguidance.com/processes-wise-itil-roles-itsm/ (Accessed: 13 July 2021).

Brambilla, M. *et al.* (2012) *Teaching material for the book Model-Driven Software Engineering in Practice Chapter 7*. Available at: www.mdse-book.com.

Breese, P.E. *et al.* (2007) ‘Education Level, Primary Language, and Comprehension of the Informed Consent Process’, *Journal of Empirical Research on Human Research Ethics*, 2(4), pp. 69–79. Available at: https://doi.org/10.1525/jer.2007.2.4.69.

Brief, I.N. (2017a) ‘In the first of a series of articles, Rollits LLP provides an essential overview of the General Data Protection Regulation’, (September), pp. 8–9.

Brief, I.N. (2017b) ‘Mind the GDPR (Pt 2)’, (December), pp. 11–12.

vom Brocke, J. *et al.* (2015) ‘Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research’, *Communications of the Association for Information Systems*, 37(August), pp. 205–224. Available at: https://doi.org/10.17705/1CAIS.03709.

vom Brocke, J., Hevner, A. and Maedche, A. (2020) ‘Introduction to Design Science Research’, (November), pp. 1–13. Available at: https://doi.org/10.1007/978-3-030-46781-4_1.

Brophy, S., Snooks, H. and Griffiths, L. (2011) ‘Searching and Reviewing the Literature’, in *Small-Scale Evaluation in Health*, pp. 12–23. Available at:

https://doi.org/10.4135/9781849209892.n2.

Bu-Pasha, S. *et al.* (2016) 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency', *European Data Protection Law Review*, 1(3), pp. 312–323. Available at: https://doi.org/10.1016/j.clsr.2017.05.015.

Bu-Pasha, S. *et al.* (2017) 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency', *European Data Protection Law Review*, 2(3), pp. 312–323. Available at: https://doi.org/10.21552/edpl/2016/3/7.

Bu-Pasha, S. (2020) 'The controller's role in determining "high risk" and data protection impact assessment (DPIA) in developing digital smart city', *Information and Communications Technology Law*, pp. 1–12. Available at: https://doi.org/10.1080/13600834.2020.1790092.

Budin-Ljøsne, I. *et al.* (2017) 'Dynamic Consent: A potential solution to some of the challenges of modern biomedical research', *BMC Medical Ethics*, 18(1), pp. 1–10. Available at: https://doi.org/10.1186/s12910-016-0162-9.

Butterworth, M. (2018) 'The ICO and artificial intelligence: The role of fairness in the GDPR framework', *Computer Law and Security Review*, 34(2), pp. 257–268. Available at: https://doi.org/10.1016/j.clsr.2018.01.004.

Button, D.R. and Fox, J. (2003) 'The syntax and semantics of the PRO forma guideline modeling language', *Journal of the American Medical Informatics Association*, 10(5), pp. 433–443. Available at: https://doi.org/10.1197/jamia.M1264.

Calabrò, A. *et al.* (2019) 'A dynamic and scalable solution for improving daily life safety', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3309772.3309796.

Cambridge English Dictionary (2022) *TARGET AUDIENCE, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/target-audience (Accessed: 9 January 2022).

Cambridge English Dictionary (no date a) *Defines Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/define?q=Define (Accessed: 14 July 2021).

Cambridge English Dictionary (no date b) *Gain Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/gain?q=Gain (Accessed: 14 July 2021).

Cambridge English Dictionary (no date c) *SERVICE meaning in the Cambridge English Dictionary., Online*. Available at: https://dictionary.cambridge.org/dictionary/english/require (Accessed: 9 July 2021).

Cambridge English Dictionary (no date d) *Use Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/use.

Cambridge English Dictionary and Dictionary, C.E. (no date a) *Defines Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/define?q=Define (Accessed: 14 July 2021).

Cambridge English Dictionary and Dictionary, C.E. (no date b) *Gain Cambridge English Dictionary, Website*. Available at:

https://dictionary.cambridge.org/dictionary/english/gain?q=Gain (Accessed: 14 July 2021).

Cambridge English Dictionary and Dictionary, C.E. (no date c) *Use Cambridge English Dictionary, Website*. Available at: https://dictionary.cambridge.org/dictionary/english/use.

Cambridge English Dictionary, Dictionary, C.E. and Cambridge English Dictionary (no date) *SERVICE meaning in the Cambridge English Dictionary., Online*. Available at: https://dictionary.cambridge.org/dictionary/english/require (Accessed: 9 July 2021).

Cane, J., O'Connor, D. and Michie, S. (2012) 'Validation of the theoretical framework', *Implementation Science*, 7, p. 37.

Carvalho, A.C., Martins, R. and Antunes, L.L.L. (2018) 'How-to Express Explicit and Auditable Consent', in *16th Anual Conference on Privacy, Security and Trust (PST)*, pp. 1–5. Available at: https://doi.org/10.1109/PST.2018.8514204.

de Carvalho, R.M. *et al.* (2020) 'Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects', *SN Computer Science*, 1(4), pp. 1–16. Available at: https://doi.org/10.1007/s42979-020-00218-8.

Cavoukian, A. (2009) 'Privacy by Design - The 7 foundational principles - Implementation and mapping of fair information practices', *Information and Privacy Commissioner of Ontario, Canada*, p. 5. Available at: https://doi.org/10.1007/s12394-010-0062-y.

Cavoukian, A. (2012) *Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices*. 1st edn. Information and Privacy Commissioner, Ontario, Canada.

Cavoukian, A. and Jonas, J. (2012) 'Privacy by Design in the Age of Big Data', *Information and Privacy Commisioner*, (June), pp. 1–17. Available at: https://doi.org/10.1126/science.aaa5945.

Celik, D. (2021) 'Sociomaterial perspective of learning design practice and Its implications on learning design software de- velopment'.

Centre, B. (no date) 'Planning a Seminar'.

Channel 4 news (2018) 'Data, Democracy and Dirty Tricks – Channel 4 News.', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Channel 4 news (2020) '"Are people going to be excluded from workplace if they don't go with contact tracing app?" - Newcastle University's Lilian Edwards', *Online* [Preprint]. Available at: https://www.channel4.com/news/are-people-going-to-be-excluded-from-workplace-if-they-dont-go-with-contact-tracing-app-newcastle-universitys-lilian-edwards.

Channel 4 news and news, C. 4 (2020) '"Are people going to be excluded from workplace if they don't go with contact tracing app?" - Newcastle University's Lilian Edwards', *Online* [Preprint]. Available at: https://www.channel4.com/news/are-people-going-to-be-excluded-from-workplace-if-they-dont-go-with-contact-tracing-app-newcastle-universitys-lilian-edwards.

Channel 4 news, news, C. 4 and Channel 4 news (2018) 'Data, Democracy and Dirty Tricks – Channel 4 News.', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Chatzipoulidis, A.A., Tsiakis, T.T. and Kargidis, T. (2019) 'A readiness assessment tool

for GDPR compliance certification', *Computer Fraud and Security*, 2019(August 2019), pp. 14–19. Available at: https://doi.org/10.1016/S1361-3723(19)30086-7.

CMS Law (no date a) *GDPR Enforcement Tracker, Website*.

CMS Law (no date b) *GDPR Enforcement Tracker, Website*. Available at: view-source:https://www.enforcementtracker.com/ (Accessed: 3 July 2022).

CNIL (2018a) *PIA: Knowledge Bases, CNIL*.

CNIL (2018b) *PIA Manual, CNIL*.

CNIL (2018c) 'Privacy Impact Assessment Templates', p. 26. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf.

CNIL (2019a) 'Privacy Impact Assessment - Methodology', *Commision Nationale Informatique & Libertés*, p. 400. Available at: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual.

CNIL (2019b) *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, Online*. Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

Cocanour, C.S. (2017) 'Informed consent—It's more than a signature on a piece of paper', *American Journal of Surgery*, 214(6), pp. 993–997. Available at: https://doi.org/10.1016/j.amjsurg.2017.09.015.

Cohen, J.E. (2003) 'DRM and privacy', *Berkeley Technology Law Journal*, 18(4), pp. 575–617. Available at: https://doi.org/10.1145/641205.641230.

Cohen, M. and Mcallister, A. (2018) 'Ready for GDPR?', (August), pp. 60–62.

Coiera, E. and Clarke, R. (2004) 'e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Enviroment', *Journal of the American Medical Informatics Association*, 11(2), pp. 129–140. Available at: https://doi.org/10.1197/jamia.M1480.Affiliations.

Colesky, M. *et al.* (2018) 'A System of Privacy Patterns for User Control', *33rd Symposium on Applied Computing*, pp. 1150–1156. Available at: https://doi.org/10.1145/3167132.3167257.

Colesky, M. and Caiza, J.C. (2018) 'A system of privacy patterns for informing users: Creating a pattern system', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3282308.3282325.

Colesky, M., Hoepman, J.H. and Hillen, C. (2016) 'A Critical Analysis of Privacy Design Strategies', *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, pp. 33–40. Available at: https://doi.org/10.1109/SPW.2016.23.

Commissioners, D.P. and P. and Data Protection and Privacy Commissioners (2010) 'Resolution on Privacy by Design', *Icdppc*, pp. 1–2.

Connor, Y.O. *et al.* (2017) 'ScienceDirect ScienceDirect Privacy by Design : Informed Consent and Internet of Things for Privacy by Design : Informed Consent Smart Health and Internet of Things for Smart Health', *Procedia Computer Science*, 113, pp. 653–658. Available at: https://doi.org/10.1016/j.procs.2017.08.329.

Cook, D.A. and Skinner, J.M. (2005) 'How to perform credible verification, validation, and accreditation for modeling and simulation', *CrossTalk*, (5), pp. 20–23.

Crespo, B.G. and Wells, J. (2020) ‘GDPR G UIDELINES AND R EQUIREMENTS’, (787068).

Cronin, M. (2009) ‘10 Principles Of Readability And Web Typography’, *Website* [Preprint]. Available at: https://www.smashingmagazine.com/2009/03/10-principles-for-readable-web-typography/.

Crown Prosecution Service and Service, C.P. (2013) ‘What is consent? Key issues for investigators and prosecutors’.

Custers, B. *et al.* (2018) ‘A comparison of data protection legislation and policies across the EU’, *Computer Law and Security Review*, 34(2), pp. 234–243. Available at: https://doi.org/10.1016/j.clsr.2017.09.001.

Cutler, S. (2018) ‘The Face-Off Between Data Privacy and Discovery : Why U . S . Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information’, *Boston College Law Review. Boston College. Law School*, 59(4), p. 1513.

Cvik, E.D., Pelikánová, R.M.G. and Malý, M. (2018) ‘Selected Issues from the Dark Side of the General Data Protection Regulation’, *Review of Economic Perspectives*, 18(4), pp. 387–407. Available at: https://doi.org/10.2478/revecp-2018-0020.

Datoo, A. (2018) ‘Data in the post-GDPR world’, *Computer Fraud and Security*, 2018(9), pp. 17–18. Available at: https://doi.org/10.1016/S1361-3723(18)30088-5.

Davies, N. and Langheinrich, M. (2013) ‘Privacy by design’, *IEEE Pervasive Computing*, 12(2), pp. 2–4. Available at: https://doi.org/10.1109/MPRV.2013.34.

Davies, N., Langheinrich, M. and Davies, N. (2013) ‘Privacy By Design [From the Editor in Chief]’, *IEEE Pervasive Computing*, 12, pp. 2–4. Available at: https://doi.org/10.1109/MPRV.2013.34.

Davis, V., And, H. and Heath, J. (1999) ‘The Good, the Bad, and the Ugly’, *Arion: A Journal of Humanities and the Classics*, 6(3), pp. 150–195. Available at: https://doi.org/10.1007/978-981-10-3473-2_11.

Debruyne, C. *et al.* (2020) ‘“Just-in-time” generation of datasets by considering structured representations of given consent for GDPR compliance’, *Knowledge and Information Systems*, 62(9), pp. 3615–3640. Available at: https://doi.org/10.1007/s10115-020-01468-x.

Debussche, J. and Cesar, J. (2018) *GDPR GUIDELINES AND REQUIREMENTS*.

DEFeND (2019) *DEFeND Consolidated Requirements new*.

Degeling, M. *et al.* (2018) ‘We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy’, *arXiv*, (February), pp. 1–15. Available at: https://doi.org/10.14722/ndss.2019.23378.

Degeling, M. *et al.* (2019) ‘We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy’, in. Internet Society. Available at: https://doi.org/10.14722/ndss.2019.23378.

Delany, C. (2008) ‘Making a difference : incorporating theories of autonomy into models of informed consent’, *Journal of Medical Ethics*, 34(9), pp. 1–5. Available at: https://doi.org/10.1136/jme.2007.023804.

Dewalt, C. (1999) *BUSINESS PROCESS MODELING WITH UML*.

Dewitte, P. *et al.* (2019) ‘A comparison of system description models for data protection

by design', *Proceedings of the ACM Symposium on Applied Computing*, Part F1477(i), pp. 1512–1515. Available at: https://doi.org/10.1145/3297280.3297595.

Diamantopoulou, V. *et al.* (2017) 'A metamodel for GDPR-based privacy level agreements', *CEUR Workshop Proceedings*, 1979(112), pp. 299–305.

Diamantopoulou, V., Pavlidis, M. and Mouratidis, H. (2017) 'Privacy level agreements for public administration information systems', *CEUR Workshop Proceedings*, 1848, pp. 97–104.

DiFonzo, N. and Bordia, P. (1998) 'Reproduced with permission of the copyright owner . Further reproduction prohibited without', *Journal of Allergy and Clinical Immunology*, 130(2), p. 556. Available at: http://dx.doi.org/10.1016/j.jaci.2012.05.050.

Dobing, B. and Parsons, J. (2006) 'How UML is used', *Communications of the ACM*, pp. 109–113. Available at: https://doi.org/10.1145/1125944.1125949.

DuBay, W.H. (2004) 'The principles of readability: A brief introduction to readability research', *Impact Information*, (949), pp. 1–72. Available at: https://doi.org/10.1.1.91.4042.

Duncan, B. and Whittington, M. (2015) 'Enhancing cloud security and privacy: Broadening the service level agreement', *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 1(1), pp. 1088–1093. Available at: https://doi.org/10.1109/Trustcom.2015.487.

Duncan, G. (2007) 'Engineering: Privacy by design', *Science*, 317(5842), pp. 1178–1179. Available at: https://doi.org/10.1126/science.1143464.

Dutta, Probal and Bose, S. and Dutta Sudipta, P. and B. (2011) 'Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations', *Economic Policy*, (2116), pp. 0–33.

Dworkin, G. (1976) 'Autonomy and Behavior Control', *The Hastings Center Report*, 6(1), pp. 23–28. Available at: https://doi.org/10.5860/choice.43-2236.

Edwards, L. (2017) 'Privacy, Security and Data Protection in Smart Cities':, *European Data Protection Law Review*, 2(1), pp. 28–58. Available at: https://doi.org/10.21552/edpl/2016/1/6.

Edwards, L. and Veale, M. (2018) 'Enslaving the algorithm: From a "right to an explanation" to a "right to better decisions"?', *arXiv*, (January), pp. 1–15.

El-Dairi, M. and House, R.J. (2019) 'Optic nerve hypoplasia', in *Handbook of Pediatric Retinal OCT and the Eye-Brain Connection*, pp. 285–287. Available at: https://doi.org/10.1016/B978-0-323-60984-5.00062-7.

Eleyan, D., Othman, A. and Eleyan, A. (2020) 'Enhancing software comments readability using flesch reading ease score', *Information (Switzerland)*, 11(9). Available at: https://doi.org/10.3390/INFO11090430.

Emanuel, E.J. and Boyle, C.W. (2021) 'Assessment of Length and Readability of Informed Consent Documents for COVID-19 Vaccine Trials', *JAMA Network Open*, 4(4), pp. 4–8. Available at: https://doi.org/10.1001/jamanetworkopen.2021.10843.

Eriksson, H.-E., Penker, M. and Training Hans-Erik, O. (no date) *Business Modeling with UML*.

European Commission (2011) ‘Privacy and Data Protection Impact Assessment Framework for RFID Applications’, (January), pp. 1–24.

European Commission (2018) *Regulation (EU) 2016/679*.

European Commission and Commission, E. (2011) ‘Privacy and Data Protection Impact Assessment Framework for RFID Applications’, (January), pp. 1–24.

European Parliament (2016) ‘General Data Protection Regulations’, *Official journal of the European Union* [Preprint]. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

European Union (2016) ‘Regulation 2016/679’, *Official Journal of the European Communities*, 2014(March 2014), pp. 1–88. Available at: https://doi.org/http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf.

Euzenat, J. *et al.* (2013) *Ontology Alignment Evaluation Initiative : six years of experience Cassia Trojahn dos Santos To cite this version : HAL Id : hal-00781141 Ontology Alignment Evaluation Initiative : six years of experience*.

Fatema, K. *et al.* (2017) ‘Compliance through informed consent: Semantic based consent permission and data management model’, *CEUR Workshop Proceedings*, 1951.

Fenton, S.H. *et al.* (2015) ‘Informed consent: Does anyone really understand what is contained in the medical record?’, *Applied Clinical Informatics*, 6(3), pp. 466–477. Available at: https://doi.org/10.4338/ACI-2014-09-SOA-0081.

Fischer, A.E. *et al.* (2021) ‘The readability of informed consent forms for research studies conducted in South Africa’, *South African Medical Journal*, 111(2), pp. 180–183. Available at: https://doi.org/10.7196/SAMJ.2021.V111I2.14752.

Flint, D. (2009) ‘Law shaping technology: Technology shaping the law’, *International Review of Law, Computers and Technology*, 23(1–2), pp. 5–11. Available at: https://doi.org/10.1080/13600860902742505.

Fowler, M. (2003) *UML Distilled: A Brief Guide to the Standard Object Modeling Language*. Third. ADDISON WESLEY.

Fowler, M. and Scott, K. (1997) *UML Distilled*.

Frank, Richard, B. and Frank B, R. (1999) *Downfall: the End of the Imperial Japanese Empire*. New York: Penguin.

Friedman, B., Felten, E. and Millett, L.I. (2000) ‘Informed Consent Online’, *DisClosure*, pp. 1–8.

Garber, J. (2018a) *GDPR-compliance nightmare or business opportunity?* Available at: http://www.londonchamber.co.uk/news/.

Garber, J. (2018b) ‘GDPR – compliance nightmare or business opportunity?’, *Computer Fraud and Security*, 2018(6), pp. 14–15. Available at: https://doi.org/10.1016/S1361-3723(18)30055-1.

Garfield, J. (2014) ‘Reductio ad absurdum: informed consent’, *The Medico-legal journal*, 82(1), pp. 38–40. Available at: https://doi.org/10.1177/0025817213513699.

Geest, T. Van Der, Pieterson, W. and Vries, P. De (2005) ‘Informed consent to address trust, control, and privacy concerns in user profiling’, *Privacy Enhanced …*, pp. 1–10. Available at: http://www.utwente.nl/ctit/cfes/docs/EN_artikelen/2005-

Informed_Consent.pdf.

Geidel, L., Bahls, T. and Hoffmann, W. (2014) *May I? - Challenges to a generic, automated electronic administration of consent, GMDS 2014. 59th Annual Meeting of the German Society for Medical Informatics, Biometry and Epidemiology (GMDS)*. 4 September 2014. Available at: https://www.egms.de/static/en/meetings/gmds2014/14gmds131.shtml.

Geier, C. *et al.* (2021) 'Informed Consent for Online Research—Is Anybody Reading?: Assessing Comprehension and Individual Differences in Readings of Digital Consent Forms', *Journal of Empirical Research on Human Research Ethics* [Preprint]. Available at: https://doi.org/10.1177/15562646211020160.

Gellert, R. (2018) 'Understanding the notion of risk in the General Data Protection Regulation', *Computer Law and Security Review*, 34(2), pp. 279–288. Available at: https://doi.org/10.1016/j.clsr.2017.12.003.

Genestier, J.O.T.I.S.F.T.A.. (2017) 'BLOCKCHAIN FOR CONSENT MANAGEMENT IN THE EHEALTH ENVIRONMENT: A NUGGET FOR PRIVACY AND SECURITY CHALLENGES Introduction and Use Case', *J Int Soc Telemed eHealth*, 5, pp. 24–25.

Genestier, J.O.T.I.S.F.T.A.. J.O.T.I.S.F.T.A.E. *et al.* (2017) 'BLOCKCHAIN FOR CONSENT MANAGEMENT IN THE EHEALTH ENVIRONMENT: A NUGGET FOR PRIVACY AND SECURITY CHALLENGES Introduction and Use Case', *J Int Soc Telemed eHealth*, 5, pp. 24–25.

Génova, G. (2009) 'What is a model: syntax and semantics', *Modeling and metamodeling in Model Driven Development* [Preprint]. Available at: http://www.kr.inf.uc3m.es/ggenova/.

Génova, G. (no date) *Modeling and metamodeling in Model Driven Development What is a model: syntax and semantics Structure of the seminar*. Available at: http://www.kr.inf.uc3m.es/ggenova/.

Gilda, S. and Mehrotra, M. (2018) 'Blockchain for Student Data Privacy and Consent', *2018 International Conference on Computer Communication and Informatics, ICCCI 2018*, pp. 1–5. Available at: https://doi.org/10.3897/zookeys.788.30148.

Goecks, L.S. *et al.* (2021) 'Design Science Research in practice: Review of applications in Industrial Engineering', *Gestao e Producao*, 28(4), pp. 1–19. Available at: https://doi.org/10.1590/1806-9649-2021v28e5811.

Gogolla, M., Büttner, F. and Richters, M. (2007) 'USE: A UML-based specification environment for validating UML and OCL', *Science of Computer Programming*, 69(1–3), pp. 27–34. Available at: https://doi.org/10.1016/j.scico.2007.01.013.

Gonzalez-Huerta, J. *et al.* (2015) 'Validating a model-driven software architecture evaluation and improvement method: A family of experiments', *Information and Software Technology*, 57(1), pp. 405–429. Available at: https://doi.org/10.1016/j.infsof.2014.05.018.

Grady, C. *et al.* (2017) 'Informed Consent Consent'.

Grönniger, H. and Rumpe, B. (no date) *Modeling Language Variability*. Available at: http://www.se-rwth.de.

Grossman, M., Aronson, J.E. and McCarthy, R. V. (2005) 'Does UML make the grade? Insights from the software development community', *Information and Software*

Technology, 47(6), pp. 383–397. Available at: https://doi.org/10.1016/j.infsof.2004.09.005.

Guardian, T. (2020) 'EasyJet reveals cyber-attack exposed 9m customers' details', *Website* [Preprint]. Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose.

Guidollet, J., Chignier, E. and Devolfe, C. (1978) 'Mechanism of biosynthesis of glycoconjugates at the level of the arterial walls after contact with alloplastic materials. [French] TT - Mecanisme de la biosynthese des glycoconjugues au nivaeu des parois arterielles apres contact avec des materiaux allop', *Annales de Biologie Clinique*, 36(2), pp. 63–67. Available at: https://doi.org/10.1007/978-3-642-29044-2.

Hall, G. *et al.* (2020) 'The Strategic Role of the Regulatory Professional', *Regulatory Focus Article Series*, 3(1).

Hall, M., Marshall, M. and Howarth, A. (2020) *Skeptics with a K*. UK: Merseyside Skeptics Society.

Hammer, M.J. (2016) 'Informed consent in the changing landscape of research', *Oncology Nursing Forum*, 43(5), pp. 558–560. Available at: https://doi.org/10.1188/16.ONF.558-560.

Hapsari, A. *et al.* (2014) *Probing Understanding*, *Journal of Chemical Information and Modeling*. Routledge. Available at: https://doi.org/10.1017/CBO9781107415324.004.

Hapsari, A. and Ritohardoyo, S. (1992) *Probing Understanding*.

Harel, D., and Rumpe, B. and Harel and Rumpe, B., D. (2004) 'Meaningful Modeling : What ' s the Semantics Much confusion surrounds the proper definition of complex modeling', *Computer Journal*, 37(10), pp. 64–72.

Harel, D. and Rumpe, B. (2000) 'Modeling Languages: Syntax, Semantics and All That Stuff - Part I: The Basic Stuff', *Syntax*, 081407(d), pp. 1–28. Available at: http://portal.acm.org/citation.cfm?id=903627.

Harel, D. and Rumpe, B. (2004) 'Meaningful modeling: What's the semantics of "semantics"?', *Computer*, 37(10), pp. 64–72. Available at: https://doi.org/10.1109/MC.2004.172.

Harshvardhan, J., Declan O'Sullivan, P. and Lewis, D. (2018) 'GDPR-driven change detection in consent and activity metadata', *CEUR Workshop Proceedings*, 2112, pp. 16–20.

Helberger, N. *et al.* (2005) 'Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations', *INDICARE Project report State of the Art*, pp. 1–147. Available at: http://www.indicare.org.

De Hert, P. *et al.* (2016) 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer Law and Security Review*, 32(2), pp. 179–194. Available at: https://doi.org/10.1016/j.clsr.2016.02.006.

De Hert, P. *et al.* (2018) 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services', *Computer Law and Security Review*, 34(2), pp. 193–203. Available at: https://doi.org/10.1016/j.clsr.2017.10.003.

Hinds, J., Williams, E.J. and Joinson, A.N. (2020) '"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal', *International Journal of Human Computer Studies*, 143(April), p. 102498. Available at:

https://doi.org/10.1016/j.ijhcs.2020.102498.

Hitzler, P. *et al.* (2012) *OWL 2 Web Ontology Language Primer (Second Edition), W3C Website*. Available at: https://www.w3.org/TR/owl2-primer/ (Accessed: 4 June 2021).

HMSO (2018) *Data Protection Act 2018, HMSO*. Available at: https://doi.org/10.1016/S1067-2516(00)80076-9.

Hoofnagle, C.J. *et al.* (2019) 'The European Union general data protection regulation: What it is and what it means', *Information and Communications Technology Law*, 28(1), pp. 65–98. Available at: https://doi.org/10.1080/13600834.2019.1573501.

Horák, M., Stupka, V. and Husák, M. (2019) 'GDPR compliance in cybersecurity software: A case study of DPIA in information sharing platform', in *ACM International Conference Proceeding Series*. Association for Computing Machinery. Available at: https://doi.org/10.1145/3339252.3340516.

Horizons, S. *et al.* (2018) 'GDPR The transfer of data power', *Journal of Business Ethics*, 14(3), pp. 37–45. Available at: https://www-jstor-org.libproxy.boisestate.edu/stable/25176555?Search=yes&resultItemClick=true&searchText=%28Choosing&searchText=the&searchText=best&searchText=research&searchText=design&searchText=for&searchText=each&searchText=question.%29&searchText=AND.

Horwitz, J. (2021) *China passes new personal data privacy law, to take effect Nov. 1, Reuters*. Available at: https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/ (Accessed: 20 August 2021).

House, C. (2020) 'CAMBRIDGE ANALYTICA(UK) LIMITED', *Website* [Preprint]. Available at: https://beta.companieshouse.gov.uk/company/09375920.

HSE (2019) 'A brief summary of Plan, Do, Check, Act.', *Webpage* [Preprint]. Available at: http://www.hse.gov.uk/managing/plan-do-check-act.htm (Accessed: 17 November 2019).

Hung, C.-C. *et al.* (no date) *The 34th Annual ACM Symposium on Applied Computing : Limassol, Cyprus, April 8-12, 2019*.

I2comply (2018) 'GDPR Training', (September). Available at: https://www.i2comply.com/gdprtraining.aspx.

iaap (2018) *2018 Privacy Tech VENDOR REPORT THE WORLD ' S MOST WIDELY USED*.

IBM (no date a) *Blockchain success starts here, Website*.

IBM (no date b) *Blockchain success starts here, Website*. Available at: https://www.ibm.com/uk-en/topics/what-is-blockchain (Accessed: 26 June 2022).

ICO (2018a) *Children, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/ (Accessed: 25 May 2019).

ICO (2018b) *What is Personal Data?, ICO website*. Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

ICO (2019a) 'Data protection by design and default', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-

default/ (Accessed: 17 November 2019).

ICO (2019b) *ICO says that voice data collected unlawfully by HMRC should be deleted, ICO website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/05/ico-says-that-voice-data-collected-unlawfully-by-hmrc-should-be-deleted/.

ICO (2019c) *Intention to fine British Airways £183.39m under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/.

ICO (2019d) *Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, Website*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

ICO (2019e) 'Penalties', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/.

ICO (2020a) 'Data protection by design and default', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (2020b) *Definitions, Website*. Available at: https://ico.org.uk/for-organisations/data-protection-fee/legal-definitions-fees/ (Accessed: 4 July 2021).

ICO (2020c) *Some basic concepts, Website*.

ICO (2020d) 'Special category data', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

ICO (2020e) 'What is valid consent?', *Website* [Preprint]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

ICO (2021a) *Consent, Website*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (Accessed: 13 July 2021).

ICO (2021b) *Controllers and processors, Websire*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/. (Accessed: 9 July 2021).

ICO (2022) *Data protection by design and default, Webpage*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 17 November 2019).

ICO (no date) *Documentation, Webpage*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (Accessed: 13 July 2021).

Idarti, C. and Arch, B.E. (2013) 'Spatial Configurations : Complex Systems Experiment of Design Automation', (February).

International Organization for Standardization *et al.* (2015) 'The process approach in ISO 9001:2015', *Iso*, p. 7. Available at: https://doi.org/BIBC II, Chemin de Blandonnet 8 , CP

401, 1214 Vernier, Geneva , Switzerland.

Isaacs, A. (2014) 'An overview of qualitative research methodology for public health researchers', *International Journal of Medicine and Public Health*, 4(4), p. 318. Available at: https://doi.org/10.4103/2230-8598.144055.

Islam, S., Mouratidis, H. and Jürjens, J. (2011a) 'A framework to support alignment of secure software engineering with legal regulations', *Software and Systems Modeling*, 10(3), pp. 369–394. Available at: https://doi.org/10.1007/s10270-010-0154-z.

Islam, S., Mouratidis, H. and Jürjens, J. (2011b) 'A framework to support alignment of secure software engineering with legal regulations', *Software and Systems Modeling*, 10(3), pp. 369–394. Available at: https://doi.org/10.1007/s10270-010-0154-z.

Islam, S., Mouratidis, H. and Wagner, S. (2010) 'Towards a framework to elicit and manage security and privacy requirements from laws and regulations', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6182 LNCS, pp. 255–261. Available at: https://doi.org/10.1007/978-3-642-14192-8_23.

Issel, L.M. (2016) 'Research that makes a difference', *Health care management review*, 41(1), p. 1. Available at: https://doi.org/10.1097/HMR.0000000000000097.

J Zuiderveen Borgesius, F *et al.* (2017) 'Digital rights management: The cost to consumers [Point of View]', *CEUR Workshop Proceedings*, 21(3), pp. 150–195. Available at: https://doi.org/10.1016/S0167-4048(02)01117-3.

J Zuiderveen Borgesius, F. *et al.* (2017) 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', *European Data Protection Law Review*, 3(3), pp. 353–368. Available at: https://doi.org/10.21552/edpl/2017/3/9.

Jacobs, B. and Popma, J. (2019) 'Medical research, Big Data and the need for privacy by design', *Big Data and Society*, 6(1), pp. 1–5. Available at: https://doi.org/10.1177/2053951718824352.

Jetu, F.T. and Riedl, R. (2012) 'Determinants of Information Systems and Information Technology Project Team Success: A Literature Review and a Conceptual Model', *Communications of the Association for Information Systems*, 30(1). Available at: https://doi.org/10.17705/1cais.03027.

Jöckel, S., Will, A. and Schwarzer, F. (2008) 'Participatory Media Culture and Digital Online Distribution—Reconfiguring the Value Chain in the Computer Game Industry', *International Journal on Media Management*, 10(3), pp. 102–111. Available at: https://doi.org/10.1080/14241270802262419.

'Juilette - 2018 - GDPR The transfer of Data Power(2).pdf' (no date).

Juilette, A. (2018) 'GDPR The transfer of Data Power', *Community Practitioner*, (June), pp. 36–39.

Kabir, G. and Sumi, R.S. (2014) 'Integrating fuzzy analytic hierarchy process with PROMETHEE method for total quality management consultant selection', *Production and Manufacturing Research*, 2(1), pp. 380–399. Available at: https://doi.org/10.1080/21693277.2014.895689.

Kelly, R., Professional, S. and Officer, D. (2017) 'Principles of Consent Guidance for nursing staff', *British Journal of Healthcare Assistants*, 11(10), pp. 498–502. Available at:

https://doi.org/10.12968/bjha.2017.11.10.498.

Kelsen, P. and Ma, Q. (no date) *A Lightweight Approach for Defining the Formal Semantics of a Modeling Language*.

Kenny, S. and Korba, L. (2002) 'Applying digital rights management systems to privacy rights management', *Computers and Security*, 21(7), pp. 648–664. Available at: https://doi.org/10.1016/S0167-4048(02)01117-3.

Kingsto, J. *et al.* (2018) 'Using Artificial Intelligence to Support Compliance with the General Data Protection Regulation', *arXiv*, 25(4), pp. 1–13. Available at: https://doi.org/10.1007/s10506-017-9206-9.

Kirwan, M. *et al.* (2020) 'What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "explicit consent"—a legal analysis', *Irish Journal of Medical Science*, 190(2), pp. 515–521. Available at: https://doi.org/10.1007/s11845-020-02331-2.

Kitchenham, B. *et al.* (1995) 'Towards a Framework for Software Measurement Validation', *IEEE Transactions on Software Engineering*, 21(12).

Knopf, J.W. (2006) 'Doing a literature review', *PS - Political Science and Politics*, 39(1), pp. 127–132. Available at: https://doi.org/10.1017/S1049096506060264.

Koch, V.G. and Elster, N.R. (2017) 'Introduction: Under attack: Reconceptualizing informed consent', *Journal of Law, Medicine and Ethics*, 45(1), pp. 6–9. Available at: https://doi.org/10.1177/1073110517703095.

Kontoghiorghes, C. (2004) 'Reconceptualizing the learning transfer conceptual framework: empirical validation of a new systemic model', *International Journal of Training and Development*, 8(3), pp. 210–221. Available at: https://doi.org/10.1111/j.1360-3736.2004.00209.x.

Kreuter, F. *et al.* (2020) 'Collecting Survey and Smartphone Sensor Data With an App: Opportunities and Challenges Around Privacy and Informed Consent', *Social Science Computer Review*, 38(5), p. 089443931881638. Available at: https://doi.org/10.1177/0894439318816389.

Kubesch, A.S. and Wicker, S. (2015a) 'Digital rights management: The cost to consumers', *Proceedings of the IEEE*, 103(5), pp. 726–733. Available at: https://doi.org/10.1109/JPROC.2015.2418457.

Kubesch, A.S. and Wicker, S. (2015b) 'Digital rights management: The cost to consumers [Point of View]', *Proceedings of the IEEE*, 103(5), pp. 726–733. Available at: https://doi.org/10.1109/JPROC.2015.2418457.

Kuchinke, W. *et al.* (2016) 'Legal assessment tool (LAT): An interactive tool to address privacy and data protection issues for data sharing', *BMC Medical Informatics and Decision Making*, 16(1), pp. 1–19. Available at: https://doi.org/10.1186/s12911-016-0325-0.

Kung, A., Freytag, J.C. and Kargl, F. (2011) 'Privacy-by-design in ITS applications', *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2011 - Digital Proceedings*, pp. 1–6. Available at: https://doi.org/10.1109/WoWMoM.2011.5986166.

Kung, A. and Kargl, F. (2011) 'Privacy-by-Design in ITS Applications The Way Forward', *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia*

Networks, pp. 1–6. Available at: https://doi.org/10.1109/WoWMoM.2011.5986166.

Kurtz, C., Semmann, M. and Böhmann, T. (2018a) 'Privacy by design to comply with GDPR: A review on third-party data processors', in *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*.

Kurtz, C., Semmann, M. and Böhmann, T. (2018b) *Privacy by Design to Comply with GDPR Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors Completed Research*.

Lachaud, E. (2016) 'Why the certification process defined in the General Data Protection Regulation cannot be successful', *Computer Law and Security Review*, 32(6), pp. 814–826. Available at: https://doi.org/10.1016/j.clsr.2016.07.001.

Lambert, P. (2021) 'Security of Personal Data', *A User's Guide to Data Protection: Law and Policy*, 1(3), pp. 3–5. Available at: https://doi.org/10.5040/9781526515735.ch-012.

Lange, C.F.J. and Chaudron, M.R. V (2006) 'In Practice: UML Software Architecture and Design Description', *Ieee Software* [Preprint].

Lavori, P.W. *et al.* (2005) 'Evaluating the quality of informed consent', *Clinical Trials*, 2(1), pp. 34–41. Available at: https://doi.org/10.1191/1740774505cn066oa.

Lazar, C. *et al.* (2017) 'Lifting the veil of the gdpr to data subjects', *Challenges of the Knowledge scociety, Public Law*, 12(1), pp. 658–667. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

Lenhard, J., Fritsch, L. and Herold, S. (2017) 'A literature study on privacy patterns research', *Proceedings - 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2017*, pp. 194–201. Available at: https://doi.org/10.1109/SEAA.2017.28.

Leung, L. (2015) 'Validity, reliability, and generalizability in qualitative research', *Journal of Family Medicine and Primary Care*, 4(3), p. 324. Available at: https://doi.org/10.4103/2249-4863.161306.

Lewis, S.D. and Tennessee, M. (2008) 'A Comparison of the Readability of Privacy Statements of Banks , Credit Counseling Companies , and Check Cashing Companies', *Journal of Organizational Culture, Communications and Conflict*, 12(2), pp. 87–94.

Lexico Dictionaries (no date) *ORGANIZATION | Definition of ORGANIZATION by Oxford Dictionary, Lexico Dictionaries Online English*. Available at: https://www.lexico.com/definition/organization (Accessed: 7 July 2021).

Lexico Dictionaries and Dictionaries, L. (no date) *ORGANIZATION | Definition of ORGANIZATION by Oxford Dictionary, Lexico Dictionaries Online English*. Available at: https://www.lexico.com/definition/organization (Accessed: 7 July 2021).

Lexico Dictionaries, Dictionaries, L. and Lexico Dictionaries (2019) *Definition of Consent by Lexico., Lexico Dictionaries Online*. Available at: https://www.lexico.com/en/definition/consent. (Accessed: 30 October 2019).

Lexology (2021) *The impact of the GDPR outside the EU - Lexology. [ONLINE], Website*. Available at: https://www.lexology.com/library/detail.aspx?g=872b3db5-45d3-4ba3-bda4-3166a075d02f (Accessed: 25 August 2021).

Li, H., Yu, L. and He, W. (2019) 'The Impact of GDPR on Global Technology Development', *Journal of Global Information Technology Management*, pp. 1–6.

Available at: https://doi.org/10.1080/1097198X.2019.1569186.

Li, Z.S. *et al.* (2020) 'GDPR Compliance in the Context of Continuous Integration', pp. 1–14. Available at: http://arxiv.org/abs/2002.06830.

Lievens, E. and Verdoodt, V. (2018) 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation', *Computer Law and Security Review*, 34(2), pp. 269–278. Available at: https://doi.org/10.1016/j.clsr.2017.09.007.

Lima, V. *et al.* (2009) 'Formal Verification and Validation of UML 2.0 Sequence Diagrams using Source and Destination of Messages', *Electronic Notes in Theoretical Computer Science*, 254, pp. 143–160. Available at: https://doi.org/10.1016/j.entcs.2009.09.064.

Linden, T. *et al.* (2018) 'The privacy policy landscape after the GDPR', *arXiv*, 2020(1), pp. 47–64. Available at: https://doi.org/10.2478/popets-2020-0004.

Literate, S. and Indonesia, J.I. (2020) 'View metadata, citation and similar papers at core.ac.uk', pp. 274–282.

Liu, Junjie; Zhang, Wei' Gao, Wei' Yu, Y. (no date) 'Conceptual model for simulatgion', 148, pp. 148–162.

Llp, B., Bird, B. and Llp, B. (2020) 'GDPR Training About', (September 2018).

Lodderstedt, T., Basin, D. and Doser, J. (no date) *SecureUML: A UML-Based Modeling Language for Model-Driven Security*.

Lomas, N. (2019) 'Most EU cookie "consent" notices are meaningless or manipulative, study finds', *Tech Crunch* [Preprint]. Available at: https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGT0n55tXVP0W5OHBZPDib2wxg5MZQRNy4q_FvRvLeY2G2HHGTAm3NW4bnyN7OVg.

Loughlin, M., Bluhm, R., Stoyanov, Drozdstoj S., *et al.* (2013) 'Explanation , understanding , objectivity and experience', *Journal of Evaluation in Clinical Practice*, 19(3), pp. 415–421. Available at: https://doi.org/10.1111/jep.12060.

Loughlin, M., Bluhm, R., Stoyanov, Drozdstoj S, *et al.* (2013) 'Explanation , understanding , objectivity and experience', 19, pp. 415–421. Available at: https://doi.org/10.1111/jep.12060.

Malatras, A. *et al.* (2017) 'Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities', *Computer Law and Security Review*, 33(4), pp. 458–469. Available at: https://doi.org/10.1016/j.clsr.2017.03.013.

Maler, E. (2015) 'Extending the power of consent with user-managed access: A standard architecture for asynchronous, centralizable, internet-scalable consent', *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pp. 175–179. Available at: https://doi.org/10.1109/SPW.2015.34.

Malgieri, G. (2018) '"User-provided personal content" in the EU: digital currency between data protection and intellectual property', *International Review of Law, Computers and*

Technology, 32(1), pp. 118–140. Available at: https://doi.org/10.1080/13600869.2018.1423887.

Malgieri, G. and Custers, B. (2018) 'Pricing privacy – the right to know the value of your personal data', *Computer Law and Security Review*, 34(2), pp. 289–303. Available at: https://doi.org/10.1016/j.clsr.2017.08.006.

Manual, U. (no date) 'SecTro Tool'.

Margulies, N. (2021a) 'Causal Analysis of GDPR Impact on Privacy Policies'.

Margulies, N. (2021b) *"Please Respect Our Terms and Conditions": Causal Analysis of GDPR Impact on Privacy Policies*.

Markosian, L.Z., Feather, M.S. and Brinza, D.E. (2011) 'Verification and Validation', *System Health Management: With Aerospace Applications*, pp. 159–183. Available at: https://doi.org/10.1002/9781119994053.ch10.

Mars, G. (2018) *Occupational crime, Occupational Crime*. Available at: https://doi.org/10.4324/9781315193854.

Martin, K. (2018) 'The penalty for privacy violations: How privacy violations impact trust online', *Journal of Business Research*, 82(August 2017), pp. 103–116. Available at: https://doi.org/10.1016/j.jbusres.2017.08.034.

Martín, Y.-S.S. and Del Álamo, J.M. (2017) 'A metamodel for privacy engineering methods', *CEUR Workshop Proceedings*, 1873(731711), pp. 41–48.

Martin, Y.S. and Kung, A. (2018) 'Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering', *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, pp. 108–111. Available at: https://doi.org/10.1109/EuroSPW.2018.00021.

Massey, R. (2018) 'GDPR consent - UK's ICO guidancere-delivers the message that "consent isnot the silver bullet for GDPR compliance', *Entertainment Law Review* [Preprint].

Mathis, K. (2021) 'Consumer Law and Economics', *Consumer Law and Economics* [Preprint]. Available at: https://doi.org/10.1007/978-3-030-49028-7.

Mavropoulos, O. (2019) 'Apparatus : A design and analysis security framework for IoT systems', (October).

Maxwell, J.C. and Antón, A.I. (2009) 'Developing production rule models to aid in acquiring requirements from legal texts', *Proceedings of the IEEE International Conference on Requirements Engineering*, pp. 101–110. Available at: https://doi.org/10.1109/RE.2009.21.

Mcdowell, B. (2017) *References 1. 'Data Breach Investigations Report*. Available at: https://community.blueliv.com/#!/.

McDowell, B. (2019) 'Three ways in which GDPR impacts authentication', *Computer Fraud and Security*, 2019(2), pp. 9–12. Available at: https://doi.org/10.1016/S1361-3723(19)30019-3.

McKernan, B. (2021) *Israeli authorities inspect NSO Group offices after Pegasus revelations*, *The Guardian website*. Available at: https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-

offices-after-pegasus-revelations (Accessed: 29 July 2021).

Meilicke, C., Shvaiko, P. and Stuckenschmidt, H. (2013) *Ontology Alignment Evaluation Initiative : six years of experience J ´ erˆ C ´ assia Trojahn dos Santos To cite this version : Ontology Alignment Evaluation Initiative : six years of experience*.

Meneszes, A. (2019) *First GDPR fine in Portugal issued against hospital for three violations, The Privacy Advisor*. Available at: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.

Merriam Webster and Webster, M. (no date) *A Function Of, Website*. Available at: https://www.merriam-webster.com/dictionary/a function of (Accessed: 14 July 2021).

van der Merwe, A., Gerber, A. and Smuts, H. (2020) 'Guidelines for conducting design science research in information systems', *Communications in Computer and Information Science*, 1136 CCIS, pp. 163–178. Available at: https://doi.org/10.1007/978-3-030-35629-3_11.

Le Métayer, D. (2013) 'Privacy by design: Formal framework for the analysis of architectural choices', *CODASPY 2013 - Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, pp. 95–104. Available at: https://doi.org/10.1145/2435349.2435361.

Le Métayer, D., Métayer, D. Le and Le Métayer, D. (2013) 'Privacy by design: Formal framework for the analysis of architectural choices', *CODASPY 2013 - Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy*, pp. 95–104. Available at: https://doi.org/10.1145/2435349.2435361.

Mezei, P. *et al.* (2017) 'Enforcement of Copyrights over the Internet: A Review of the Recent ECJ Case Law', *Journal of internet law*, 21(4), pp. 13–28.

Miglicco, G. (2018) 'GDPR is here and it is time to get serious', *Computer Fraud and Security*, 2018(9), pp. 9–12. Available at: https://doi.org/10.1016/S1361-3723(18)30085-X.

Minhas, M.R. and Potdar, V. (2020) 'Decision support systems in construction: A bibliometric analysis', *Buildings*, 10(6). Available at: https://doi.org/10.3390/BUILDINGS10060108.

Morales-trujillo, M.E. *et al.* (2018) 'Privacy by design in software engineering: A systematic mapping study', *Avances en Ingenieria de Software a Nivel Iberoamericano, CIbSE 2018*, 22(1), pp. 107–120.

Morales-Trujillo, M.E. *et al.* (2018) 'Privacy by design in software engineering: A systematic mapping study', *Avances en Ingenieria de Software a Nivel Iberoamericano, CIbSE 2018*, 22(1), pp. 107–120.

Mostert, M. *et al.* (2016) 'Big Data in medical research and EU data protection law: Challenges to the consent or anonymise approach', *European Journal of Human Genetics*, 24(7), pp. 956–960. Available at: https://doi.org/10.1038/ejhg.2015.239.

Mouratidis, H. (no date a) 'Secure Tropos', 50(3), pp. 198–202.

Mouratidis, H. (no date b) 'Secure Tropos Methodology', 50(3), pp. 198–202.

MOURATIDIS, H. *et al.* (2018) 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach', *Computer Law and Security Review*. 1st edn. Edited by S. Schiffner et al., 10(1), pp. 1–10. Available at:

https://doi.org/10.1016/j.procs.2017.08.329.

Mouratidis, H., Argyropoulos, N. and Shei, S. (2016) 'Security requirements engineering for cloud computing: The secure tropos approach', *Domain-Specific Conceptual Modeling: Concepts, Methods and Tools*, pp. 357–380. Available at: https://doi.org/10.1007/978-3-319-39417-6_16.

Mouratidis, H. and Giorgini, P. (2007) 'Secure Tropos: A security-oriented extension of the Tropos methodology', *International Journal of Software Engineering and Knowledge Engineering*, 17(2), pp. 285–309. Available at: https://doi.org/10.1142/S0218194007003240.

Mouratidis, H., Jürjens, J. and Fox, J. (2006) 'Towards a comprehensive framework for secure systems development', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 48–62. Available at: https://doi.org/10.1007/11767138_5.

Mouratidis, P.H., Fotis, T. and Pavlidis, M. (2018) 'Transfer Document Secure Recovery Management for Health-based Critical Infrastructures Myrsini Athinaiou Supervisors : University of Brighton Department of Life , Health and Physical Sciences School of Computing , Engineering and Mathematics'.

Mourby, M. *et al.* (2018) 'Are "pseudonymised" data always personal data? Implications of the GDPR for administrative data research in the UK', *Computer Law and Security Review*, 34(2), pp. 222–233. Available at: https://doi.org/10.1016/j.clsr.2018.01.002.

Mouzas, S. and Ford, D. (2018) 'The mediating role of consent in business marketing', *Industrial Marketing Management*, 74(April), pp. 195–204. Available at: https://doi.org/10.1016/j.indmarman.2018.03.011.

Muravyeva, E. *et al.* (2020) 'Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited', *Ethics and Information Technology*, 22(3), pp. 223–238. Available at: https://doi.org/10.1007/s10676-020-09531-5.

Musselman, K. and Reilly, J.O. (2002) 'Proceedings of the 2002 Winter Simulation Conference E. Yiicesan. C.-H. Chen, J. L.', *Simulation*, (1997), pp. 1825–1830.

Mutiso, M.M., Theses, E. and Citation, R. (2017) *Rapid discharge failure prediction model for solar charged lithium-ion batteries*. Strathmore University.

Neisse, R. *et al.* (2015) 'An agent-based framework for Informed Consent in the internet of things', *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, (3), pp. 789–794. Available at: https://doi.org/10.1109/WF-IoT.2015.7389154.

Nicol, D.M., Sanders, W.H. and Trivedi, K.S. (2004) 'Model-based evaluation: From dependability to security', *IEEE Transactions on Dependable and Secure Computing*, 1(1), pp. 48–64. Available at: https://doi.org/10.1109/TDSC.2004.11.

Nicole, O. (2021) 'Implementing Privacy By Design', *Webpage* [Preprint]. Available at: https://www.privacypolicies.com/blog/privacy-by-design/.

Nijhawan, L.P. and Janodia, M.D. (2013) 'Informed consent : Issues and challenges', 4(3). Available at: https://doi.org/10.4103/2231-4040.116779.

Nord, K. (2018) 'Capable parents : Freedom of choice under the GDPR'.

O'Connor, Y. *et al.* (2017) 'Privacy by Design: Informed Consent and Internet of Things for Smart Health', *Procedia Computer Science*, 113, pp. 653–658. Available at:

https://doi.org/10.1016/j.procs.2017.08.329.

O'Neil, O. (2003) 'Some limits of informed consent', *Journal of Medical Ethics*, 29(1), pp. 4–7. Available at: https://doi.org/10.1136/jme.29.1.4.

O'Neil, O., O\'Neill, O. and O'Neil, O. (2003) 'Some limits of informed consent', *Journal of Medical Ethics*, 29(1), pp. 4–7. Available at: https://doi.org/10.1136/jme.29.1.4.

O'neill, O. (2017) 'Some limits of informed consent', *The Elderly: Legal and Ethical Issues in Healthcare Policy*, pp. 103–106. Available at: https://doi.org/10.4324/9781315240046-9.

O'Neill, O. (2001) 'Informed Consent and Genetic Information', *Studies in History and Philosophy of Science Part C :Studies in History and Philosophy of Biological and Biomedical Sciences*, 32(4), pp. 689–704. Available at: https://doi.org/10.1016/S1369-8486(01)00026-7.

Of, M. and Literature, T.H.E. (no date) '3 METHODOLOGY OF THE LITERATURE REVIEW Chapter 3 Roadmap Background Concepts'. Available at: http://study.sagepub.com/sites/default/files/Onwuegbuzie.

Office), I. (Information C.O. (Information C. (Information C. (2019) 'Guide to the General Data Protection Regulation (GDPR)', *Guide to the General Data Protection Regulation*, (May), p. n/a. Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

Olsson, B. and Sidenblom, L. (2010) *Business models for video games*. Lund University.

Omar, M.F., Trigunarsyah, B. and Wong, J. (2009) 'A design science approach for consultant selection decision support system', *4th International Conference on Cooperation and Promotion of Information Resources in Science and Technology, COINFO 2009*, pp. 90–94. Available at: https://doi.org/10.1109/COINFO.2009.73.

OMG (2021a) *About the Unified Modeling Language Specification Version 2.0, Website*. Available at: https://www.omg.org/spec/UML/2.0/About-UML/ (Accessed: 14 March 2021).

OMG (2021b) *Welcome To UML Web Site!, Website*. Available at: https://www.uml.org/ (Accessed: 14 March 2021).

Onwuegbuzie, Anthony J and Frels, R. (2016a) 'METHODOLOGY OF THE LITERATURE REVIEW', in *Seven Steps to a comprehensive literature review*. Sage, pp. 49–64.

Onwuegbuzie, Anthony J and Frels, R. (2016b) 'METHODOLOGY OF THE LITERATURE REVIEW BT - Seven Steps to a comprehensive literature review', in *Seven Steps to a comprehensive literature review*, pp. 49–64.

Onwuegbuzie, Anthony J. and Frels, R. (2016) 'Seven Steps to a Comprehensive Literature Review', 23(2), pp. 48–64.

van Ooijen, I. and Vrabec, H.U. (2019) 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective', *Journal of Consumer Policy*, 42(1), pp. 91–107. Available at: https://doi.org/10.1007/s10603-018-9399-7.

Orange (2022) *Blockchain for consent management: improved privacy and user control, Website*.

Pace, E. (1997) ‘P. G. Gebhard, 69, Developer Of the Term “Informed Consent”’, *The New York Times*, p. Section D Page 21. Available at: https://www.nytimes.com/1997/08/26/us/p-g-gebhard-69-developer-of-the-term-informed-consent.html.

Paige, R.F., Ostroff, J.S. and Brooke, P.J. (no date) *Principles for modeling language design*. Available at: www.elsevier.nl/locate/infsof.

Palmirani, M. *et al.* (2018) ‘Legal ontology for modelling GDPR concepts and norms’, *Frontiers in Artificial Intelligence and Applications*, 313, pp. 91–100. Available at: https://doi.org/10.3233/978-1-61499-935-5-91.

Palmirani, M. and Governatori, G. (2018) ‘Modelling legal knowledge for GDPR compliance checking’, in *Frontiers in Artificial Intelligence and Applications*. Available at: https://doi.org/10.3233/978-1-61499-935-5-101.

Pandit, H.J. (2018) *A consent ontology based on the GDPR*. Available at: http://purl.org/vocab/vann.

Pandit, H.J. *et al.* (2019) ‘GConsent - A consent ontology based on the GDPR’, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 270–282. Available at: https://doi.org/10.1007/978-3-030-21348-0_18.

Pandit, H.J. *et al.* (no date) *GConsent-A Consent Ontology based on the GDPR*. Available at: https://w3id.org/GConsent.

Pavlidis, M. *et al.* (2017) ‘Selecting Security Mechanisms in Secure Tropos’, *Trust, Privacy and Security in Digital Business, Trustbus 2017*, 10442, pp. 99–114. Available at: https://doi.org/10.1007/978-3-319-64483-7_7.

Peffers, K. *et al.* (2006) ‘THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH’, *1st International Conference, DESRIST 2006 Proceedings. (pp. 83-106). Claremont Graduate University.*, 18, pp. 583–594.

Perera, C. *et al.* (2016) ‘Privacy-by-design framework for assessing internet of things applications and platforms’, *ACM International Conference Proceeding Series*, 07-09-Nove, pp. 83–92. Available at: https://doi.org/10.1145/2991561.2991566.

Perera, C. *et al.* (2020) ‘Designing privacy-aware internet of things applications’, *Information Sciences*, 512, pp. 238–257. Available at: https://doi.org/10.1016/j.ins.2019.09.061.

Perry, R. (2019) ‘GDPR – project or permanent reality?’, *Computer Fraud and Security*, 2019(1), pp. 9–11. Available at: https://doi.org/10.1016/S1361-3723(19)30007-7.

Petrlic, R. (2012) ‘Privacy-preserving digital rights management in a trusted cloud environment’, *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, (Sfb 901), pp. 958–963. Available at: https://doi.org/10.1109/TrustCom.2012.225.

Pilone, Dan; Pitman, N. and Pilone Neil, D.P. (2005) *UML 2.0 in a nutshell, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Available at: https://doi.org/10.1007/3-540-39967-4_1.

Piras, L., Paja, E., Giorgini, P., Mylopoulos, J., *et al.* (2017) 'Gamification solutions for software acceptance: A comparative study of Requirements Engineering and Organizational Behavior techniques', *Proceedings - International Conference on Research Challenges in Information Science*, pp. 255–265. Available at: https://doi.org/10.1109/RCIS.2017.7956544.

Piras, L., Paja, E., Giorgini, P. and Mylopoulos, J. (2017a) 'Goal models for acceptance requirements analysis and gamification design', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10650 LNCS, pp. 223–230. Available at: https://doi.org/10.1007/978-3-319-69904-2_18.

Piras, L., Paja, E., Giorgini, P. and Mylopoulos, J. (2017b) 'Goal Models for Acceptance Requirements Analysis and Gamification Design Goal Models for Acceptance Requirements Analysis and Gamification Design Recommended Citation : L . Piras , E . Paja , P . Giorgini and J . Mylopoulos , " Goal Models for Acceptance', (July). Available at: https://doi.org/10.1007/978-3-319-69904-2.

Piras, L. (2018) *Agon : a Gamification-Based Framework for Acceptance Requirements*. Universita Degli Studi Di Trento. Available at: http://eprints-phd.biblio.unitn.it/3424/.

Piras, L. *et al.* (2019) 'DEFeND Architecture: A Privacy by Design Platform for GDPR Compliance', pp. 78–93. Available at: https://doi.org/10.1007/978-3-030-27813-7_6.

Piras, L. *et al.* (2021) 'A Data Scope Management Service to Support Privacy by Design and GDPR Compliance', *Journal of Data Intelligence*, 2(2), pp. 136–165. Available at: https://doi.org/10.26421/jdi2.2-3.

Piras, L., Giorgini, P. and Mylopoulos, J. (2016) 'Acceptance Requirements and Their Gamification Solutions', *Proceedings - 2016 IEEE 24th International Requirements Engineering Conference, RE 2016*, pp. 365–370. Available at: https://doi.org/10.1109/RE.2016.43.

Plain English Campaign (2021) *Plain English Book Mark, Website*. Available at: https://plainenglish.co.uk/services/plain-english-book-mark.html (Accessed: 5 October 2021).

Plain English Campaign and Campaign, P.E. (2020) *Plain English Campaign, Website*. Available at: http://www.plainenglish.co.uk/.

Policy, D. and Policy, D. (2020) 'Repositório ISCTE-IUL The Critical Success Factors of GDPR Implementation : a Systematic Literature Review', (351).

Politou, E. *et al.* (2018) 'Backups and the right to be forgotten in the GDPR: An uneasy relationship', *Computer Law and Security Review*, 34(6), pp. 1247–1257. Available at: https://doi.org/10.1016/j.clsr.2018.08.006.

Politou, E., Alepis, E. and Patsakis, C. (2018) 'Forgetting personal data and revoking consent under the GDPR: Challenges and Proposed Solutions', *Journal of Cybersecurity*, 4(February), pp. 1–20. Available at: https://doi.org/10.1093/CYBSEC/TYY001.

Pope-Rhodius, A. and Howard, M. (2018) 'Working with Your Supervisor', *Excelling in Sport Psychology*, (December), pp. 60–74. Available at: https://doi.org/10.4324/9780203729649-6.

Practical Law Employment, Employment, P.L. and Practical Law Employment (2020) *Comparisons: DPA 1998 v GDPR and DPA 2018, Website*. Available at:

https://uk.practicallaw.thomsonreuters.com/w-011-6935?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (Accessed: 21 May 2020).

Practice, T. (2004) 'Mechanisms in an Electronic Environment', *Journal of the American Medical Informatics Association*, 11(2), pp. 129–140. Available at: https://doi.org/10.1197/jamia.M1480.j.

Preibusch, S. *et al.* (2007) *Ubiquitous Social Networks: Opportunities and Challenges for Privacy-Aware User Modelling DIW Discussion Papers, No. 698 Provided in Cooperation with: German Institute for Economic Research (DIW Berlin) Suggested*. Berlin.

Presthus, W. and Sørum, H. (2018) 'Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation', *Procedia Computer Science*, 138, pp. 603–611. Available at: https://doi.org/10.1016/j.procs.2018.10.081.

Protection, D. *et al.* (2001) 'Informed Consent and Genetic Information Onora O ' Neill *', 32(4), pp. 689–704.

Purtova, N. (2018) 'The law of everything. Broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology*, 10(1), pp. 40–81. Available at: https://doi.org/10.1080/17579961.2018.1452176.

Question pro (2020) *Target Audience: What is and how to define it, Website*. Available at: https://www.questionpro.com/blog/what-is-a-target-audience/.

Raab, C. and Szekely, I. (2017) 'Data protection authorities and information technology', *Computer Law and Security Review*, 33(4), pp. 421–433. Available at: https://doi.org/10.1016/j.clsr.2017.05.002.

Ramadan, Q. *et al.* (2020) 'A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization, and fairness requirements', *Software and Systems Modeling*, 19(5), pp. 1191–1227. Available at: https://doi.org/10.1007/s10270-020-00781-x.

Rau, H. *et al.* (2020) 'The generic Informed Consent Service gICS®: implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research', *Journal of Translational Medicine*, 18(1), pp. 1–12. Available at: https://doi.org/10.1186/s12967-020-02457-y.

Ray, L. and Peter, A. (2003) 'QUT Digital Repository : study', 5, pp. 214–220.

Readable (2021) *Flesch Reading Ease and the Flesch Kincaid Grade Level – Readable., Website*. Available at: t: https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/. (Accessed: 8 August 2021).

Reichard, B. *et al.* (2020) 'Writing impact case studies: a comparative study of high-scoring and low-scoring case studies from REF2014', *Palgrave Communications*, 6(1). Available at: https://doi.org/10.1057/s41599-020-0394-7.

Renaud, K. and Shepherd, L.A. (2018) 'How to make privacy policies both GDPR-compliant and usable', in *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*. Available at: https://doi.org/10.1109/CyberSA.2018.8551442.

Reupert, A. (2018) 'Research that makes a difference', *Advances in Mental Health*, 16(2), pp. 101–104. Available at: https://doi.org/10.1080/18387357.2018.1492513.

Rights, D. (2003) ‘The Good, the Bad, and the Ugly’, pp. 63–66.

Ringmann, S.D., Langweg, H. and Waldvogel, M. (2018) ‘Requirements for legally compliant software based on the GDPR’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11230 LNCS(1), pp. 258–276. Available at: https://doi.org/10.1007/978-3-030-02671-4_15.

Rishipathak, P. *et al.* (2014) ‘2 and 3 May 2014 Symbiosis Institute of Health Sciences (SIHS)’, in A.P. Pandit (ed.).

Robak, M. and Buchmann, E. (2019) ‘Deriving workflow privacy patterns from legal documents’, *Proceedings of the 2019 Federated Conference on Computer Science and Information Systems, FedCSIS 2019*, 18, pp. 555–563. Available at: https://doi.org/10.15439/2019F275.

Robol, M. *et al.* (2018) ‘Modeling and reasoning about privacy-consent requirements’, *Lecture Notes in Business Information Processing*, 335(May), pp. 238–254. Available at: https://doi.org/10.1007/978-3-030-02302-7_15.

Rodríguez, A. *et al.* (2011) ‘Secure business process model specification through a UML 2.0 activity diagram profile’, *Decision Support Systems*, 51(3), pp. 446–465. Available at: https://doi.org/10.1016/j.dss.2011.01.018.

Romanou, A. (2018) ‘The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise’, *Computer Law and Security Review*, 34(1), pp. 99–110. Available at: https://doi.org/10.1016/j.clsr.2017.05.021.

Romberg, T. (2007) ‘Software platforms - How to win the peace’, *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1–10. Available at: https://doi.org/10.1109/HICSS.2007.495.

Roy, C.J. and Oberkampf, W.L. (2011) ‘A comprehensive framework for verification, validation, and uncertainty quantification in scientific computing’, *Computer Methods in Applied Mechanics and Engineering*, 200(25–28), pp. 2131–2144. Available at: https://doi.org/10.1016/j.cma.2011.03.016.

Ruan, C. and Yeo, S.S. (2009) ‘Modeling of an Intelligent e-Consent System in a Healthcare Domain’, *Journal of Universal Computer Science*, 15(12), pp. 2429–2444.

Russell, N. *et al.* (2006) ‘On the suitability of UML 2.0 Activity Diagrams for business process modelling’, in *Conferences in Research and Practice in Information Technology Series*. Australian Computer Society Inc, pp. 95–104. Available at: http://portal.acm.org/citation.cfm?id=1151866http://portal.acm.org/citation.cfm?id=1151866.

Saglam, R.B. *et al.* (2020) ‘Is your chatbot GDPR compliant? Open issues in agent design’, *arXiv* [Preprint]. Available at: https://doi.org/10.1145/3405755.3406131.

Salnitri, M. *et al.* (2020) ‘Modelling the interplay of security, privacy and trust in sociotechnical systems: a computer-aided design approach’, *Software and Systems Modeling*, 19(2), pp. 467–491. Available at: https://doi.org/10.1007/s10270-019-00744-x.

Samudrala, R. (2008) ‘Join the Hunt for Super-Rice’, *Technology*, (October), pp. 1–9.

Santos, A.L., Koskimies, K. and Lopes, A. (2008) ‘Automated Domain-Specific Modeling Languages for generating framework-based applications’, *Proceedings - 12th International*

Software Product Line Conference, SPLC 2008, pp. 149–158. Available at: https://doi.org/10.1109/SPLC.2008.17.

Sargent, R.G. (2010) 'Verification and validation of simulation models', pp. 166–183.

Satyanarayana Rao, K.H.H. (2008) 'Informed consent: An ethical obligation or legal compulsion?', *Journal of Cutaneous and Aesthetic Surgery*, 1(1), p. 33. Available at: https://doi.org/10.4103/0974-2077.41159.

Schartum, D.W. (2016) 'Making privacy by design operative', *International Journal of Law and Information Technology*, 24(2), pp. 151–175. Available at: https://doi.org/10.1093/ijlit/eaw002.

Schiffner, S. (2019) 'Privacy Technologies and Policy'. Edited by S. Schiffner et al., 11498. Available at: https://doi.org/10.1007/978-3-319-44760-5.

Schmidt, D.C., C. Schmidt and Schmidt, D.C. (2018) 'Google Data Collection', *Digital Content Next*, (AUgust), p. 53. Available at: http://bf4dv7zn3u.search.serialssolutions.com.myaccess.library.utoronto.ca/?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rfr_id=info:sid/Ovid:emed18b&rft.genre=article&rft_id=info:doi/10.1016%2Fj.ijmm.2016.11.008&rft_id=info:pmid/&rft.issn.

Schreier, M. and Prügl, R.W. (2011) 'ePub WU Institutional Repository', *Library*, 1(September), pp. 269–288. Available at: https://doi.org/10.1007/s10551-011-0925-7.

Schryen, G. (2015) 'Writing qualitative is literature reviews -Guidelines for synthesis, interpretation, and guidance of research association for nformation ystems writing qualitative is literature reviews - guidelines for Synthesis, Interpretation, and Guidance of Research', *Communications of the Association for Information Systems*, 37(12), pp. 286–325. Available at: http://aisel.aisnet.org/cais.

Schwarz, A. *et al.* (2007) 'Understanding Frameworks and Reviews : A Commentary to Assist us in Moving Our Field Forward by Analyzing Our Past', *The DATA BASE for Advances in Information Systems*, 38(3), pp. 29–50. Available at: https://doi.org/http://doi.acm.org/10.1145/1278253.1278259.

Scrum.org (2019) 'What is Scrum?', *Online* [Preprint]. Available at: https://www.scrum.org/resources/what-is-scrum (Accessed: 17 November 2019).

Seidewitz, E. (2003) 'What models mean', *IEEE Software*, 20(5), pp. 26–32. Available at: https://doi.org/10.1109/MS.2003.1231147.

Senarath, A. and Arachchilage, N.A.G.G. (2018a) 'Why developers cannot embed privacy into software systems?: An empirical investigation', in *ACM International Conference Proceeding Series*. Association for Computing Machinery. Available at: https://doi.org/10.1145/3210459.3210484.

Senarath, A. and Arachchilage, N.A.G.G. (2018b) 'Why developers cannot embed privacy into software systems?', *arXiv* [Preprint]. Available at: https://doi.org/10.1145/3210459.3210484.

Seo, J. *et al.* (2018) 'An analysis of economic impact on IoT industry under GDPR', *Mobile Information Systems*, 2018, pp. 879–881. Available at: https://doi.org/10.1155/2018/6792028.

Shei, S. (2016) *A model-driven approach towards designing and analysing secure systems*

for multi-clouds. Brighton.

Shore, J. *et al.* (2015) 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy', *Technology Science*, pp. 1–37. Available at: http://techscience.org/a/2015081102/.

Shore, J. and Steinman, J. (2015) 'Did You Really Agree to That? The Evolution of Facebook's Privacy Policy', *Technology Science*, pp. 1–37. Available at: http://techscience.org/a/2015081102/.

Simkulet, W. (2018) 'Nudging, informed consent and bullshit', *Journal of Medical Ethics*, 44(8), pp. 536–542. Available at: https://doi.org/10.1136/medethics-2017-104480.

Sing, E. (2018) 'A Meta-Model Driven Method for Establishing Business Process Compliance to GDPR'.

Singh, J. and Cobbe, J. (2019) 'The Security Implications of Data Subject Rights', *IEEE Security and Privacy*, 17(6), pp. 21–30. Available at: https://doi.org/10.1109/MSEC.2019.2914614.

Sion, L. *et al.* (2019) 'An architectural view for data protection by design', *Proceedings - 2019 IEEE International Conference on Software Architecture, ICSA 2019*, (i), pp. 11–20. Available at: https://doi.org/10.1109/ICSA.2019.00010.

Sirur, S., Nurse, J.R.C.C. and Webb, H. (2018) 'Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)', *arXiv*, (iii), pp. 88–95. Available at: https://doi.org/10.1145/3267357.3267368.

Skemp, R.R. (2020) 'Relational Understanding and Instrumental Understanding', *The Arithmetic Teacher*, 26(3), pp. 9–15. Available at: https://doi.org/10.5951/at.26.3.0009.

Smith, C.M. and Shaw, D. (2019) 'The characteristics of problem structuring methods: A literature review', *European Journal of Operational Research*, 274(2), pp. 403–416. Available at: https://doi.org/10.1016/j.ejor.2018.05.003.

Smooth Radio (no date) *Smooth Chil - Music To Chill To, Webpage*. Available at: https://www.smoothradio.com/chill/ (Accessed: 4 September 2022).

Sobolewski, M., Mazur, J. and Paliński, M. (2017) 'GDPR: A step towards a user-centric internet?', *Intereconomics*, 52(4), pp. 207–213. Available at: https://doi.org/10.1007/s10272-017-0676-5.

Society, R.E. (2019) 'Author (s): Paola Sapienza , Anna Toldra-Simats and Luigi Zingales Published by : Oxford University Press on behalf of the Royal Economic Society Stable URL : https://www.jstor.org/stable/42919277', 123(573), pp. 1313–1332.

Solnyshkina, M.I. *et al.* (2017) 'Evaluating text complexity and Flesch-Kincaid grade level', *Journal of Social Studies Education Research*, 8(3), pp. 238–248. Available at: https://doi.org/10.17499/jsser.79630.

Solove, D.J. (2008) 'Privacy: A Concept in Disarray Privacy', *Understanding Privacy*, (May), pp. 1–11. Available at: https://doi.org/10.1191/0969733006nej901oa.

Spataru-Negura, L.-C., Cornelia, □ and □□ L. (no date) *LIFTING THE VEIL OF THE GDPR TO DATA SUBJECTS*. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

Spiekermann-hoff, S. (2017) 'ePub WU Institutional Repository', (March).

Spiekermann, S. (2012) ‘The challenges of privacy by design’, *Communications of the ACM*, 55(7), pp. 38–40. Available at: https://doi.org/10.1145/2209249.2209263.

Spike, J.P. (2017) ‘Informed consent is the essence of capacity assessment’, *Journal of Law, Medicine and Ethics*, 45(1), pp. 95–105. Available at: https://doi.org/10.1177/1073110517703103.

Sreenivasan, G. (2003) ‘Does informed consent to research require comprehension?’, *Lancet*, 362(9400), pp. 2016–2018. Available at: https://doi.org/10.1016/S0140-6736(03)15025-8.

Staff, I. and IEEE Staff (2017) *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE.

State of Callifornia Department of Justice; Office of the Attorney General (2021) *California Consumer Privacy Act (CCPA), Website*. Available at: https://www.oag.ca.gov/privacy/ccpa (Accessed: 25 August 2021).

Steinman, J.S.J. *et al.* (2015) ‘Did You Really Agree to That? The Evolution of Facebook’s Privacy Policy’, *Technology Science*, pp. 1–37. Available at: http://techscience.org/a/2015081102/.

Störrle, H. (2005) ‘Semantics and verification of data flow in UML 2.0 activities’, *Electronic Notes in Theoretical Computer Science*, 127(4), pp. 35–52. Available at: https://doi.org/10.1016/j.entcs.2004.08.046.

Tachepun, C. and Thammaboosadee, S. (2020) ‘A Data Masking Guideline for Optimizing Insights and Privacy under GDPR Compliance’, *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3406601.3406627.

Talk, P. (no date) *Language Modeling Tips*. Available at: http://www.asha.org/public/speech/development/Parent-Stim-Activities.htm.

Tamburri, D.A. (2020) ‘Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation’, *Information Systems*, 91, p. 101469. Available at: https://doi.org/10.1016/j.is.2019.101469.

The Open Data Institute (2018) ‘ODI survey reveals British consumer attitudes to sharing personal data’, *Website* [Preprint]. Available at: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/.

The Open Data Institute and Institute, T.O.D. (2018) ‘ODI survey reveals British consumer attitudes to sharing personal data’, *Website* [Preprint]. Available at: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/.

Thomes, T.P. (2013) ‘An economic analysis of online streaming music services’, *Information Economics and Policy*, 25(2), pp. 81–91. Available at: https://doi.org/10.1016/j.infoecopol.2013.04.001.

Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018) ‘EU General Data Protection Regulation: Changes and implications for personal data collecting companies’, *Computer Law and Security Review*, 34(1), pp. 134–153. Available at: https://doi.org/10.1016/j.clsr.2017.05.015.

Tort, A. and Olivé, A. (2010) ‘An approach to testing conceptual schemas’, *Data and Knowledge Engineering*, 69(6), pp. 598–618. Available at:

https://doi.org/10.1016/j.datak.2010.02.002.

Tutorials Point and Point, T. (2021) *UML 2.0 - Overview - Tutorialspoint, Website*. Available at: https://www.tutorialspoint.com/uml/uml_2_overview.htm (Accessed: 28 January 2021).

Tzolov, T. (2018) 'One model for implementation GDPR based on ISO standards', *2018 International Conference on Information Technologies, InfoTech 2018 - Proceedings*, (46116), pp. 1–3. Available at: https://doi.org/10.1109/InfoTech.2018.8510716.

Utz, C. *et al.* (2019) '(Un)informed Consent: Studying GDPR consent notices in the field', *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 973–990. Available at: https://doi.org/10.1145/3319535.3354212.

Vandercruysse, L., Buts, C. and Dooms, M. (2020) 'A typology of Smart City services: The case of Data Protection Impact Assessment', *Cities*, 104(July 2019), p. 102731. Available at: https://doi.org/10.1016/j.cities.2020.102731.

Varnhagen, C.K. *et al.* (2005) 'How informed is online informed consent?', *Ethics and Behavior*, 15(1), pp. 37–48. Available at: https://doi.org/10.1207/s15327019eb1501_3.

Veale, M., Binns, R. and Ausloos, J. (2018) 'When data protection by design and data subject rights clash', *International Data Privacy Law*, 8(2), pp. 105–123. Available at: https://doi.org/10.1093/idpl/ipy002.

Veale, M. and Edwards, L. (2018) 'Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling', *Computer Law and Security Review*, 34(2), pp. 398–404. Available at: https://doi.org/10.1016/j.clsr.2017.12.002.

Velykien, R. (2013) 'Applications of Dependable Computing Concepts to National Infrastructure Systems'.

Viana, M.C., Penteado, R.A.D.D. and Do Prado, A.F. (2013) 'Domain-Specific Modeling Languages to improve framework instantiation', *Journal of Systems and Software*, 86(12), pp. 3123–3139. Available at: https://doi.org/10.1016/j.jss.2013.07.030.

Vinet, L. and Zhedanov, A. (2011) 'PIA Knowledge Bases', *Journal of Physics A: Mathematical and Theoretical*, 44(8), pp. 1689–1699. Available at: http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12.

Vitolins, V. and Kalnins, A. (2005) 'Semantics of UML 2.0 activity diagram for business modeling by means of virtual machine', *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*, pp. 181–192. Available at: https://doi.org/10.1109/EDOC.2005.29.

Wachter, S. (2018) 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', *Computer Law and Security Review*, 34(3), pp. 436–449. Available at: https://doi.org/10.1016/j.clsr.2018.02.002.

Wagner, I. and Eckhoff, D. (2018a) 'Technical privacy metrics: A systematic survey', *ACM Computing Surveys*. Association for Computing Machinery. Available at: https://doi.org/10.1145/3168389.

Wagner, I. and Eckhoff, D. (2018b) 'Technical Privacy Metrics', *ACM Computing*

Surveys, 51(3), pp. 1–38. Available at: https://doi.org/10.1145/3168389.

Wheeler, R. (2012) 'The evolution of informed consent', *British Journal of Surgery*, 104(9), pp. 1119–1120. Available at: https://doi.org/10.1002/bjs.10520.

White, R. and Gunstone, R. (2014) *Probing Understanding*, *Journal of Chemical Information and Modeling*. Available at: https://doi.org/10.1017/CBO9781107415324.004.

Wicker, S.B. and Schrader, D.E. (2011) 'Privacy-aware design principles for information networks', *Proceedings of the IEEE*, 99(2), pp. 330–350. Available at: https://doi.org/10.1109/JPROC.2010.2073670.

Wiggins, G. and McTighe, J. (1955) *Association for Supervision and Curriculum Development*, *Nursing Research*. Available at: https://doi.org/10.1097/00006199-195506000-00009.

Wiggins, G. and McTighe, J. (2005) *Understanding by Design*, *Association for Supervision and Curriculum Development*.

Wiggins, R. (2004) 'Google Storms the Webmail Market', *Searcher:Magazine for Database Professionals*, 12(7), pp. 15–21.

Wiles, R. *et al.* (2005a) 'Informed Consent in Social Research : A Literature Review ESRC National Centre for Research Methods Methods Paper No', *Methods*, pp. 1–27.

Wiles, R. *et al.* (2005b) 'Informed Consent in Social Research: A Literature Review', *NCRM Review Paper* [Preprint], (001). Available at: http://eprints.ncrm.ac.uk/85/1/MethodsReviewPaperNCRM-001.pdf.

Williams, N. (2019) 'Report For first APR', (July).

Wilson, E. (2006) 'ADS IN CONTEXT', *NMA Report*, 14(Webmail advertising).

Wohlin, C. *et al.* (2012) *Experimentation in software engineering*, *Experimentation in Software Engineering*. Available at: https://doi.org/10.1007/978-3-642-29044-2.

Wolters, P.T.. . (2018) 'The control by and rights of the data subject under the GDPR', *Journal of Internet Law*, 22(1), pp. 1–8. Available at: http://proxy.lib.sfu.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=131103593&site=ehost-live.

Wong, J.C. (2019) 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook', *The Guardian* [Preprint]. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

Wuyts, K., Scandariato, R. and Joosen, W. (2014) 'Empirical evaluation of a privacy-focused threat modeling methodology', *Journal of Systems and Software*, 96, pp. 122–138. Available at: https://doi.org/10.1016/j.jss.2014.05.075.

Yale, T. *et al.* (2019) 'Fundamental Legal Conceptions as Applied in Judicial Reasoning Author (s): Wesley Newcomb Hohfeld Stable URL : https://www.jstor.org/stable/786270', 26(8), pp. 710–770.

Yetti, D. (2021) 'An Analysis of Readability level of Reading Material in English Textbook for First Grade of Senior High School', *Journal of Education and Teaching*, 2(1), pp. 1–7. Available at: http://ejournal.uin-suska.ac.id/index.php/JETE.

Yi, M.Y. and Davis, F.D. (2003) 'Developing and validating an observational learning

model of computer software training and skill acquisition', *Information Systems Research*, 14(2), pp. 146–169. Available at: https://doi.org/10.1287/isre.14.2.146.16016.

Young, D.R., Hooker, D.T. and Freeberg, F.E. (1990) 'Informed consent documents: increasing comprehension by reducing reading level.', *Irb*, 12(3), pp. 1–5. Available at: https://doi.org/10.2307/3564107.

Zarrabi, F. *et al.* (2012a) 'A Meta-model for Legal Compliance', *CAiSE 2012 Workshops LNBIP*, (112), pp. 46–60.

Zarrabi, F. *et al.* (2012b) 'A Meta-model for Legal Compliance and Trustworthiness of Information Systems', *CAiSE 2012 Workshops LNBIP*, (112), pp. 46–60.

Zhang, K. and Katona, Z. (2012) 'Contextual Advertising', *Marketing Science*, 31(6), pp. 980–994. Available at: https://doi.org/10.1287/mksc.1120.0740.

Zhang, M., Chow, A. and Smith, H. (2020) 'COVID-19 contact-tracing apps: Analysis of the readability of privacy policies', *Journal of Medical Internet Research*, 22(12), pp. 1–6. Available at: https://doi.org/10.2196/21572.

Zhang, X. *et al.* (2020) 'Pattern-based software process modeling for dependability', *Journal of Software: Evolution and Process*, 32(9), pp. 1–21. Available at: https://doi.org/10.1002/smr.2262.

Zimmermann, A. *et al.* (2021) 'Written informed consent—translating into plain language. A pilot study', *Healthcare (Switzerland)*, 9(2). Available at: https://doi.org/10.3390/healthcare9020232.