Article

Privacy Goals for the Data Lifecycle

Jane Henriksen-Bulmer *, Cagatay Yucel, Shamal Faily and Ioannis Chalkias

Department of Computing and Informatics, Bournemouth University, Fern Barrow, Poole BH12 5BB, UK
* Correspondence: jhenriksenbulmer@bournemouth.ac.uk

Abstract: The introduction of Data Protection by Default and Design (DPbDD) brought in as part of the General Data Protection Regulation (GDPR) in 2018, has necessitated that businesses review how best to incorporate privacy into their processes in a transparent manner, so as to build trust and improve decisions around privacy best practice. To address this issue, this paper presents a 7-stage data lifecycle, supported by nine privacy goals that together, will help practitioners manage data holdings throughout data lifecycle. The resulting data lifecycle (7-DL) was created as part of the Ideal-Cities project, a Horizon-2020 Smart-city initiative, that seeks to facilitate data re-use and/or repurposed. We evaluate 7-DL through peer review and an exemplar worked example that applies the data lifecycle to a real-time life logging fire incident scenario, one of the Ideal-Cities use cases to demonstrate the applicability of the framework.

Keywords: privacy; privacy goals; data governance; privacy by design; cyber; data lifecycle; GDPR; decision making; smart city; circular economy

check for updates

Citation: Henriksen-Bulmer, J.; Yucel, C.; Faily, S.; Chalkias, I. Privacy Goals for the Data Lifecycle. *Future Internet* **2022**, *14*, 315. https://doi.org/10.3390/fi14110315

Academic Editor: Christos Kalloniatis

Received: 26 September 2022
Accepted: 29 October 2022
Published: 31 October 2022

1. Introduction

The European Union (EU) is keen to promote reuse of resources throughout the European Economic Area (EEA) and have, as part of this drive, created an initiative to promote a *"circular economy"* [1], which encompasses, among other things, data, specifically looking at how data can be reused and/or repurposed safely to provide more opportunities for creating value for businesses and citizens to become prosumers (i.e., co-creators or co-producers of data generated from their devices into smart city use) [2]. To this end, an opportunity arose for Bournemouth University (BU), to participate in a Horizon 2020 European Project, that investigates how smart city data can be reused as open data as part of the circular economy to unlock value opportunities for citizens and businesses. *Ideal-Cities* (Intelligence-Driven Urban Internet-of-Things Ecosystems for Circular, SAfe and IncLusive Smart CITIES) is a consortium of six organisations spanning multiple countries including France, Greece, Poland and the UK.

Many of the benefits from smart cities and advanced technologies stem from data, including personal data, being processed and flowing trough the technological ecosystem. This, in turn, gives rise to a number of potential cyber threats that present potential security and privacy risks to data, that those who process the data will need to consider and mitigate against. When businesses consider privacy, they will normally consider privacy from a perspective of the risk to the business of data being inadvertently released or shared unintentionally and/or without permission. However, to consider privacy risk, practitioners must also look at what are the goals they need to achieve in order to safeguard the data and preserve privacy, and this involves considering what decisions will need to be considered at each stage of the data lifecycle.

To address some of these challenges, BU's task within the Ideal-Cities project was to focus on security and privacy for the project. In order to achieve this, we sought to build on two existing privacy risk assessment frameworks, CLIFOD (ContextuaL Integrity for Open Data) [3] and the DPIA Data Wheel [4], to create a business decision support framework that could complement these and help businesses make better decisions, not just at the beginning of a project or data collection exercise, but throughout the data lifecycle. Further, the introduction of Data Protection by Default and Design (DPbDD), that was brought in as part of the General Data Protection Regulation (GDPR) in 2018, meant that any such framework would also need to be fully aligned and compliant with this new regulation.

This paper presents the resulting privacy decision support framework, a seven-stage privacy data lifecycle for data governance (7-DL) that incorporates 9 privacy goals. 7-DL and the privacy goals were developed from existing work, an analysis of existing privacy goal frameworks, and GDPR. These were adapted and amalgamated into one framework, 7-DL, designed to aid practitioners in making appropriate privacy, security and data protection decisions, and in actively managing and maintaining the privacy and security of their data holdings at all stages of the data lifecycle.

Although 7-DL was created to support decision making throughout the data lifecycle for the Ideal-Cities project, we contend these tools can be equally applied to any business to support privacy decision making. Together, 7-DL and the associated privacy goals, will allow any businesses to make informed decisions that, in turn, will help facilitate securing and safeguarding information or data throughout the data lifecycle, whilst optimising the opportunity for reusing those elements that do not contain any personally identifiable information (PII).

The rest of the paper is organised as follows. We start by discussing related work in Section 2, followed in Section 3 by a brief outline of the methodology used to conduct this study. Section 4 outlines how the Altman et. al data lifecycle [5] was adapted into a more comprehensive 7-step data lifecycle (7-DL), that is then complemented with a set of privacy goals, created to support 7-DL, based on an analysis of existing privacy and security goals in Section 5. We then align both these tools to GDPR in Section 6, followed by an evaluation that includes a peer review and an exemplar worked example in Section 7, that applies the concepts to one of the Ideal-Cities use cases, to evaluate the framework and demonstrate how the privacy goals can be used in combination with the data lifecycle developed in this paper. The paper concludes in Section 8, we answer the research question set in Section 3 and provide a summary of the contribution (Section 8.1) and a discussion of future work (Section 8.2).

2. Related Work

Businesses, and devices (e.g., smart city apps or devices), collect and use vast quantities of data, including data relating to individuals. This is classified as *'personal data' or 'personally identifiable information'* (PII) and thus, protected by law under GDPR. PII may be collected from external sources or provided voluntarily by the users (also known as the *'data subjects'*). For example, when applying for a loan with a credit agency or broker, the user (*a.k.a. the customer or data subject*), may provide the broker with details of their name, address, bank details etc. to help them obtain the loan. In the case of a smart city app, devised to assist users in an emergency (one of the use cases for Ideal-Cities), users may disclose alternate details including perhaps their location, contact details for their next of kin, and any special needs that need addressing or accommodating in an emergency (e.g., disabilities etc.).

Data, is a collection or *"set of data"*, that may be stored electronically [6]. The main purpose of data is to capture activities or events and therefore, most data is historical, unless it is used for forecasting or illustration purposes [7]. *Information*, on the other hand, is the *"knowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told"* [6], i.e., it is the meaning that may be derived from the data either through processing, decisions taken or analysis [8]. For instance, data collected may be used to offer suitable products to the user or determine suitability for credit. Hence, data that has been interpreted and analysed, turn into information that can then be used to inform decisions [9]. This means that, when a business collects information about users, each piece of information is not held as a separate stand-alone entity, rather, it is collated and processed in some way, to make it useful for the purpose of that business. Similarly, the information may be turned back into data and potentially reused for other purposes by collating it in another way or removing some of the interpreted meaning. This, therefore, can aid the business to repurpose data or indeed, analyse so they can derive meaning to serve their particular purpose. That does not mean that processing data is necessarily negative, data promises opportunities for data analytics, research and indeed, affording the business the opportunity of gaining competitive advantage through the power of data [10]. Thus, data analytics can inform business decisions and provide powerful insight to help prevent fraud, determine risk exposure, or inform strategy [11]. In the case of Ideal-Cities, data can be used to help navigate a user with limited mobility safely through a Smart City.

2.1. Data Privacy

Academic research into privacy looks at privacy either from the perspective of the individual and how they may perceive privacy, e.g., [12,13], or whether we have a right to expect privacy [14,15]. Privacy has also been considered through a technical lens looking, for example, at how technical manipulation of data can be achieved. This may involve redacting, obfuscating or removing PII [16–19]. Alternatively, privacy may be achieved through security controls, such as user authentication [20], or more secure system design [21].

Westin was the first to distinguish privacy in terms of someone's right to manage personal information, rather than autonomy or dignity. Moreover, he recognised that, just as the value of data is content dependant, any right to privacy is context dependent [22]. And it is this notion of context that asks us to consider whether users have a right to privacy around how their data is used by others [23].

2.2. Privacy Risk

According to the International Standards Office (ISO), a privacy risk can be defined the same as any other risk [24,25]. More specifically, a privacy risk should consider the probability or 'likelihood' and 'consequence' of a violation of, or the loss of, an individual's privacy. A violation of privacy occurs when privacy is lost or breached. Gavinson defined this as the *"extent to which we are known to others; the extent to which we are the subject of others' attention; and the extent to which others have physical access to us"* [26]. The loss of data privacy can occur in many ways, including; personal information being disclosed without knowledge [15,27], consent [28], through leakage, e.g., as a result of a data breach [29].

Therefore, safeguarding data privacy requires that data is obtained and handled by those who obtain it in accordance with agreed terms, and that the data is managed in a way that minimises the risk of a privacy violation, e.g., a data breach. This requires that appropriate security is applied in such a way that any potential cyber security threat is minimised or removed. To this end, however, the business must first establish what the areas of potential risk are within each stage of the data journey within the business.

2.3. Privacy Goal Modelling

One method for looking at privacy risk is through privacy goal modelling. The idea of using goals to elicit requirements or objectives has been used in requirements engineering for over 30 years [30]. This was extended to include anti-goals for security threat modelling [31], and later, to also define *"desired properties"* that required protection as security goals [32]. More recently, privacy was also introduced as an extension to this, with many of the existing privacy frameworks also reviewing privacy through privacy goals or properties. For example, the LINDDUN framework based their work on (STRIDE [32] and KAOS [31], two security goal modelling frameworks, and extended this to include privacy [33]. Essentially, privacy goals seek to ascertain the properties or aims that need protection against a particular action (i.e., 'a threat' in security terms). LINDDUN takes each privacy threat types and maps these to system elements to derive privacy requirements [34].

Similarly, IRIS (*"Integrating Requirements and Information Security"*) and CAIRIS (*"Computer Aided Integration of Requirements and Information Security"*) [35] seek to gather and visualise security requirements, vulnerabilities and threats using goal modelling, including privacy [21]. Effectively what privacy goals seek to establish are aims or properties that need protection against a particular action (in security terms 'a threat').

Another example that extended the idea of security goal modelling into privacy is the *"Privacy Safeguard"* (PRiS) framework, a privacy requirements gathering method [36] that considers 8 privacy goals (authentication, authorisation, identification, data protection, anonymity, pseudonymity, unlinkability, and unobservability), using these as organisational goals to incorporate privacy into systems and processes [37]. These goals can then be used to analyse and assess the effect and impact each of privacy goals may have on the system, thereby incorporating privacy into system design [37].

2.4. GDPR

Another way to view privacy risk is through a legal lens. The GDPR, introduced in 2018, was arguably, highly instrumental in bringing privacy into the foreground of business decision making. GDPR brought considerable change in privacy law, and introduced a series of additional and new obligations on businesses to safeguard data, and indeed the users and data subjects. Because GDPR is a regulation, it has taken effect immediately in all member states within the EU from the effective date. This means that, in contrast to a directive, which must be enacted by each member state within the EU, the regulation is legally binding in its entirety from the effective date across all member states, no enactment at national or individual Country level is necessary [38]. Article 5 of GDPR sets out 7 principles:

Principle 1: Lawfulness, fairness and transparency *Lawful* : Businesses must define the legal basis under which data is processed (Article 6 and 9): *Fair*: Data must be processed fairly, with data subjects (*'users/customers'*) interest in mind: *Transparency*: Keeping data subject(s) informed about what data processing will be done, and why (Article 12), including informing them about how the data will be used in plain, easy to understand language (Articles 13 and 14; Recital 39)

Principle 2: Purpose Limitation Establishing and communicating to the data subject the specific purpose for processing the data, before processing starts. Further, no processing beyond this original stated purpose is allowed without prior informed consent (Article 7, Recital 32)

Principle 3: Data Minimisation Data collected should be adequate, relevant and not excessive. This means you should collect minimum data needed for the specified purpose (Article 25(2))

Principle 4: Accuracy Data should be kept accurate and up to date

Principle 5: Storage Limitation Data should only be kept for as long as absolutely necessary (Recital 39); anonymise, pseudonymise and delete data as soon as it is no longer needed for the original purpose (Article 25); and securely delete and/or destroy data no longer needed

Principle 6: Integrity and confidentiality *Integrity*: Safeguard the accuracy and completeness of the data; *Confidentiality*: Process and store the data securely ensuring data is protected from harm, unauthorised or unlawful disclosure, use, modification, damage or access (Recital 39). Making sure staff are trained in how to safely and securely process data. *Security*: Ensure appropriate security measures are in place both technically and organisationally. This should include polices, processes and technical measures (Article 32)

Principle 7-Accountability the business (*"Data Processor"*) must be able to demonstrate compliance with these principles.

Through these principles, GDPR places a number of obligations on businesses, including an obligation to implement data protection by design and default (DDbDD) (Article 25), a requirement to keep a record of *"processing activities"* (Article 30) and implementing *"appropriate security and confidentiality of the personal data"* (Recital 39, Article 5(f)), along with mandatory reporting of data breaches within 72 h (Article, 33(1)). The provisions brought in by GDPR also afford data subjects (*'users'*) extensive rights including, the right to be forgotten (Article 17), and stricter rules have been placed around consent. These state that consent must be freely given, explicit (Article 7), and provided by a *"clear affirmative act"* (Recital 32) [39]. Furthermore, GDPR requires that businesses must assess privacy risk for any processing that could potentially result in "high risk" to the data subject(s) whose data is being processed (Article 35(1)) and to ensure appropriate safeguards are put in place to keep such data secure (Article 32). Thus, as part of any decision making around privacy, the legal provisions of GDPR will need to be taken into account.

2.5. Decision Theory

In decision theory, decisions were first thought to be made by *"economic man"*, who makes decisions based only on accurate information or *"organisation man"*, who makes rationally bounded decisions based on knowledge, intellect, taking into account any social or societal constraints [40]. Thus, economic man is rational, fully informed and he can therefore make objective decisions as the options available are continuous and differentiable, hence they are riskless and calculable [41] while organisation man allows for subjectivity, realising that there are no riskless choices.

An alternate decision theory is game theory, based on statistics and mathematical programming. While game theory offers little help in developing strategies, it offers rules about how to choose among a set of options [41]. Thus, it can be argued that today's economic man is likely to use risk as a way to calculate odds of an event happening or indeed, he may calculate exposure or likelihood using formulas. However, not all risks are tangible and adding a value to these requires more ingenuity than in adding some form of economic value. This is where the decision style of *"organisation man"* comes to the fore.

"Organisation man" understands that he does not know everything, instead he is assumed to consider context as part of any decision he makes. This means that in order to be objective, a decision must be made without knowing all of the facts or, indeed, having adequate detailed knowledge of the consequences of actions taken. As a result, consideration must be given to what is known, and what alternative solutions exist that could solve the problem, so as to determine the best course of action [40,42]. As part of this, Simon [40] contends that *"organisation man"* will, rather than continue searching for an *"optimum"* solution, stop the decision-making process once he finds a *satisfactory* solution.

Business Decision Making

This trend of decision making behaviour has also been found in business when management make decisions [43,44]. Accordingly, decision-making in business consists of selecting appropriate actions based on: *"evaluating alternatives for meeting an objective"* [45] which will, in turn, involve *"some random elements"* and therefore, decisions are *"subject to risk"* [46]. Thus, *"organisation man"* makes decisions based on information available, that, while not necessarily perfect, is sufficient to enable a decision to be made.

Relating this to the likely users for the output of this work, the practitioner most likely to use the framework will be *"organisation man"*, as they will be unlikely to have all facts available to them, nor will they have the option to make riskless choices. However, to establish how best to do that, we need to first understand at what points the business must make what decisions.

2.6. Data Lifecycle

Irrespective of the proposed uses of the data, once the business has data, decisions will need to be made about what to do with the data: how to manage and use the data, and whether to store or share with others. Previous work conducted has explored decision-making: prior to sharing data as open data (CLIFOD [3]), and for assessing privacy risks with the DPIA Data Wheel [4]. However, data is not just used or collected once, it is continually being processed in different scenarios. Thus, to better inform decisions made, it is helpful to first break down what is to be given consideration into manageable chunks, so that it becomes easier to understand which decisions need to be made at which stage of the data lifecycle.

Altman et al. [5] devised a data lifecycle for managing data within a business that broke data management into 5 lifecycle stages: *collection, transformation, retention, access/release and post-access*. This lifecycle applied to decision making would mean that the practitioner would, for instance, at the earliest stage of the data lifecycle, *collection*, decide, among other things, what data they are going to collect, how they are going to collect and use the data, and whether or not they need to obtain consent from the data subject while later in the data lifecycle, decisions will need to focus on other areas such as whether or not to retain or share the data.

However, we contend it is not enough to simply identify the different stages of data during the lifecycle [5], it is also necessary to establish what decisions will need to be made at each stage of the data lifecycle to facilitate effective privacy decision-making as part of the business decision-making processes.

To this end, this study considered the Altman classifications and determined that these could be equally applied to any data flow decision-making process. From this we revised the Altman lifecycle to include all aspects of data management and thereby facility full lifecycle privacy decision making (Section 4). Further, a series of privacy goals were then created to support this (Section 5), and aligned this with GDPR (Section 6).

3. Methodology

This paper took the form of a case study following Yin [47]. This case study was granted ethics approval from University Ethics Committee. The unit of analysis is *the practitioner* who must make decisions around the data.

The research question asked was: *How can we create a comprehensive privacy-specific decision making support framework that encompasses every stage of the data journey within a business?*

To answer this question, the following steps were planned:

Step 1 Adapting the Altman et al. data lifecycle [5] (Section 4)

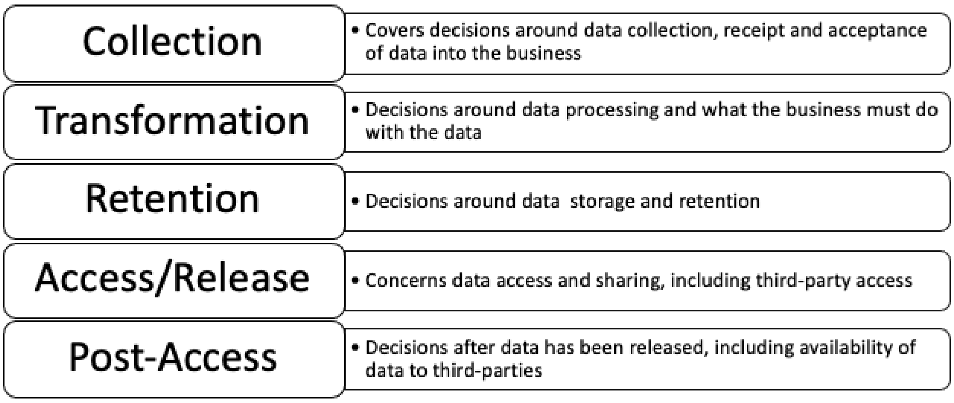
Step 2 Devising a series of Privacy Goals to support decision making and safeguard data holdings (Section 5)

Step 3 Aligning the Privacy Goals to GDPR and the data lifecycle (Section 6)

Step 4 Evaluating the lifecycle and privacy goals. This will be done, firstly by peer review of the framework and privacy goals, second, through a worked example using the life logging 'Fire incident' scenario from Ideal-Cities as the unit of analysis (Section 7).

4. Step 1-Adapting the Data Lifecycle

To frame the decision making process within a framework, this study determined that the Altman classifications (Section 2.6), will be equally applicable to any data flow within the decision-making process, including privacy decisions. Thus, as a first step to creating a privacy data lifecycle, we adapted the Altman model to provide a visual depiction of which decisions will fit where within the data lifecycle (see Figure 1).



Collection
- Covers decisions around data collection, receipt and acceptance of data into the business

Transformation
- Decisions around data processing and what the business must do with the data

Retention
- Decisions around data storage and retention

Access/Release
- Concerns data access and sharing, including third-party access

Post-Access
- Decisions after data has been released, including availability of data to third-parties

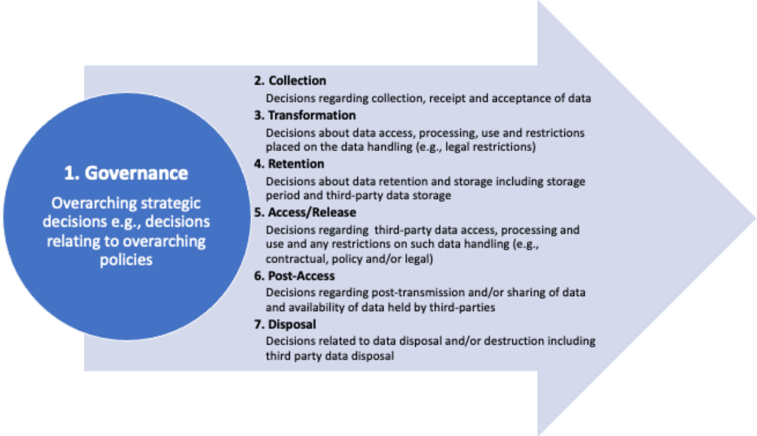
Figure 1. Adaptation of Altman's data lifecycle for decision-making [5].

Figure 1 demonstrates how the Altman data lifecycle stages can be equally applied to provide a useful division of areas within which decisions need to take place regarding data management and/or release the data.

From Altman's 5 to 7-DL

The first step involved revisiting Altman et al.'s data lifecycle [5]. The aim was to establish how this can be adapted to serve as a model for data governance that incorporates the full data journey that data being processed within a business need to make. The Altman model consists of five phases, however, there is no provision for the end of life deletion or destruction of data, or indeed for making overarching decisions that encompass a holistic view of the data, such as the creation of a suitable privacy policy etc. Thus, because the practitioner must also consider these aspects, while the Altman model covers most data handling processes that a business needs to carry out, it does not include any stages for handling data disposal or governance, two elements that, given GDPR and the new obligations this introduced, must be considered as part of any decision making around data.

To rectify this, the Altman model was expanded to include a further two further steps, resulting in a 7-stage Data Lifecycle (7-DL) for managing data privacy throughout its life with an organisation, see Figure 2.



1. Governance
Overarching strategic decisions e.g., decisions relating to overarching policies

2. Collection
Decisions regarding collection, receipt and acceptance of data

3. Transformation
Decisions about data access, processing, use and restrictions placed on the data handling (e.g., legal restrictions)

4. Retention
Decisions about data retention and storage including storage period and third-party data storage

5. Access/Release
Decisions regarding third-party data access, processing and use and any restrictions on such data handling (e.g., contractual, policy and/or legal)

6. Post-Access
Decisions regarding post-transmission and/or sharing of data and availability of data held by third-parties

7. Disposal
Decisions related to data disposal and/or destruction including third party data disposal

Figure 2. 7-stage Data Lifecycle (7-DL), adapted from Altman et al. [5].

5. Step 2-Creating a Set of Privacy Goals

To support 7-DL, a decision was taken to use the concept of *privacy goals* to further support the decision making process within the data lifecycle. The notion of having supporting *goals*, has been used for requirements gathering [30], threat modelling [32], secure system design [21] and, more recently, to support privacy risk identification and protection in system design [33,36].

The idea was to create a series of privacy goals that decision makers can use to support their decisions, so that they can ensure all identified risks have been supported by appropriate mitigation strategies at every stage of the data life journey through the business. To this end an analysis of existing standards and goal based frameworks that incorporate privacy was carried out. This analysis considered the following frameworks in depth:

PriS *"Privacy Safeguard"* a privacy requirements gathering system [36] that uses privacy requirements as organisational goals to incorporate privacy into processes and systems [37]

IRIS/CAIRIS the IRIS *"Integrating Requirements and Information Security"* and CAIRIS *"Computer Aided Integration of Requirements and Information Security"* [35] method seek to elicit and visualise security requirements, vulnerabilities and threats using goal modelling. This framework now also incorporates privacy considerations [21]

LINDDUN A privacy threat modelling framework [33]. LINDDUN stands for: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure, content Unawareness and policy and consent Non-compliance;

Pfitzmann & Hansen A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management [48]

Schleswig-Holstein DPA Studies by the Schleswig-Holstein Data Protection Authority, the Independent Centre for Privacy Protection (ICPPS) around privacy terminology and goals: [49,50];

ENISA Guidance from the European Union Agency for Network and Information Security (ENISA) around data protection and privacy goals [51] and

ISO the ISO guides for security and privacy risk [25,52].

Privacy Goal Analysis

The privacy goal analysis took each of these frameworks and looked at what each framework considered a privacy goal or principle and how they defined each goal. This resulted in 16 goals being identified between the 6 frameworks (Table 1).

Taking these 16 goals, a comparison was made to establish which of these goals could be considered privacy goals for the purpose of supporting 7-DL. For this, we began by analysing which of these were considered *privacy goals* and by how many of the frameworks. From this, it was then decided that, where the majority of the frameworks considered a goal as a *privacy goal*, that goal would be included as a supporting goal for 7-DL (see Appendix A for more detailed analysis). This resulted in the first 7 goals (no's 1–7) being included as privacy goals. The next two goals (no's 8 and 9), although only classed as goals by some of the researchers, were also included, as they represent legal obligations under GDPR. Thus, we ended up with a list of nine Privacy Goals:

Table 1. Privacy Goals Compared incl. Definitions.

No.	Goal	Mentioned in following Frameworks	Meaning
1.	Confidentiality	LINDDUN, IRIS (CAIRIS), ICPPS, ENISA-ISO mention but not as a goal	*Ensuring data is usable on demand and accessible to authorised stakeholders.*
2.	Integrity	LINDDUN, IRIS (CAIRIS), ICPPS-ENISA, PriS-ISO mention but not as a goal	*Ensuring non-repudiation and reliability for each piece of data, i.e., processing accurate, authentic, and unmodified data.*
3.	Availability	LINDDUN, IRIS (CAIRIS), ICPPS, ENISA-ISO mention but not as a goal	*Ensuring data is usable on demand and accessible to authorised stakeholders.*
4.	Unlinkability	PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010, ENISA, ICPPS	*Ensuring data cannot be sufficiently distinguished to linked across platforms or domains with similar context or purpose.*
5.	Unobservability	PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010-ICPPS mentions but not as a goal	*Ensuring no unauthorised party can observe what data or service is being utilised or performed, even if they gain access to the system.*
6.	Anonymity	LINDDUN, PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010, ENISA-ICPPS and ISO mention but not as a goal	*Obfuscating links between data and identity, i.e., the ability to distinguish any one individual from the data..*
7.	Pseudonymity	LINDDUN, PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010-ENISA, ICPPS and ISO mention but not as a goal	*Replacing identifying data with pseudonyms ensuring any links to original data cannot be made by unauthorised parties..*
8.	Intervenability	ENISA 2014, ICPPS	*Enabling data subject access and/or supervisory authority access to affect action on the records (e.g., to correct inaccuracies, request modification and/or deletion). In that way it can be seen as a safeguarding measure that must be included within any process or system involving personal data.*
9.	Transparency	ENISA 2014, ICPPS- PriS and ISO mention but not as a goal	*Openness-Providing assurance, accountability and traceability for internal and external stakeholders.*
10.	Authentication	LINDDUN, PriS - Pfitzmann and Hansen, ICPPS and ENISA mention but not as a goal	*Verifying the identity of a process, device or user*
11.	Undetectability	Pfitzmann and Hansen 2010-ICPPS mention but not as a goal	*Ensuring data is annonymised so that anonymity and undectability of the individual is preserved.* and *Ensuring data cannot be sufficiently distinguished to establish whether it exists or not.*
12.	Accountability	LINDDUN, IRIS (CAIRIS), ENISA, Pfitzmann and Hansen, ICPPS and ISO29100 mention but not as a goal	*Having someone designated as 'accountable'-ensuring that someone takes responsibility for how data is processed and that, for example, privacy goals are followed and adhered to*
13.	Identification	PriS	*This concerns user identifying themselves within a system*
14.	Data Protection	PriS	*Ensuring personal data is appropriately processed and stored*
15.	Authorisation	LINDDUN, PriS, IRIS (CAIRIS) mention but not as goal	*Ensuring user accessing a system or process has authority to do so.*
16.	Non-repudiation	LINDDUN, ENISA mentions this as a threat, not a privacy goal - ICPPS and IRIS (CAIRIS) mention but not as goal	*Proof of action, e.g., making sure that a user who processes an item of data cannot at a later stage deny having processed that item of data.*

6. Step 3-Aligning the Privacy Goals to GDPR and the Data Lifecycle

Next, while some of the final list of goals consider some aspects covered by GDPR, most of the frameworks analysed were created prior to the introduction of GDPR. Therefore, to account for this and ensure compliance with the regulation, the next piece of work involved making sure 7-DL is aligned to GDPR, so that practitioners can demonstrate they are considering their obligations under GDPR as part of 7-DL, and be confident that data is safeguarded throughout. For example, before any data is processed, governance decisions will need to be made around what data to collect, how long data will be stored for, why etc. Similarly, at first stage of doing something with the data (Stage 2 in the data lifecycle), when data is being collected, the decisions that need to be made will be focused on informing the data subject about the purpose of the data collection, how the data will be used and ensuring that consent has been obtained. Later in the lifecyle however, the decisions that need to be made may focus on whether or not to destroy or retain the data.

GDPR consist of 7 principles: Lawfulness, Fairness and Transparency (P1), Purpose Limitation (P2), Data Minimisation (P3), Accuracy (P4), Storage Limitation (P5), Integrity and Confidentiality (P6), and Accountability (P7) (Section 2.4, [39]). Thus, to ensure these principles are incorporated into 7-DL, an analysis was carried out that looked at each principle in turn to decide where within 7-DL that principle should be considered so that practitioners can be sure they have both fully safeguarded the data, and complied with GDPR throughout 7-DL.

6.1. GDPR Principle 1: Lawfulness, Fairness and Transparency

The definition of lawfulness, fairness and transparency under GDPR, is that business must ensure that any data processed has a valid legal basis for being processed (Article 5(1)(a)). GDPR then goes on to further outline the permitted legal basis (or conditions) for lawfulness in Articles 6 and 9. Further, lawfulness and fairness are discussed in Recitals, 45 (lawfulness of processing), 50 (lawfulness of processing beyond original purpose), 63 (data subject right to of access) and 138. Further, GDPR includes transparency as part of principle 1 (Article 5(1)(a)) and further considers this principle in Article 88(2) and Recitals 13, 39, 58, 60, 71, and 78 (keeping data processing activities transparent). Article 12(1) and 13(2), 14(2) and Recitals 39, 58, 60 (keeping data subjects informed). Article 43(3) and Recital 100 (establishing privacy certification mechanisms), Article 53(1) and Recital 121 (transparency of decisions made by governing authorities).

Comparing this to how the other frameworks have treated these concepts, ENISA and Schleswig-Holstein DPA have separated out transparency as a separate privacy goal, while LINDDUN and PRiS do not consider either of these concepts as privacy goals at all. The other two aspects, (lawfulness and fairness) are mentioned by ENISA and Schleswig-Holstein DPA, but not as a goal, rather, they contend these should be overriding considerations that support the protection goals [50,51]. Turning to ISO29100, ‘purpose legitimacy and specification’ are considered as part of privacy principles 2 and transparency as part of principle 7: ‘openness, transparency and notice’. Thus, in 7-DL this means that decisions around lawfulness and fairness should be considered as an overarching consideration that can influence the whole of the data lifecycle. Therefore, in 7-DL this will be incorporated into the governance stage as decisions will need to be made before data collection and processing commences and appropriate policies and procedures put in place. It will also figure as part of the Collection (7-DL:2), Transformation (7-DL:3), Access/Release (7-DL:5), and Post-Access (7-DL:6) stages to ensure data is processed in accordance with this principle.

6.2. GDPR Principle 2: Purpose Limitation

Purpose limitation involves making sure that data is only processed for the specified purpose (GDPR, Article 5(1)(b)), keeping the customer informed such purpose(s) and obtaining appropriate consent from the customer (GDPR, Article 5(1)(b)). Furthermore, any further processing beyond the originally agreed purpose, should only be done with explicit consent having been obtained from the data subject (GDPR, Articles 7 and 13(3)). This refers to businesses only processing data in accordance with specified purpose and consent (Article 5(12)(b)). For the other frameworks analysed, there are different classifications used across the different across the analysed frameworks. For example, ENISA considers purpose limitation as part of a few of the design strategies (minimise, separate and enforce), while Schleswig-Holstein DPA classifies this as a legal demand, and LINDDUN considers this one of the “soft privacy goals” stating that data should be processed “with specified purpose and consent". ISO29100 does not discuss purpose limitation directly, but it could be considered part of privacy principle 2 which considers "purpose legitimacy".

Interestingly, other frameworks have linked consent to various goals, considering consent as a legal control and link this to policy (LINDDUN),or intervenability (Schleswig-Holstein DPA and ENISA). Consent in GDPR is linked to both Principles 1 and 2 (Article 5(1)(a and b). It is defined in Article 4(11) as: "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". It also relates to Articles 6(1)(a) and 9(2)(a) which requires that consent must be obtained from the data subject. The conditions under which consent must be obtained are set out in Article 7, and Article 8 for child consent. Moreover, Article 13 explains how the data subject must be kept informed about their rights. Also discussed at length in the Recitals, e.g., Recital 32, 33 and 43, 71, 111 (informed consent), 38 (consent relating to children), 40 (data to be processed "on the basis of consent"), 42 and 43 (must be able to demonstrate consent obtained), 50, 51 and 54 (proportionate overriding the need for consent), 65 (right to withdraw consent), 68 (data portability). However, in terms of 7-DS, we agree with Schleswig-Holstein DPA's interpretation that: purpose limitation should be considered as part of a legal control that ensures processing must be carried out in accordance with agreed guidelines, and therefore, this interpretation has been adopted. Thus, in 7-DL, purpose limitation is considered to incorporate ta requirement to ensure informed consent is obtained unless overriding principles apply (e.g., vital interest, Article 6(1)(d)).

For 7-DL that means that purpose limitation will need to be considered at multiple points within the data lifecycle, meaning this must be related to stages 1, 2, 3, 5 and 6 of 7-DL, as overarching decisions about data collection and use will need to be made at 7-DL:1 (Governance) and 7-DL:2 (Collection), while processing will take place at stages 7-DL:3 (Transformation), 7-DL:5 (Access/Release) and 7-DL:6 (Post-Access) and therefore, care will need to be taken that any processing activities are carried out in accordance with this principle.

6.3. GDPR Principle 3: Data Minimisation

This refers to the requirement that only data that are actually required for the specified purpose should be processed and deleted or anonymised as soon as is practicable (see principle 6). GDPR considers data minimisation as one of the overarching principles (Article 5(1)(c)), and also as part of Data Protection by Default and Design (Articles, 25(1)), 47(2)(d), and 89(1) and discussed in Recital 156 (supervision authorities to enforce). The term data minimisation refers to the requirement that only data that are actually required for the specified purpose should be processed and deleted or anonymised as soon as is practicable. Similarly, ISO 29100 has included this as privacy protection goal number 4. ENISA, LINDDUN and Schleswig-Holstein DPA consider this a a data protection principle. Schleswig-Holstein DPA suggest that processors should consider not collecting such data in the first place or, if they really do need the data, deleting the data "as soon as possible" after use. LINDDUN considers data minimisation a data protection goal, describing this as an element of "content awareness" which involves making sure the data subject is aware what is collected, what the data is used for and how it will be used. It is interesting to note the different interpretations of concepts across the frameworks analysed. For example, LINDDUN considers data minimisation part of user awareness and keeping the data subject informed which, for others, has been incorporated within the goal of transparency. Overall, most of the frameworks agree this concept is an important part and certainly, for decision making, while this may not be a privacy goal, it does need to be considered as part of all of the stages within 7-DS. For example, at data collection, businesses will need to make decisions about what data they collect, whether they really need the data, and how such data will be processed and by who.

This means that data minimisation must be considered as part of every stage within 7-DL as consideration needs to be give to what data, and how much of it, is collected (7-DL:2), processed (7-DL:3), shared (7-DL:5 and 6),or stored (7-DL:4 and 7). This, in turn, then requires that any procedures or policies also reflect this, hence, 7-DL:1 will also need to be invoked.

6.4. GDPR Principle 4: Accuracy

While this is one of the main principles of GDPR (Article 5(1)(d)), upon reading the regulation, it was noted that this principle is considered predominantly from the perspective of the rights of the data subject, which, as discussed above, in the other frameworks is covered as part of intervenability, or as part of integrity (LINDDUN), while ISO29100 has this as one of the data privacy principles, Principle 6 (accuracy and quality). PriS and Hansen et al. do not consider this as a goal, while ENISA considers accuracy as one of the "procedural safeguards" within the data lifecycle.

For decision making, while accuracy is an important aspect that should (and must) be maintained, it is argued that this relates to the processing action(s), rather than the decision making per se. Alternatively, it could be argued that, to ensure that accuracy is upheld, there needs to be direction from Management, stipulating that accuracy should be facilitated and maintained and therefore, this belongs within the first stage of 7-DS, Governance as well as the 2nd and 3rd stage, Collection and Transformation, and the 5th stage, Access/Release where decisions that need to be made around sharing of the data and therefore, how accuracy will be maintained as part of any sharing agreement(s) made.

6.5. GDPR Principle 5: Storage Limitation

Storage limitation (Article 5(1)(e)) requires that data is kept no longer than absolutely necessary and destroyed or anonymised as soon as possible after processing has been completed. The regulation also considers this in Article 6(3) (justification of data storing periods), 18, 23, 25(2), 28, 47 and Recital 45. Interestingly, none of the other frameworks consider storage limitation as a privacy goal. Rather, if they discuss storage at all, it is in relation to processing operations (ISO29100) or storage locations (Hansen et al.). Looking at this therefore, in a bit more detail, when GDPR talks about storage limitation, it actually relates this to the obligation to not keep personal data in a format that allows for identification for longer than absolutely necessary. Thus, in terms of decision making, for 7-DL this principle needs to be considered as part of Governance (7-DL:1), Retention (7-DL:4), Access/Release (7-DL:5) and, Disposal (7:DL:7).

6.6. GDPR Principle 6: Integrity and Confidentiality

For privacy, the concepts of integrity and confidentiality are considered as part of GDPR Principle 6. It is defined in Article 5(1)(f) as ensuring data is: "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". In addition, Article 32 clarifies the security aspects and which are also mentioned in Recitals: 39 (lawful processing), 49 (proportionality and necessity), 75 (risks to data subject), 83 (requirement of business to assess and evaluate privacy risk), 85 (requirement to notify authorities in event of data breach) and 112 (data transfer obligations). Availability is not incorporated as a GDPR principle although it is discussed in relation to the security of processing in Article 32(1)(b and c) and in Recitals: 49 (proportionality and necessity) and 108 (data subject enforceability rights).

Applying this to 7-DL, it was decided that, because the *aim* of the privacy goals is to ensure that privacy is maintained, this GDPR principle is the optimal area to place all the privacy goals. This will ensure that any security measures implemented to protect the data (and therefore, privacy), will consider both the security and privacy aspects and thus, aid the practitioner in meeting both privacy-by-design and security-by-design principles in their risk considerations. Therefore, it makes sense to insert the nine privacy goals as subgoals to this principle. With the following goals, privacy can be incorporated by design and default (Article 25), into both the decision making process, and the setting up of appropriate security principles which they will help to facilitate this is met (as depicted in Table 2):

i Confidentiality
ii Integrity
iii Availability
iv Unlinkability
v Unobservability/Undetectability
vi Anonymity
vii Pseudonymity
viii Intervenability
iv Transparency

Table 2. Final Privacy Goals.

1. Confidentiality	6. Anonymity
2. Integrity	7. Pseudonymity
3. Availability	8. Intervenability
4. Unlinkability	9. Transparency
5. Unobservability/Undetectability	

6.7. GDPR Principle 7: Accountability

GDPR Principle 7 (Article 5(2)), *Accountability* places an obligation on the business to not only be accountable, but also to be able to demonstrate compliance with the regulation. This applies both in terms of being accountable to their stakeholders and users (*the data subjects*), and any third-party that might process the data on behalf of the data controller (Article 28(3)), but also the relevant Data Protection Authority (DPA) in charge of overseeing GDPR within a member state. For the DPA this requires that the business maintains a record of their processing activities (GDPR, Recital 82), including details of the data they collect and why (Article 30), and provide the DPA with any information requested as part of any investigation carried out (GDPR, Article 57). For the customers accountability requires that the business is open and transparent about their data processing practices and providing users with a mechanism for asserting their rights, e.g., should they wish to assert their rights in relation to data pertaining to them (Articles 16–22) this information is available for them to see.

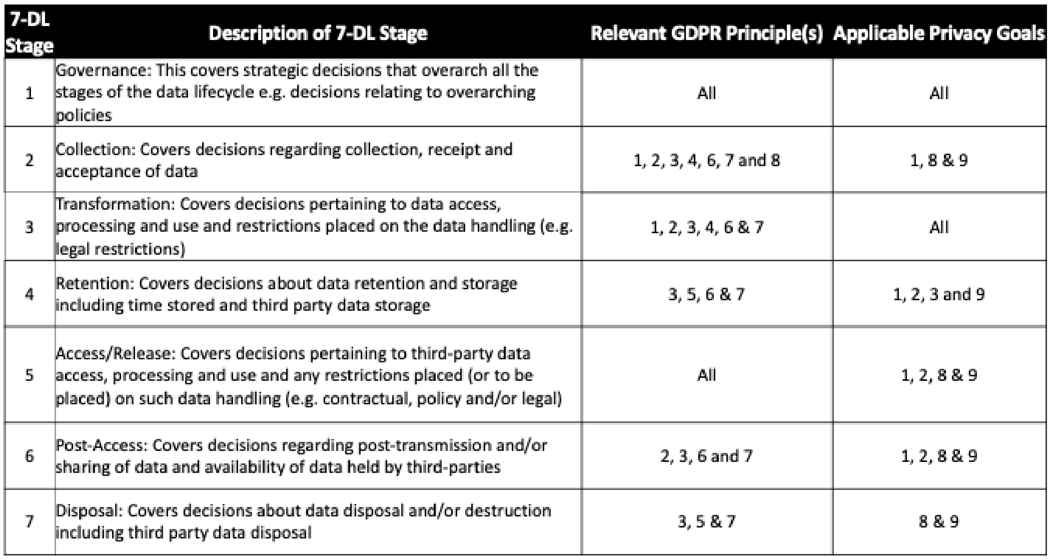
Therefore, for 7-DL, the goal of accountability has been linked in with transparency (Privacy Goal 9) which, in turn, then involves considering three aspects: ensuring customers are kept informed, being open and transparent in how the business intends to use the data (thus, providing assurance, accountability and traceability), and being transparent in how decision are made by the business. Transparency applies for this scenario as the business will need to be open and honest with the customer about why they are collecting the data, how long it will be kept for and for what purposes the data will be used (GDPR, Article 13). They can do this by having a clear privacy policy, written in plain, easy to understand language (GDPR, Recital 39, 7-DL:1). In addition, the business will need to be transparent in their data collection procedures and recording what data they collect and why (Article 30) so that, should the data subject wish to assert their rights in relation to data pertaining to them (Articles 16–22), or indeed, the authorities wish to inspect (GDPR, Article 31), this information is available for them to see (Privacy Goal 8). As regards the supervisory authorities, the business must keep a record of their processing activities (GDPR, Recital 82), including details of the data they collect and why (Article 30), and provide them with any information requested as part of any investigation carried out by the Supervisory Authority (GDPR, Article 57). This means that accountability must be considered first and foremost, a Governance (7-DL:1) aspect that must be considered. However, it will equally apply to each of the other stages as any intervention from the data subject or the Supervisory Authorities might affect any stage within the data lifecycle. Therefore, this has been included in all the stages of 7-DL.

6.8. GDPR Principle "8": Proportionality

Proportionality requires that any processing that may result in limitation on any of the rights of the individual must be justified. The principle of proportionality is discussed in Recital 4, 156, and 170. While not 'officially' a GDPR principle, this is an aspect that practitioners are asked to consider as part of any Data Protection Impact Assessment (DPIA) they conduct in relation to "the necessity and proportionality of the processing operations" (Article 35(7)(b)). Thus, for the purposes of this analysis we have referred to this as the 8th principle of GDPR and stage 1 of 7-DL, Governance and stage 2, Collection, as practitioners must ensure that any measure(s) taken in processing the data do not disproportionally limit the rights of the data subject.

6.9. Final Mapping of GDPR to 7-DL and the Privacy Goals

To recap, in Figure 3, a visual mapping of how the privacy goals were embedded into GDPR is presented. This shows where each GDPR principle needs to be considered within 7-DL.



7-DL Stage	Description of 7-DL Stage	Relevant GDPR Principle(s)	Applicable Privacy Goals
1	Governance: This covers strategic decisions that overarch all the stages of the data lifecycle e.g. decisions relating to overarching policies	All	All
2	Collection: Covers decisions regarding collection, receipt and acceptance of data	1, 2, 3, 4, 6, 7 and 8	1, 8 & 9
3	Transformation: Covers decisions pertaining to data access, processing and use and restrictions placed on the data handling (e.g. legal restrictions)	1, 2, 3, 4, 6 & 7	All
4	Retention: Covers decisions about data retention and storage including time stored and third party data storage	3, 5, 6 & 7	1, 2, 3 and 9
5	Access/Release: Covers decisions pertaining to third-party data access, processing and use and any restrictions placed (or to be placed) on such data handling (e.g. contractual, policy and/or legal)	All	1, 2, 8 & 9
6	Post-Access: Covers decisions regarding post-transmission and/or sharing of data and availability of data held by third-parties	2, 3, 6 and 7	1, 2, 8 & 9
7	Disposal: Covers decisions about data disposal and/or destruction including third party data disposal	3, 5 & 7	8 & 9

Figure 3. Mapping GDPR principles to 7-DL and the Privacy Goals.

Using these privacy goals as part of each stage of the 7-DL, will allow businesses to make informed decisions at every stage of the data lifecycle relating to the data. This, in turn, will help them identify any potential privacy threats and put in place suitable safeguards and security measures to ensure the privacy goal is met so that the threat cannot be realised.

7. Step 4-Evaluating the 7-DL Framework and the Privacy Goals

7.1. Peer Evaluation

Once the privacy goals had been agreed and identified, a spreadsheet was used to present the 7-DL framework and associated privacy goals for evaluation. The format of the evaluation was to ask 9 evaluators, divided into three groups based on expertise, to review and comment on these.

Within each group we sent the spreadsheet to the following evaluators from three different peer demographics to capture differing levels of expertise and perspective as follows:

Academics Three academics were asked to review. The evaluators had expertise in security, IT and computing, and requirements engineering, respectively

Practitioners Three practitioners evaluated the list: a Data Protection Officer (DPO), an IT Consultant, and an IT Security Manager

Student Peers The last group of evaluators were three PhD students who study security, computing, and risk, respectively.

Most of the feedback received from these three groups consisted of minor corrections and suggestions for amendments. Overall, they all agreed that incorporating a set of privacy goals within 7-DL is an effective way to ensure both data privacy and security is fully considered as part of 7-DL. Peer reviewers considered that the explanations provided were *"informative and conducive to understanding how this might work"* (R5). As regards to the privacy goals, one practitioner responded with some minor rephrasing of wordings, commenting: *"... it looks good and captures everything that we, the InfoSec team, would look for. I think seeing it "used in anger" will be a really useful exercise and I can't wait to see the outcomes"* (R3).

7.2. Ideal-Cities-Worked Example

To illustrate how these can be used to support decision making throughout 7-DL, the privacy goals are evaluated with the use of a worked example. This example will look at each of the privacy goals and explain how these might be applied in practice to help readers understand how they can put the framework into context and apply this to their business. This worked example will consider one of the Ideal-Cities circularity use cases, created as part of the project data management plan.

The use case scenario that will be used is the *life logging "Fire Incident"* use case from the Ideal-Cities project [53]. This use case was one of the pilot use cases trialled as part of the project's evaluation. Its aim is *increasing citizen safety through life logging and location information*. In this use case, the idea is that a user reports a fire in real-time (using the fire evacuation app). Users can report an incident either manually or through a GPS locator embedded within the app. To support the ability to use the GPS locator, a series of QR codes for each location are pre-installed in strategic locations throughout the building. Once a user has reported an incident, users within the affected building or within close vicinity of that building, will be notified and advised to evacuate the area. In the pilot trial case, the project used pre-existing QR stickers on doors within the buildings to facilitate location GPS and to record pre-determined evaluation point locations for each building so that users can be directed accordingly.

To demonstrate how to align this use case with 7-DL, we will describe each stage in 7-DL in turn in relation to the use case, 7-DL, GDPR and the privacy goals.

The data flow diagram presented in Figure 4 provides a full overview of the worked example. The figure is designed to depict the flow of the data among the elements of the scenario and the framework connections as the data flow. Steps *7-DL1: Governance* and *7-DL7: Disposal* are not tagged into any flow or the process since the governance step covers all the decisions that have been made in this diagram and the disposal step is a post consideration, also being one of the crucial steps of the framework.

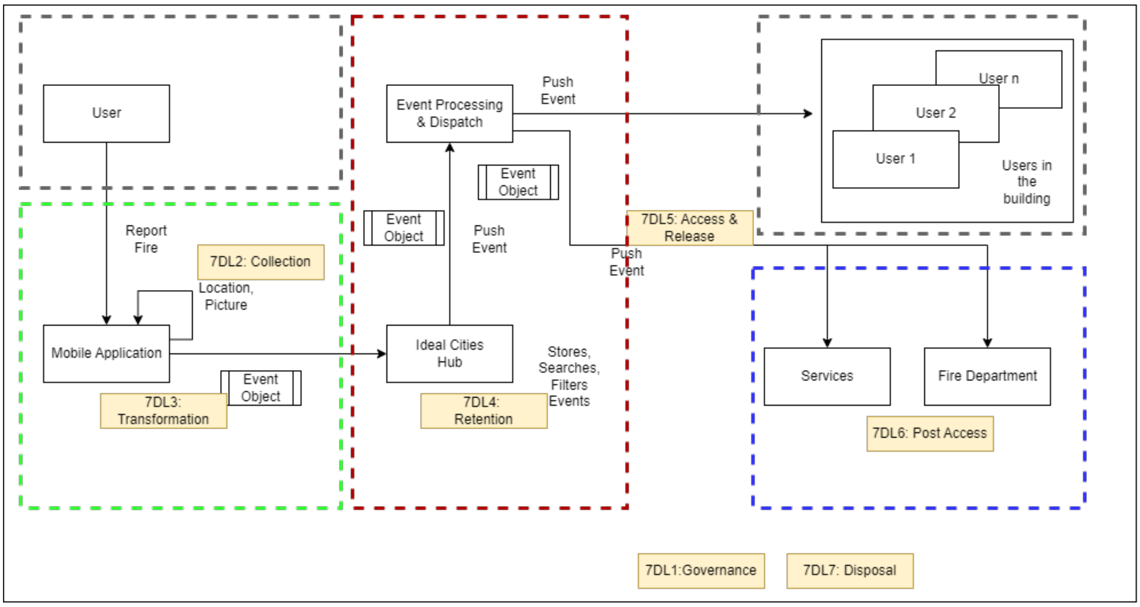


Figure 4. Data flow diagram for the worked example.

The use case data flow starts with the user initiating the fire event by reporting the fire using the application. Immediately after this action, the location information from the GPS access of the mobile device and a picture from the event have been collected following the *7-DL2: Collection* step. After the collection, the flow proceeds with the transformation of the collected data into an event object. This step follows the *7-DL3: Transformation* considerations of the framework. Then, the created event for the incident is stored, filtered, and traced in the Ideal-Cities Hub which fulfils the *7-DL4: Retention* steps. The event information is then pushed to the users in the same building, related services and the fire department utilising the *-DL5: Access and Release*. Further post access of this event by the fire departments and the services and consideration of the post access is given with the *7-DL6: Post Access* step of the framework. In the next sections, one can find the 'step-by-step' explanation of the data flow and the framework.

The dashed boxes on Figure 4 depict the trust boundaries of the worked example. Main distinctions between trust boundaries can be seen between independent computation units where the data flows. The initial trust boundary alternation (Green Box) is when the data is being captured on the mobile device from the user, as several considerations come into play regarding trust, such as the security posture of the mobile device or installed applications on the mobile device. As the data moves towards the Ideal Cities Hub identities towards the data flow diagram, the trust boundary changes in accordance. As can be seen in the boundary defining Ideal Cities Hub (Red Box), information processing and event dispatching is considered within the same boundary. This reflects on the governance of the data within the Ideal Cities' entities. Another change in the trust boundaries resides from Ideal Cities Hub to the various entities of the data flow diagram. Fire Department or other services are grouped into another trust boundary and depicted with the Blue Box on Figure 4. Push events returning to the other users of the hub are considered as the same trust boundary as the initial user and depicted with a grey box on Figure 4.

7.3. 7-DL:1-Governance

Governance should cover overarching strategic decisions for all stages of the data lifecycle. For the Ideal-Cities project, the DPIA Data Wheel created in earlier work [54] was adopted at an early stage of the project, as the vehicle for conducting data protection impact assessments (DPIAs) as part of the privacy risk assessment framework to be used within the project. This framework had already been devised and proven applicable to different use cases and scenarios [4]. From this, further work was carried out as explained in this paper, to create a supporting decision making framework (7-DL) that could be used within the project for supporting practitioners in decision making throughout the data lifecycle.

The first stage of 7-DL involves data governance, which covers decisions that overarch all the stages of the data lifecycle. Therefore, by extension, this will also involve consideration of all the privacy goals identified. For our life logging scenario this means that, for example, all of the privacy goals will need to be considered when creating data protection and security policies surrounding how the app will collect data and how this data will be managed for the use case, making sure a Data Protection Officer (DPO) is assigned and that appropriate data subject request procedures are put in place (Privacy Goal 8, Intervenability).

7.4. 7-DL:2-Collection

Collection considers any decisions pertaining to the collection, receipt and/or acceptance of data within the business. For the life logging scenario, at the collection stage, Privacy Goal 1 dictates that there must be justification for collecting data from citizens (a.k.a. the data subject(s)). Here, the legal basis should be consent (Article 6(1)(a)) or, if necessary, in an emergency situation where the citizen's life may be in peril and consent has not been obtained, "vital interest" (Article 6(1)(d) can be used. Fairness requires that the citizen understands and has been informed of the purpose of the data collection and how the data will be used within the life logging scenario, who it will be shared with (Privacy Goal 9) and giving the citizen the opportunity to opt out of data collection as part of the contract between the citizen and the project (Privacy Goal 8). Accuracy requires that the collected data is correct which means the person collecting the data must take care to note down the information correctly or, in the case of the life logging scenario, the citizen themselves, need to check that they input the information correctly and update as needed. Purpose limitation and data minimisation dictate that data collected should only be used in accordance with the specified, agreed purpose(s) and any reuse will required consent before the data can be shared. Integrity and confidentiality refer to ensuring the data is collected appropriately, using recognised techniques, maintaining the confidentiality of the citizen (Privacy Goal 1). In this scenario, the citizen themselves will input their own information into the app. This means that they are responsible for checking the accuracy of information input themselves and for only entering data they are happy to share with the app. There will need to be settings available within the app to allow citizens choices around which elements of data can and cannot be shared, stored and used (Privacy Goals 1, 8 and 9).

7.5. 7-DL:3-Transformation

At transformation stage, decisions regarding data processing and use, and any restrictions placed on how data is processed must be considered. For the life logging scenario, transformation concerns handling of the data (part of the act of *processing* under GDPR, Article 4(2)). In terms of processing, this refers to those who manage the data and the app and how they process the data which means a lot of decisions will need to be made around how the data is processed (including by whom and to what extent). First of all, those who process the data on behalf of the project, will need to be trained on GDPR and the privacy goals, to ensure they understand their obligations. This, arguably, could also be considered a governance decision as any such training will need to encompass all aspects of data processing and sharing. However, this is the first of potential interactions for those who work with the data while processing. There are a number of potential risk in this phase (sometimes referred to as insider threat) that can be avoided by ensuring those who work with the data understand what they can and cannot do with the data and how this might affect both themselves, their employer and the data subjects whose data they are processing.

Next, each of the principles within GDPR will apply to data processing. Lawfulness requires that data is processed in accordance with GDPR principles, in a fair and transparent manner (Article 5(1)(a)), while purpose limitation (Article 5(1)(b) seeks to ensure that data is only processed in accordance with agreed terms (Privacy Goals 8 and 9). This means whatever decisions have been made at the data collection stage by the citizens must be respected and followed. So, if for example, the citizen has opted to not share their location details beyond the time spent in the building, a facility must be made available to select what data can be shared, with whom and for what period of time (e.g., only while in the building, continually, or not at all). Data minimisation requires that only strictly necessary data is processed (Article 5(1)(c)). This means that, if the citizen is not in the building, they do not need to receive a notification of the incident. Accuracy requires that data is kept up to date (Article 5(1)(d)), and integrity and confidentiality (Article 5(1)(e)) requires that data is processed securely including, for example, implementing effective access controls to ensure data cannot be accessed without authorisation. This means that data should be available as needed to those who are authorised to handle the data (Privacy Goal 3), while maintaining all of the other privacy goals. It also means that Confidentiality (Privacy Goal 1) and integrity (Privacy Goal 2) must be maintained, while ensuring unlinkability (Privacy Goal 4) and unobservability (Privacy Goal 5) to any user not authorised to view or process the data. This may require data to be anonymised (Privacy Goal 6) or pseudonymised (Privacy Goal 8) as part of the processing. Finally, interveneability (Privacy Goal 8) and transparency (Privacy Goal 9) requires that either the citizen (or indeed, the supervisory authorities) must be able to intervene at any point should the need arise or, if they so wish.

7.6. 7-DL:4-Retention

At the retention stage, decisions concerning whether and how any data is stored must be considered. This includes decisions regarding, what, how, where and for how long data is retained, as well as third-party data storage. While the decision that needs to be made for the life logging scenario will affect data availability (Privacy Goal 3), and potentially the quality of the data available, any decision at this stage, must be informed by taking into account any consent given by citizens (7-DL:2, Privacy Goal 1), and the agreed purposes for which the data is processed (7-DL:3, Privacy Goal 9). Therefore, in the life logging scenario, this means that data retention should determine which elements of the data collected and processed, if any, should be stored within the system and for how long. Transparency requires that citizens must be informed about the length of time data will be retained for, this can be done through the privacy policy and/or contract with the citizen (Privacy Goal 9). This requires that data minimisation is considered so that only necessary, consented to, data is stored, for the agreed/specified period of time only. Once those elements have been established, the way the data is stored must ensure that integrity and confidentiality is maintained (Privacy Goals 1 and 2).

7.7. 7-DL:5-Access/Release

The Access/Release stage is where decisions are made as to whether any third-parties require and/or are granted access to the data. This should cover all types of access, whether for viewing only or for processing purposes in accordance with the wishes of the citizen. This means that, where, for example, the citizen has agreed (*consented*) to allow their data to be shared beyond the original use within the app, then, any on-sharing of the data must align with the level of consent obtained the data collection stage. This, in turn, means that where such data is to be shared, decisions will also need to cover the use and any restrictions placed (or to be placed) on such data sharing, including the setting up of contracts between stakeholders. This aspect will come into play if the project plans to share the data with anyone outside the business, such as other smart city operators. As part of this transparency will dictate that the contact should be clear on what the third-party can do with the data and where the boundaries lie. Accountability dictates that the contact should be made available to Supervision Authorities or other affected stakeholder, such as the data subject's appointed representative (GDPR, Article 80), where requested. For the life logging scenario, this requires that the data controller (Ideal-Cities) considers who, if anyone, outside the project, will need to be able to access the data and, and for what purpose. If it is determined that third-party access will be required, then the nature of that access will need to also be decided, will they have view only access or will they be able to manipulate the data for example. As part of this, consideration also needs to be given to whether the data can/will be shared with third-parties and therefore, this decision should also take into account what the data subject has consented to (or not, Privacy Goals 8 and 9). If consent has been obtained, other considerations that will need to be determined and incorporated into any contract between parties, include ensuring consent choices of the data subject as to the extent of sharing allowed, and decisions are made around the logistics of such sharing, including how that third-party must maintain the confidentiality (Privacy Goal 1), and integrity (Privacy Goal 2) of the data and the citizens and their data.

7.8. 7-DL:6-Post-Access

Once data has been shared, the post-access stage is where decisions concerning any post-transmission matters including the ability of the citizen to exercise their rights, whether further on-sharing can be permitted (again, this will depend on consent obtained at data collection stage) and availability of data held by third-parties who process or access the data need to be made. For the life logging scenarios, where data is shared with a third-party, if that third-party will have access to process the data, (e.g., where the business uses a third-party business to process all their orders), then lawfulness dictates that a contract must be in place between the data controller (*Ideal-Cities*) and the data processor (*the other party* (Article 28(3)). This must cover all aspects of GDPR including, purpose limitation, on-sharing and data minimisation which dictates that any data shared are released only to be used for the agreed purpose(s) consented to, and only necessary data for can be released for that purpose. Accuracy, accountability, integrity and confidentiality require that any third-parties that receive, and subsequently process the data is contractually bound to process the data in accordance with GDPR, for the purposes consented to by the citizens only (Privacy Goals 1, 2, 8 and 9). Further, this contract should specify exactly what that third-party may or may not do with the data GDPR, Article 28(3)). Further, where a third-party is engaged to process the data on behalf of the project, the third-party must, upon request, fully collaborate with the project in putting together a complete response to any request from the citizen to exercise their rights under GDPR (GDPR, Article 28(3)(e)). Therefore, Ideal-Cities must ensure that this is captured within any data sharing contracts set up with third parties (Section 7.3).

7.9. 7-DL:7-Disposal

At disposal, decisions about when and how data is disposed off or destroyed, including third-party data disposal are made. This relates directly to data retention, where any data is retained as part of 7-DL:4. When the agreed time limit has been reached (and no valid constraints exist that require continued storage, e.g., for a minimum statutory period) data must be disposed of. Such disposal must be in accordance with appropriate security controls and procedures as set out in the Privacy Goals. The faster the project can move to either fully anonymise or dispose of the data, the better (GDPR, Articles: 5(1)(e)). Further, The citizen can request that data related to them to be deleted or removed from the records (GDPR, Article 12 and 17, Privacy Goals 8 and 9). Also, if the citizen has placed a requests for their data to be deleted, the project must inform any third-party the data has been shared with and ask them to also delete the data and/or erase any links they have to such data that have been shared with them about the customer (GDPR, Recital 66, Article 12). This means that the Ideal-Cities project will need to decide how they will deal with any such requests and set up processes accordingly, bringing us back full circle to Governance (7-DL:1) where appropriate policies and procedures must be created to account for this.

Thus, this worked example demonstrates how a business can use 7-DL and the associated privacy goals in a holistic manner, as an overarching privacy risk tool to assess their data assets and how best to protect these against potential threats. Alternatively, these can be used as a complementary risk assessment tool to support the implementation of privacy by design and default (GDPR, Article 25), into every process the business carries out, thereby also facilitating improved security-by-design.

8. Conclusions and Future Work

In this study we asked *How can we create a comprehensive privacy-specific decision making support framework that encompasses every stage of the data journey within a business?* To answer that question, we adapted an existing 5-step data lifecycle for decision-making [5] to create a seven-stage data lifecycle (7-DL, (Figure 2) and a set of 9 privacy goals (Figure 2) that are also aligned with current statutory obligations (GDPR). 7-DL incorporates all aspects of data management from collection through to disposal and together, these tools enable the business to proactively make decisions about their data holdings throughout the data lifecycle. The 7-DL Data Governance Lifecycle Framework was evaluated first, by 3 independent sets of peers (academics, practitioners and student peers, Section 7.1). Second, we provided an exemplar worked example from the Ideal-Cities project to demonstrate how this can be applied in practice in 7-DL (Section 7.2).

8.1. Contribution

This paper contributes to the contemporary literature by presenting the integration of the privacy goals with the data lifecycle, thus constructing the 7-DL Data Governance Lifecycle Framework. In doing so, we have demonstrated how organisations can use this framework to improve decision making around privacy risk and, as part of this, facilitate that appropriate security measures are put in place at each stage of the data lifecycle, from collection through to disposal.

To further strengthen and evidence the contribution of this research, we also applied the framework to a real-time example scenario and the GDPR compliance has been elucidated in the worked example section. The worked example took a use case from the Ideal-Cities project (the fire incident life logging use case) thereby demonstrating how businesses can consider privacy, not as an afterthought, but continuously, as part of the data lifecycle. Furthermore, once applied, the framework can be used as an automation of compliance (i.e., consent form checks at every request–7-DL2 or sanitisation checks at every software object creation–7-DL:4) or as a basis for risk assessment automation, as the framework is capable of integrating inherently to the business processes.

8.2. Future Work

Future work will look at how 7-DL and the nine privacy goals can be aligned with the business processes and form an integral part of the organisational risk assessment procedures. We also plan to look at how the whole process can be automated to improve privacy and security by design and default.

Author Contributions: Conceptualization, J.H.-B. and S.F.; methodology, J.H.-B.; validation, J.H.-B., C.Y. and I.C.; formal analysis, J.H.-B., C.Y.; investigation, J.H.-B.; resources, Ideal-Cities; writing—original draft preparation, J.H.-B.; writing—review and editing, J.H.-B., C.Y. and I.C.; visualisation, J.H.-B., C.Y. and I.C.; supervision, S.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from the H2020-MSCA-RISE-2017 project, under the grant agreement no 778228 (IDEAL-CITIES).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable, the study does not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

7-DL	7-stage Data Lifecycle
BU	Bournemouth University
CAIRIS	Computer Aided Integration of Requirements and Information Security
CLIFOD	ContextuaL Integrity for Open Data
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPbDD	Data Protection by Default and Design
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
Ideal-Cities	Intelligence-Driven Urban Internet-of-Things Ecosystems for Circular, SAfe and IncLusive Smart CITIES
IRIS	Integrating Requirements and Information Security
ISO	International Standards Office
PII	Personally identifiable information
PriS	Privacy Safeguard
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure, content Unawareness and policy and consent Non-compliance

Appendix A.

Table A1. Privacy Goal Comparison Table.

No.	Goal	Mentioned in Following Frameworks	Privacy Meaning	Inclusion/Exclusion
1.	Confidentiality	LINDDUN, IRIS (CAIRIS), ICPPS, ENISA - ISO mention but not as a goal	*Ensuring data is usable on demand and accessible to authorised stakeholders.*	Part of the CIA triangle (Confidentiality, Integrity and Availability), widely accepted as standard practice to include for both security and privacy [51]. Included as a Privacy Goal
2.	Integrity	LINDDUN, IRIS (CAIRIS), ICPPS - ENISA, PriS - ISO mention but not as a goal	*Ensuring non-repudiation and reliability for each piece of data, i.e., processing accurate, authentic, and unmodified data.*	Confidentiality, Integrity and Availability form part of the CIA triad in security terms [55]. Included as a Privacy Goal
3.	Availability	LINDDUN, IRIS (CAIRIS), ICPPS, ENISA - ISO mention but not as a goal	*Ensuring data is usable on demand and accessible to authorised stakeholders.*	Part of the CIA triad [55]. ENISA, Hansen et al. and LINDDUN discuss these concepts as 'classic' security properties or protection goals with similar meanings for privacy and security. Availability, however, has a slightly different meaning in terms of privacy. In security terms this partly refers to the availability of the system (e.g., uptime) and partly availability of the data. In privacy terms, this relates to the availability of the data and/or being able to access the data as required (assuming, of course, the user is authorised to access the data). Included as a Privacy Goal
4.	Unlinkability	PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010, ENISA, ICPPS	*Ensuring data cannot be sufficiently distinguished to linked across platforms or domains with similar context or purpose.*	ENISA considers this one of the "privacy protection goals" while Pfitzmann and Hansen refer to this as one of the data protection goals, linking this to necessity and data minimisation. Included as a Privacy Goal

Table A1. *Cont.*

No.	Goal	Mentioned in Following Frameworks	Privacy Meaning	Inclusion/Exclusion
5.	Unobservability	PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010-ICPPS mentions but not as a goal	*Ensuring no unauthorised party can observe what data or service is being utilised or performed, even if they gain access to the system.*	Included as 7-DL Privacy Goal with *Undetectability* (see Line 11). In terms of data, both are mechanisms for hiding information to facilitate the unobservability and undetectability of the data concerning the individual data subject. It could be argued these should be split into two separate goals. The reason these two have been grouped in 7-DL is because, unobservability refers to whether the users' actions (e.g., sending or receiving) are observable and ensuring that the data itself cannot be observed either. This, arguably, includes undetectability as, if an attacker or unauthorised person, cannot observe then they cannot detect, thus, these terms have been grouped together.
6.	Anonymity	LINDDUN, PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010, ENISA-ICPPS and ISO mention but not as a goal	*Obfuscating links between data and identity, i.e., the ability to distinguish any one individual from the data.*	GDPR discusses anonymisation in relation to different communication and data processing activities within system but then goes on to say that, once data has been anonymised, it is no longer subject to data protection regulation (Recital 26). Included as a Privacy Goal.
7.	Pseudonymity	LINDDUN, PriS, IRIS (CAIRIS), Pfitzmann and Hansen 2010- ENISA, ICPPS and ISO mention but not as a goal	*Replacing identifying data with pseudonyms ensuring any links to original data cannot be made by unauthorised parties..*	GDPR discusses this in term of pseudonymisation as a means of achieving confidentiality, defining this as: "Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person" (Article 4(5). However, GDPR considers that pseudonymised data still poses a privacy risk (Recitals 75 and 85) and therefore, will remain classed as personal data after pseudonymisation has been applied (Recital 26). Included as a Privacy Goal
8.	Intervenability	ENISA 2014, ICPPS	*Enabling data subject access and/or supervisory authority access to affect action on the records (e.g., to correct inaccuracies, request modification and/or deletion). In that way it can be seen as a safeguarding measure that must be included within any process or system involving personal data.*	ENISA and Hansen et al. have made intervenability a separate privacy goal, while ISO29100 take a slightly different approach in that they incorporate this in privacy principle 7, "openness, transparency and notice", thus, considering this part of transparency. Thus, intervenability will come into play as part of all the aspects of the data lifecycle where decisions need to be made about the data, internal, or indeed outside, the business (e.g., with third parties), including the accuracy of the data they collect and process. This, in turn, means that any affected stakeholder(s) (data subject or authorities) should be able to intervene at any stage of the data lifecycle. Requirement for compliance with GDPR and therefore included as a Privacy Goal
9.	Transparency	ENISA 2014, ICPPS- PriS and ISO mention but not as a goal	*Openness-Providing assurance, accountability and traceability for internal and external stakeholders.*	Requirement for compliance with GDPR and therefore included Included as a Privacy Goal

Table A1. *Cont.*

No.	Goal	Mentioned in Following Frameworks	Privacy Meaning	Inclusion/Exclusion
10.	Authentication	LINDDUN, PriS - Pfitzmann and Hansen, ICPPS and ENISA mention but not as a goal	Verifying the identity of a process, device or user	Only LINDDUN and PriS consider this a privacy goal. Arguably this is a system or process setting requirement rather than a goal-it is a validation that the person/system is who they claim to be which, in privacy terms, should be covered as part of integrity. Therefore this has not been included as a privacy goal.
11.	Undetectability	Pfitzmann and Hansen 2010-ICPPS mention but not as a goal	*Ensuring data is annonymised so that anonymity and undectability of the individual is preserved.* and *Ensuring data cannot be sufficiently distinguished to establish whether it exists or not*	Included Included as a Privacy Goal together with *unobservability* (see Line 5).
12.	Accountability	LINDDUN, IRIS (CAIRIS), ENISA, Pfitzmann and Hansen, ICPPS and ISO29100 mention but not as a goal		Arguably this relates to compliance and transparency as, in order to meet compliance, there has to be accountability. In privacy terms this can be related to having an accountable person and having accountability over what data is collected, used, processed or shared. Therefore, this is considered to be incorporated within transparency.
13.	Identification	PriS	This concerns user identifying themselves within a system	Not included in PLAN. This concerns user identifying themselves in a system as opposed to identification of an individual or risk of re-identification which is the opposite of identifiability and therefore not a privacy goal.
14.	Data Protection	PriS	Ensuring personal data is appropriately processed and stored	This is considered embedded within all of the above privacy goals. and therefore, not included as a Privacy Goal.
15.	Authorisation	LINDDUN, PriS, IRIS (CAIRIS) mention but not as goal		This is similar to authentication in that a system or process will need to have this property for validation purposes but, for privacy, this forms part of integrity and confidentiality. Not included as a Privacy Goal.
16.	Non-repudiation	LINDDUN, ENISA mentions this as a threat, not a privacy goal - ICPPS and IRIS (CAIRIS) mention but not as goal	Proof of action, e.g., making sure that a user who processes an item of data cannot at a later stage deny having processed that item of data	As above, this is part of integrity and thus, not included as a Privacy Goal.

References

1. EEA. Circular Economy in Europe: Developing the Knowledge Base. 2016. Available online: https://www.socialistsanddemocrats.eu/sites/default/files/Circular%20economy%20in%20Europe.pdf (accessed on 25 September 2022).
2. EEA. Circular by Design: Products in the Circular Economy. 2017. Available online: https://circulareconomy.europa.eu/platform/sites/default/files/circular_by_design_-_products_in_the_circular_economy.pdf (accessed on 25 September 2022).
3. Henriksen-Bulmer, J.; Faily, S.; Katos, V. Translating Contextual Integrity into Practice using CLIFOD. In Proceedings of the 2018 Networked Privacy Workshop at CSCW, Jersey City, NJ, USA, 3–7 November 2018.
4. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. Implementing GDPR in the Charity Sector: A Case Study. In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20–24. 2018, Revised Selected Papers*; Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 173–188. [CrossRef]
5. Altman, M.; Wood, A.; O'Brien, D.R.; Vadhan, S.; Gasser, U. Towards a modern approach to privacy-aware government data releases. *Berkeley Technol. Law J.* **2015**, *30*, 1967. [CrossRef]
6. Oxford University Press. Oxford English Dictionary. 2017. Available online: https://www.oed.com/ (accessed on 25 September 2022).
7. Liew, A. Understanding Data, Information, Knowledge And Their Inter-Relationships. *J. Knowl. Manag. Pract.* **2007**, *7*, 1–16.

8. Liew, A. DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships. *Bus. Manag. Dyn.* **2013**, *2*, 49–62.
9. Ackoff, R. From data to wisdom. *J. Appl. Syst. Anal.* **1989**, *16*, 3–9.
10. McAfee, A.; Brynjolfsson, E. Big data: The management revolution. *Harv. Bus. Rev.* **2012**, *90*, 60–66. 68, 128.
11. Acito, F.; Khatri, V. Business analytics: Why now and what next? *Bus. Horizons* **2014**, *57*, 565–570. [CrossRef]
12. Pilton, C.; Faily, S.; Henriksen-Bulmer, J. Evaluating Privacy-Determining User Privacy Expectations on the Web. *Comput. Secur. J.* **2021**, *105*, 1–36. [CrossRef]
13. Lee, H.; Kobsa, A. Confident privacy decision-making in IoT environments. *ACM Trans. -Comput.-Hum. Interact.* **2020**, *27*, 1–39. [CrossRef]
14. Solove, D.J. *Nothing to Hide: The False Tradeoff between Privacy and Security*; Yale University Press: Yale, CT, USA, 2011.
15. Ohm, P. Broken Promises of Privacy: Responding to the surprising failure of anonymization. *UCLA Law Rev.* **2010**, *57*, 1701–1777.
16. Yucel, C.; Chalkias, I.; Mallis, D.; Cetinkaya, D.; Henriksen-Bulmer, J.; Cooper, A. Data Sanitisation and Redaction for Cyber Threat Intelligence Sharing Platforms. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Cyber Security and Resilience (CSR), Virtual, 26–28 July 2021; pp. 343–347.
17. Lablans, M.; Borg, A.; Ückert, F. A RESTful interface to pseudonymization services in modern web applications. *BMC Med. Inform. Decis. Mak.* **2015**, *15*, 1–10. [CrossRef]
18. Samarati, P. Protecting respondents' identities in microdata release. *IEEE Trans. Knowl. Data Eng.* **2001**, *13*, 1010–1027. [CrossRef]
19. Cynthia, D.; Nitin, K.; Deirdre, M. Differential Privacy in Practice: Expose your Epsilons! *J. Priv. Confidentiality* **2019**, *9* . Available online: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/689 (accessed on 25 September 2022).
20. Sasse, M.A.; Brostoff, S.; Weirich, D. Transforming the 'Weakest Link' a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technol. J.* **2001**, *19*, 122. [CrossRef]
21. Faily, S. *Designing Usable and Secure Software with IRIS and CAIRIS*, 1st ed.; Springer International Publishing: New York, NY, USA, 2018.
22. Westin, A.F. Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I–The Current Impact of Surveillance on Privacy. *Columbia Law Rev.* **1966**, *66*, 1003–1050. [CrossRef]
23. Nissenbaum, H.F. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Stanford Law Books: Stanford, CA, USA, 2010.
24. *BS ISO 31000*; British Standards Document BS ISO 31000:2009: Risk Management. Principles and Guidelines. Technical report; British Standard and the International Organization for Standardization (ISO): Geneva, Switzerland 2009.
25. *ISO/IEC 29100*; BS ISO/IEC29100: Information Technology-Security Techniques-Privacy Framework. Technical report; BSI Standards Publication: London, UK, 2020.
26. Gavison, R. Privacy and the limits of the law. *Yale Law J.* **1980**, *89*, 421–471. [CrossRef]
27. Lin, P.C.; Lin, P.Y. Unintentional and Involuntary Personal Information Leakage on Facebook from User Interactions. *KSII Trans. Internet Inf. Syst.* **2016**, *10*, 3301.
28. Borghi, M.; Ferretti, F.; Karapapa, S. Online Data Processing Consent under EU Law: A Theoretical Framework and Empirical Evidence from the UK [article]. *Int. J. Law Inf. Technol.* **2013**, *21*, 109. [CrossRef]
29. Ungoed-Thomas, J.; Hookham, M.; Belfield, R.; Ramzan, I. British Airways hack was 'a disaster waiting to happen'. *Times* **2021** . Available online: https://sourceforge.net/projects/openccg/ (accessed on 25 September 2022).
30. Dardenne, A.; van Lamsweerde, A.; Fickas, S. Goal-directed requirements acquisition. *Sci. Comput. Program.* **1993**, *20*, 3–50. [CrossRef]
31. Lamsweerde, A.V.; Brohez, S.; Landtsheer, R.D.; Janssens, D.; Informatique, D.D. From System Goals to Intruder Anti-Goals: Attack Generation and Resolution for Security Requirements Engineering. *Proc. RHAS* **2003**, *3*, 49–56.
32. Howard, M.; Lipner, S. *The Secuirty Development Lifecycle*; Number 9780735622742; Microsoft Press: Redmond, WA, USA, 2006. [CrossRef]
33. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *16*, 3–32. [CrossRef]
34. Wuyts, K.; Scandariato, R.; Joosen, W. Empirical evaluation of a privacy-focused threat modeling methodology. *J. Syst. Softw.* **2014**, *96*, 122–138. [CrossRef]
35. Faily, S.; Fléchais, I. Towards tool-support for Usable Secure Requirements Engineering with CAIRIS. *Int. J. Secur. Softw. Eng.* **2010**, *1*, 56–70. [CrossRef]
36. Kavakli, E.; Kalloniatis, C.; Loucopoulos, P.; Gritzalis, S. Incorporating privacy requirements into the system design process: The PriS conceptual framework. *Internet Res.* **2006**, *16*, 140–158. [CrossRef]
37. Kalloniatis, C.; Kavakli, E.; Gritzalis, S. Addressing privacy requirements in system design: The PriS method. *Requir. Eng.* **2008**, *13*, 241–255. [CrossRef]
38. European Commission. Types of Legislation. 2022. Available online: https://www.legislation.gov.uk/draft/2022 (accessed on 25 September 2022).
39. European Parliament and the Council of Europe. *General Data Protection Regulation (GDPR)*; Regulation (EU) 2016/679 5419/1/16; European Parliament and the Council of Europe: Brussels, Belgium, 2016.
40. Simon, H.A. A Behavioral Model of Rational Choice. *Q. J. Econ.* **1955**, *69*, 99–118. [CrossRef]
41. Edwards, W. The theory of decision making. *Psychol. Bull.* **1954**, *51*, 380–417. [CrossRef]

42. Simon, H.A. Rational Decision Making in Business Organizations. *Am. Econ. Rev.* **1979**, *69*, 493–513.
43. Fleming, J.E. Study of a Business Decision. *Calif. Manag. Rev.* **1966**, *9*, 51–56. [CrossRef]
44. Cowling, K.; Sugden, R. The essence of the modern corporation: Markets, strategic decision-making and the theory of the firm. *Manch. Sch.* **1998**, *66*, 59. [CrossRef]
45. Harrison, E.F.; Pelletier, M.A. The essence of management decision. *Manag. Decis.* **2000**, *38*, 462–470. [CrossRef]
46. Galanc, T.; Kolwzan, W.; Pieronek, J.; Skowronek-Gradziel, A. Logic and risk as qualitative and quantitative dimensions of decision-making process. *Oper. Res. Decis.* **2016**, *26*, 21.
47. Yin, R.K. *Case Study Research: Design and Methods*; SAGE: Los Angeles, CA, USA, 2013.
48. Pfitzmann, A.; Hansen, M. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. 2010. Available online: https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (accessed on 25 September 2022).
49. Hansen, M. Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In *Privacy and Identity for Life*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 375, pp. 14–31.
50. Hansen, M.; Jensen, M.; Rost, M. Protection Goals for Privacy Engineering. In Proceedings of the 2015 IEEE Security and Privacy Workshops. Unabhan̈giges Landeszentrum fur̈ Datenschutz Schleswig-Holstein (ULD), San Jose, CA, USA, 21–22 May 2015; pp. 159–166. [CrossRef]
51. ENISA. *Privacy and Data Protection by Design Privacy and Data Protection by Design—From Policy to Engineering*; Technical Report; European Union Agency for Network and Information Security (ENISA): Athens, Greece, 2014. [CrossRef]
52. *BS ISO 27000:2017*; British Standards Document BS ISO 27000:2017: Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary; Technical Report; British Standard and the International Organization for Standardization (ISO): Geneva, Switzerland, 2017.
53. Forth and NodalPoint and Bluesoft and Bournemouth University and Ecole des Ponts Business School and DGS. Ideal-Cities. 2022.
54. Henriksen-Bulmer, J.; Faily, S.; Jeary, S. DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems. *Future Internet* **2020**, *12*, 1–23. [CrossRef]
55. Bishop, M. *Computer Security: Art and Science. [Electronic Resource]*; Addison-Wesley Professional: Boston, MA, USA, 2002.