decode

Privacy Interface Guidelines

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement no. 732546

Project no. 732546

DECODE

DEcentralised Citizens Owned Data Ecosystem

D4.7 - Privacy Interface Guidelines

Version Number: V1.0

Lead beneficiary: TW

Due Date: December 2017

Author(s): Jen Hughes, Andrei Biasprozvanny, Priya Samuel, Jill Irving, James Barritt, Rylan Gooch (ThoughtWorks)

Editors and reviewers: Francesca Bria, Oleguer Sagarra, Javier Rodriguez (IMI), David Laniado, Matteo Manca (Eurecat), Federico Bonelli (Dyne)

Dissemination level:		
PU	Public	PU
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Approved by: Francesca Bria, Chief Technology and Digital Innovation Officer, Barcelona City Council (IMI)

Date: 30/12/2017

This report is currently awaiting approval from the EC and cannot be not considered to be a final version.

Contents

Abbreviations

GDPR	General Data Protection Regulations
PdB	Privacy by Design
UI	User Interface
UX	User Experience
IoT	Internet of Things
DECODE	Decentralised Citizen-owned Data Ecosystem

1.0 Introduction

Privacy and control of personal data is at the core of the DECODE project. This document is focused on identifying considerations specifically related to the privacy guidelines of the user interface. There are additional documents detailed in related deliverables that address privacy and security from other perspectives such as legal[1], technological[2] and social[3] considerations.

DECODE considers three different practical use cases: collaborative economy/hospitality, participatory citizen sensing, and open democracy, with a specific focus on how this relates to user communities in two European cities - Amsterdam and Barcelona. These use cases are implemented in the form of four different pilot candidates, outlined in more detail in deliverable 1.1, Pilot Scenarios and Requirements[4]

- iDigital / BCNow Platform in collaboration with Decidim Barcelona and the Barcelona City Council
- IoT Pilot with Making Sense (that uses SmartCitizen platform) in Barcelona
- Holiday Rental Register / FairBnB in Amsterdam
- Gebiedonline (Neighbourhood Online) in Amsterdam

The design of the interfaces in each pilot will empower users to share their data in a privacy preserving way that is easy to understand and use.

Section 1 explores the scope and background information for this deliverable, and the relationship with other project deliverables. Section 2 then lists the user interfaces in DECODE and their significance, which is followed by section 3, which presents several considerations for user interfaces listed in relation to Privacy by Design and GDPR.

[1] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino), De Martin, Juan Carlos (Politecnico di Torino)... "D1.8 Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

[2] Danezis, George. Bano, Shehar. Al Bassam, Mustafa... "D1.4 - First version of the DECODE architecture.' Oct. 2017 https://decodeproject.eu/publications/decode-architecture-first-version Accessed 23 Nov. 2017

[3] Symons, Tom. Bass, Theo. "Me, my data and I: The future of the personal data economy | DECODE." 18 Sep. 2017, https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy. Accessed 21 Nov. 2017.

[4] Irving, Jill, Barritt, James... "Pilot Scenarios and Requirements | DECODE." 27 Sep. 2017, https://www.decodeproject.eu/publications/pilot-scenarios-and-requirements. Accessed 21 Nov. 2017.

Finally, section 4 presents the challenges and the next steps in evolving the user interfaces in terms of privacy.

DECODE will be developed with a Privacy by Design approach and it is also important that we consider GDPR legislation that will come into effect during the project lifespan. The interface considerations set out in this document will be tested with real world users via interviews, sketches and prototypes in order to gather early feedback and iteratively improve on the user experience guidelines. DECODE will engage end users (from the pilot projects) throughout the design and development of the ecosystem. Application developers and communities will also be engaged throughout the project with hackathons and summer schools[5].

1.1 Scope

This report has been created as part of DECODE (DEcentralised Citizen Owned Data Ecosystem) - a EU Horizon 2020 Research and Innovation project.

DECODE employs a user-centric methodology, meaning user involvement and feedback during the design and development process is crucial. This document does not replace this need.

With the introduction of the more stringent GDPR regulations, information and work around privacy interface design is constantly being published. Therefore, it is likely that information and examples will change and be updated during the project.

Every interface design will have its own requirements, constraints and context and the considerations presented here are not exhaustive for every situation or interface. They can provide a starting point for designing privacy interfaces.

This report references legal issues and regulations as they are important topics to consider when designing for privacy (GDPR as an example). However, this report is focused on designing interfaces for end users, and any references to regulations are with this in mind. Compliance with regulations is not covered. Legal information for DECODE can be found in D1.8 - Legal frameworks for digital commons, DECODE OS and legal guidelines[6].

There are many examples of guidelines and principles relating to privacy design in addition to the legal regulations. Many of these relate to privacy design as a whole which encompasses interface design along with architectural and other elements of system design.

This document describes 8 general considerations related to privacy design that are particularly relevant to interface design and user experience and are useful to consider when designing privacy interfaces for DECODE.

[5] DECODE Proposal: ICT-12-2016 DECODE

[6] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino), De Martin, Juan Carlos (Politecnico di Torino)... "D1.8 Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

As the project progresses, the project code and design will incorporate the latest thinking on the interface design requirements.

1.2 Relationship to Other Tasks and Deliverables

D1.2 - Privacy Design Strategies for the DECODE Architecture[7]

Deliverable 1.2, led by consortium partner Radboud University, describes privacy by design and the privacy design strategies to be adopted at the architectural level of the DECODE project, many of which are also relevant to the interface design and should also be considered when designing user interfaces for DECODE.

D1.8 - Legal frameworks for digital commons, DECODE OS *and* legal guidelines[8]

Deliverable 1.8, led by consortium partner Politecnico di Torino (POLITO) reviews the legalities surrounding the DECODE project. Particularly relevant to this document is the information around GDPR.

D1.7 - Me, My Data and I: The future of the personal data economy[9]

Deliverable 1.7, led by consortium partner Nesta and published in September 2017, provides an overview of the DECODE project, including the problems that the project is trying to address and how DECODE might provide a solution. It is very relevant to this report in terms of providing context and background of some of the current challenges and why privacy is important to users.

D1.1 - Pilot Scenarios and Requirements[10]

Deliverable 1.1, led by consortium partner ThoughtWorks and published in September 2017, provides details and background for the DECODE pilot projects. It also contains proto personas created for each pilot during inception workshops.

[7] Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora... - "Privacy Design Strategies for the DECODE Architecture" June 2017

[8] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino), De Martin, Juan Carlos (Politecnico di Torino)... "Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

[9] Symons, Tom. Bass, Theo. "Me, my data and I: The future of the personal data economy | DECODE." 18 Sep. 2017, https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy. Accessed 21 Nov. 2017.

[10] Irving, Jill, Barritt, James... "Pilot Scenarios and Requirements | DECODE." 27 Sep. 2017, https://www.decodeproject.eu/publications/pilot-scenarios-and-requirements. Accessed 21 Nov. 2017.

D6.5 - Co-creation framework, methodologies and templates[11]

Deliverable 6.5, led by consortium partner Dyne and published in July 2017, provides insight into different co-creation methods that can be used within DECODE.

D3.3 - DECODE language design patterns[12]

Deliverable 3.3, led by consortium partner Dyne explains the nature of smart rules in DECODE. It establishes guidelines and requirements for the implementation of an execution engine for a new domain specific language. It also contains a section outlining some of the usability requirements for a smart rules language.

T4.4 - DECODE graphical interface design for smart-rules implementation[13]

The motivation for the task in the proposal states:

> *"While sharing potentially privacy sensitive information according to consensual choices, a good user experience and is paramount for the DECODE ecosystem. The consequences of one's actions should be extremely clear at all points, the defaults conservative, and the feedback optimal. An inclusive design, in which the end user is fully informed and empowered is one of the core values of the whole DECODE project."*

This report will provide background research to help inform the interface designs created as part of Task 4.4.

[11] van Kranenburg, Rob. Bonelli, Federico. Veldman, Jennifer "Co-creation framework, methodologies and templates" Jul. 2017

[12] Roio, Dennis, "DECODE language design patterns" Nov. 2017

[13] DECODE Proposal: ICT-12-2016 DECODE

2.0 DECODE Context

This section lists the user interfaces within DECODE that privacy considerations can be applied to and their relevance to the user. The aim of DECODE is to provide state of the art tools to give people better control of their data on the internet[14] and having privacy aware user interfaces is a central component that defines the user experience.

2.1 DECODE Interfaces

Giving users tools to control their data online also implies giving users access to user friendly interfaces to express and understand these entitlements. DECODE currently has two components (the DECODE wallet and smart language for entitlements) that include interfaces that users will interact with. As the DECODE architecture and the user journeys evolve, these interfaces will also evolve in the future.

2.1.1 The DECODE wallet

Every person who wishes to trade any asset across a private or public network requires access to the network. This access occurs via a software application that mediates between user and the DECODE ledger. The software application, often called a "wallet," can be installed directly on a device or accessed via a web browser. Depending on how it is designed, a wallet can be used to send and/or receive digital assets. Some wallets allow for direct transacting without a mediating third-party, while other wallets are run by third parties who maintain custodianship of users' digital assets on their behalf.[15]

A DECODE wallet is an implementation of a software wallet that stores cryptographic material which identifies the user. The user may interact with their DECODE wallet to "Login with DECODE" into applications. In this scenario, the user attempting to log into a pilot application would be redirected to their DECODE wallet, authenticate there as above and then an exchange of application specific cryptographic credentials would be passed back to the application, allowing them to be authenticated.

The DECODE wallet can be used for

- Registration with DECODE services and pilots.
- Configuring entitlements to user's data.

[14] Danezis, George. Bano, Shehar. Al Bassam, Mustafa… "D1.4 - First version of the DECODE architecture.' Oct. 2017 https://decodeproject.eu/publications/decode-architecture-first-version Accessed 22 Nov. 2017

[15] Alexander Grech, Anthony F. Camilleri - "Blockchain for education" http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf Accessed 22 Nov. 2017

- Registering with a particular third party application (where you have to enter profile information).
- Secure authentication with multi-factor authentication and account recovery

DECODE will explore both online hosted wallets, where users log into an online wallet, as well as desktop, mobile or in-browser wallets. Users will need to understand the security implications of the choices they make, particularly around the storage and exchange of personal data.

2.1.2 Smart language for entitlements

Objective 3 of the DECODE project is to 'Empower citizens to control and own their data.'[16] DECODE aims to achieve user control of their data using entitlements, expressed through smart rules. Deliverable 3.1 - Survey of technologies for ABC, Entitlements and Blockchains[17] - provides an introduction to entitlements. It says of data entitlements:

> *"Data entitlements could be thought of as an evolution of a traditional authorization scheme specialized for the securing of both personal, business and IoT data. Giving the data owner full control of the access and discovery of their data creates a system of empowerment whose currency is privacy. Privacy is a fundamental right. The relationship of privacy and data entitlement is subject to many nuances. Users might allow a party to search and access their data, but only under the understanding that they will not be personally identified or only under specific circumstances. For example, a driver of a motor vehicle with an on-board camera might want to entitle the emergency services access to his data when there is a road traffic accident. However, the driver might not want to be identified as being in a certain geographical area or that he was exceeding the speed limit at the time. Data, when available, can directly or indirectly compromise privacy in a way that would surprise a user."*

The user experience and interface design in DECODE will be important to allowing users to successfully apply entitlements to their data so that they are aware and can share their data as they intend.

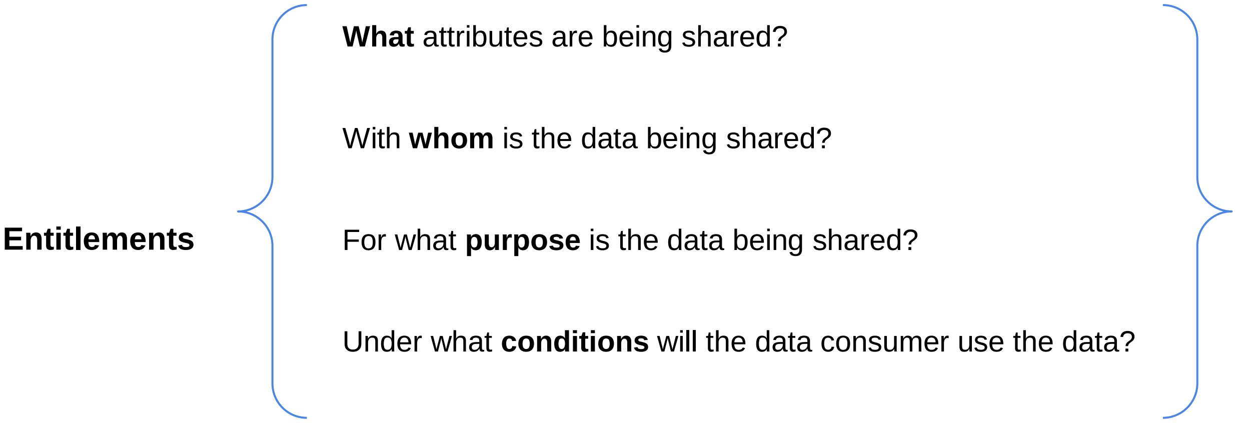
In DECODE an entitlement is defined in a policy and implemented with the application of cryptography. Some examples of data entitlement policies[18] in DECODE are expressed in Figure 1. The DECODE smart rule language will aim to naturally avoid

[16] DECODE Proposal: ICT-12-2016 DECODE

[17] Al-Bassam, Mustafa, Bano, Shehar, Danezis, George... "D3.1 - Survey of Technologies for ABC, Entitlements and Blockchains" June 2017

[18] Danezis, George. Bano, Shehar. Al Bassam, Mustafa... "D1.4 - First version of the DECODE architecture.' Oct. 2017 https://decodeproject.eu/publications/decode-architecture-first-version Accessed 22 Nov. 2017

complex constructions and define sets of transformations that can be then easily represented with visual metaphors.[19]



Entitlements

What attributes are being shared?

With **whom** is the data being shared?

For what **purpose** is the data being shared?

Under what **conditions** will the data consumer use the data?

Figure 1. Data entitlement policies in DECODE

[19] D3.3 DECODE language design patterns - Denis Roio, Dyne.org

3.0 Privacy Design Considerations

3.1 Why is it important to consider privacy when designing user interfaces?

The user interface is the point where the user interacts with the system. It is where users input personal data, choose to share data with others and exercise their privacy preferences. It is often also the place where privacy policies and information are displayed to the user. As such, it is imperative that privacy issues and concerns are considered during the design and development of interfaces as much as they are during the design and development of the backend systems.

The inner workings of the architecture, such as cryptographic features, are not always visible to end users. The users rely on what is presented to them to make decisions on whether or not to trust the system and make choices about their personal data and privacy.

Additionally, there are legal implications to processing personal data. GDPR regulations that will be enforced from May 2018 will influence the user interface in relation to privacy, for example, how privacy information is presented and how consent is obtained.

3.2 What is 'personal' data?

Referred to throughout this document is the term 'personal' data. It is important to understand what constitutes personal data when designing user interfaces and user experiences to know when specific legal and other issues should be considered.

Article 4 of GDPR[20] defines personal data as

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*[21]

[20] "General Data Protection Regulation - European Commission." 4 May, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 30 Oct. 2017.

[21] "General Data Protection Regulation - European Commission." 4 May. 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 18 Oct. 2017.

Concerning the applicability of the rules provided by GDPR, it is crucial to stress the meaning of 'personal data processing'. According to Article 4(1), point 2, personal data processing is

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*[22]

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is considered to be 'sensitive data'[23,24]. Article 9 of GDPR also covers the processing of sensitive data which have further processing restrictions.[25]

3.3 Privacy Design Considerations

There are many other examples of guidelines and principles relating to privacy design in addition to the legal regulations. Many of these relate to privacy design as a whole which encompasses interface design along with architectural and other elements of system design. Some examples of other privacy guidelines are included in appendix A.

The following section describes 8 general considerations related to privacy design that are particularly relevant to interface design and user experience and are useful to consider when designing privacy interfaces for DECODE.

[22] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino),De Martin, Juan Carlos (Politecnico di Torino)... "Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

[23] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino),De Martin, Juan Carlos (Politecnico di Torino)... "Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

[24] "Guide to the General Data Protection Regulation (GDPR) | ICO." https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr. Accessed 22 Nov. 2017.

[25] "General Data Protection Regulation - European Commission." 4 May. 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 26 Oct. 2017.

3.3.1 User-Focused

Design and develop user interfaces with the user front of mind. Understand and consider the users' goals and motivations, test with users often, and iterate designs based on user feedback.

'You are not your user[26] is a phrase that is regularly heard in the user experience industry. Users have different backgrounds, product knowledge, and life experience to the designers and developers whose biases can influence design decisions. An article by Jakob Nielsen[27] highlights the difference in technology skills between designers and developers and the broader population. He says:

> *"One of usability's most hard-earned lessons is that you are not the user. This is why it's a disaster to guess at the users' needs. Since designers are so different from the majority of the target audience, it's not just irrelevant what you like or what you think is easy to use — it's often misleading to rely on such personal preferences."*

Focusing on the end user and considering their behaviours, goals and motivations throughout the design and development process increases the confidence that what is presented to the user is understandable, usable and most importantly allows the user to accomplish their privacy goals and control their personal data. Co-creation methodologies[28], involving the users are a method to achieve this goal.

Principle 7 of Privacy by Design[29] is related to focusing on the interests of the user:

> *'Respect for User Privacy — Keep it User-Centric*
>
> *Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.'*

In June 2012, a paper was published exploring in more detail Privacy by Design and User Interfaces[30]. It covers four UI/UX topics related to privacy - Context, Awareness,

[26] "The Distribution of Users' Computer Skills: Worse Than You Think." 13 Nov. 2016, https://www.nngroup.com/articles/computer-skill-levels/. Accessed 24 Nov. 2017.

[27] "The Distribution of Users' Computer Skills: Worse Than You Think." 13 Nov. 2016, https://www.nngroup.com/articles/computer-skill-levels/. Accessed 24 Nov. 2017.

[28] van Kranenburg, Rob. Bonelli, Federico. Veldman, Jennifer "Co-creation framework, methodologies and templates" Jul. 2017

[29] Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles - Information and ...." https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Accessed 21 Nov. 2017.

[30] Cavoukian, Ann. Weiss, Justin B. "Privacy by Design and User Interfaces - Information and Privacy ...." 1 Jun. 2012, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces_Yahoo.pdf. Accessed 21 Nov. 2017.

Discoverability and Comprehension, developed through a study by Create with Context.

3.3.2 User Control

The interface should provide users with the information and mechanisms to exercise control over their personal data. It should aim to make privacy information and controls easy to find and simple to use, empowering the user to control their personal data. Privacy should be the default setting.

The interface is where the user will interact with the systems developed to facilitate control of their personal data. The design of the interface can impact on how easy or difficult, or even what is possible for the user to accomplish in terms of controlling their data.

Control is related to three of the other considerations outlined in this document, *Clarity and Understandability*, *Inform* and *Consent*. To exercise control over their data, users need to be adequately informed about the use of their data and their options (Inform), be able to understand the information provided (Clarity and Understandability) and exercise their control through relevant mechanisms (for example, Consent). See GDPR, Article 12[31] on "Transparent information, communication and modalities for the exercise of the rights of the data subject"

User Control and GDPR

Vint Cerf, an internet pioneer and co-inventor of TCP/IP, captured the user-centricity of the internet:

> *"[It's] open, neutral architecture has proven to be an enormous engine for market innovation, economic growth, social discourse, and the free flow of ideas. The remarkable success of the Internet [...] gives consumers choice and control over their online activities".*[32]

Since its origins, the internet has undergone substantial changes. Growing commercial marketplaces and the rise of business models based on utilisation of personal data shifted the balance of control away from users.[33]

The GDPR is designed to give control back to individuals. It introduces strict protection measures and new obligations for service providers that enhances the control of end users over their personal data. For example, the GDPR provides the following rights for

[31] "General Data Protection Regulation - European Commission." 4 May, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 18 Oct. 2017.

[32] Patry, W., 2009. Moral Panics and the Copyright Wars. Oxford University Press

[33] "GDPR: A Step Towards a User-centric Internet? | Intereconomics." https://archive.intereconomics.eu/year/2017/4/gdpr-a-step-towards-a-user-centric-internet/. Accessed 23 Nov. 2017.

individuals: the right to be informed, the right of access, the right to rectification, the right to erase, the right to data portability and others.

Interfaces should provide easy to use tools for users to be able to exercise these rights. They should be and feel in control and easily make, review and change their privacy related decisions. A single place should be given for users to configure various settings with privacy friendly settings enabled by default. If an application processes data in unexpected ways or data is sensitive, 'just-in-time' notifications should be considered to inform the user what's happening.

Privacy by Design principle 3 refers directly to 'Privacy as the Default Setting'. It says:

> *"We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default"'*[34]

3.3.3 Information and Device Context

Be aware of the context in which users will be presented with privacy information and choices, both within the interface and external influences such as the device being used.

Context in an interface can be used in a number of ways to describe different aspects of how a user perceives and relates to an interaction, in relation to other aspects of the interface. Relevant to interface design and user experience are:

- Position in an interface's interaction **-** This can refer either to the position in the sequence of a user journey, or the location on a specific screen of the interface.
- Device type **-** For example, mobile, tablet, desktop, smartwatch.

Position in interface

Of particular relevance to privacy is when a user is asked to change their privacy settings, which allows a different amount of data to be shared. UX best practice is to ask for information from a user as close as possible to the point in the user journey at which it is necessary. This means for example, only asking a user to increase the audience to which their data will be shared just before the sharing is about to happen, rather than earlier in the process, such as the application's onboarding journey.

Device type

[34] Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles - Information and ...." https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Accessed 21 Nov. 2017.

The categories of mobile, tablet, desktop, smartwatch and voice interface are becoming increasingly fragmented and boundaries increasingly blurred between the types. This is particularly evident in the mobile/tablet category, where size is often used as the way to categorise.

Statistics from Statcounter show that as of October 2017 in Europe 36.07% of web usage is on mobile and 57.76% on desktop/laptop. Tablet use is less significant at 6.18%.[35]

Consideration also needs to be given to non-screen based interfaces ie. Voice/chat enabled interfaces. There can be particularly high impact on privacy when a device is listening and potentially recording sound in a home, or monitoring other aspects such as electricity consumption. These non-screen based devices are disconnected from the visual interface where a user is able to control settings.

Omnichannel user journeys present a specific challenge, in that users now expect to be able to start a user journey on one device, and continue it on another device with no loss of the information input. Appropriate care needs to be taken to make sure that privacy impact is correctly communicated in the right places on the user journey.

Privacy expectations from devices:

- Mobile – personal, private, accessed only by the individual who owns the phone
- Laptop – more likely to be shared within the home by more than 1 family member, or for example in a school or academic setting
- Tablet – although a personal device, also often shared amongst family members

Devices need to be carefully considered and current usage researched. For example, mobile devices cannot be assumed to be mostly used outside the home, and tablets may be devices which never leave a single room.

3.3.4 Consent

Consent should be informed and captured in a clear, unambiguous way. Users should be able to withdraw consent as easily as giving it.

Article 4(11) of GDPR[36] defines consent as

> *"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*

[35] "Desktop vs Mobile vs Tablet Market Share Europe | StatCounter ...." http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe. Accessed 24 Nov. 2017.

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), see http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent is a crucial mechanism to empower users to have control over their data. As such it is extremely important to consider when and how consent should be handled in both the user journey and also in the interface design. It is closely related to the consideration of Clarity and Understanding which impact directly on how consent options are presented to the end user. There are a number of patterns for obtaining consent in use throughout the digital world, varying in terms of how consent is described, presented, captured and withdrawn.

- Explicit consent means that the user is clearly presented with an option to accept or decline a data processing request. Examples of explicit consent are ticking a box when creating an account with a website or signing a consent form that explains why an organisation needs to collect your information.

- Implied consent means that a user's permission is inferred from their actions rather than expressly provided. The following statement informs that consent will be given implicitly: "By clicking submit at the end of the study you are providing your consent for us using your personal data to send you promotional emails".

- Opt-out consent means that the user is only given an explicit option to decline consent (e.g. pre-ticked check box) - if they don't, consent is considered to be granted. Bundling consent means that consent request is incorporated into terms & conditions agreement.

Consent and GDPR

The predecessor of GDPR, Data Protection Directive (Directive 95/46/EC), does not specify any formal requirements for consent, however, it includes a definition of consent (Article 2(h))[37]. In GDPR, the importance of consent is clear with a definition and requirements provided.

GDPR emphasises that long, illegible terms and condition texts can no longer be used. The recommendation is to present a consent request in a distinguishable, easily accessible, granular form in plain language. GDPR specifically bans pre-ticked opt-in boxes - there now must be some form of clear affirmative action or, in other words, a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity[38].

[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[38] "Consent | ICO." https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/consent/. Accessed 23 Nov. 2017.

The message that consent communicates should be specific and informative. It must specifically cover the controller's[39] identity, the purposes of the processing, the processing activities and the right to withdraw consent at any time.

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent.[40]

It is not sufficient to only consider the giving of consent in the user journey and interface design. Article 7(3) of GDPR states that it should be as easy to withdraw consent as it is to give it, and that users have the right to withdraw their consent at any time.

The ICO (Information Commissioner's Office) in the UK provides detailed information about consent and GDPR. More information is available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/consent/.

3.3.5 Clarity and Understandability

Present privacy information and choices in a clear, accessible and easy to understand manner.

- *Use clear and easy to understand language, appropriate for audience*
- *Be aware of technical jargon*
- *Adhere to accessibility standards*

To exercise control over their personal data, users must first be able to understand the information presented to them and what the implications of their choices are. Design choices and copy in the user interface can impact this.

Clear and easy to understand means different things to different people and it is very important to be user focused when considering if something is understandable. Testing with end users will help to highlight when information or options are not clear.

It is also important to consider some users may have different requirements to ensure that something is clear and understandable.

Web Content Accessibility Guidelines[41] and Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines Apply to Mobile[42] explain how to make content more

[39] "Data controllers and data processors: what the difference is and what the governance implications are", Data Protection Act, https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

[40] "Consultation: GDPR consent guidance", https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

[41] "WCAG Overview | Web Content Accessibility Guidelines Overview", https://www.w3.org/WAI/intro/wcag. Accessed 21 Nov. 2017.

accessible to those with disabilities. Information being addressed to a child may require different language.

GDPR also stipulates that information about data processing is presented to users in a clear and transparent way. Section 1.3.1.2 of deliverable 1.8[43] outlines that:

> *"Personal data "shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used"'*

Section 1.3.1.2 of deliverable 1.8 gives more information about the general principles and definitions on personal data processing.

3.3.6 Inform

"Provide data subjects with adequate information about which personal data is processed, how it is processed, and for what purpose'[44].

Inform is a strategy outlined in Deliverable 1.2 - Privacy design strategies for DECODE architecture and it is particularly relevant to the user interface design and so is included here as it is described in Privacy design strategies for DECODE Architecture[45]:

"Associated tactics:

***Supply:** making available extensive resources on the processing of personal data, including*

policies, processes, and potential risks.

***Notify**: alerting data subjects to any new information about processing of their personal data in a timely manner.*

***Explain:** detailing information on personal data processing in a concise and understandable form"'*[46]

[42] "Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines ...." 26 Feb. 2015, https://www.w3.org/TR/mobile-accessibility-mapping/. Accessed 24 Nov. 2017.

[43] Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino),De Martin, Juan Carlos (Politecnico di Torino)... "Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

[44] Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora..., - "Privacy Design Strategies for the DECODE Architecture" June 2017

[45] Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora..., - "Privacy Design Strategies for the DECODE Architecture" June 2017

The associated tactics outlined what information should be presented to the user. In relation to the user interface design and user experience, also consider:

- Where in the user journey privacy information should be presented.
- How easy it is for users to locate and access the resources outlined in ‘Supply’.
- Where and how notifications are conveyed to the user.

With regards to user interface design, ‘Inform’ is closely related to the consideration of ‘Clarity and Understandability’, which focuses on how users understand the content presented. See GDPR Article 12[47] on "Transparent information, communication and modalities for the exercise of the rights of the data subject".

3.3.7 Educate

Educate users about their personal data, where and how it is stored, protected and accessed, and raise awareness about data privacy issues and technology in general.

The interface design can help to educate users about where and how their personal data is stored and used and also raise awareness about data privacy issues and technology.

Distributed ledger technology and complex cryptographic methods are not necessarily widely understood.

A principle outlined in Tijem Schep’s book “Design My Privacy”, is to ‘Open the Black Box’.[48] This primarily refers to designing for ‘Smart’ products, but the principle can be applied generally. By exposing or explaining some of the workings of the software, it can help the user understand why the system behaves in a certain manner.

The GSMA also outlines Education as one of their Mobile Privacy Principles[49]. ‘Education - Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.’

Raising Awareness

[46] Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora..., - “Privacy Design Strategies for the DECODE Architecture” June 2017

[47] "Article 12 and ff. General Data Protection Regulation - European Commission." 4 May, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 18 Oct. 2017.

[48] Schep, Tijmen “Design My Privacy” BIS, 2017

[49] "Mobile Privacy Principles - GSMA." http://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf. Accessed 22 Nov. 2017.

In addition to educating users about where and how their personal data is stored and used, DECODE also aims to raise awareness about data privacy issues and technology in general.

Users should be encouraged to understand the basics of privacy aware technologies. Things must be made simple for users so that level of effort is not a barrier. The option to access and promote "technological and data literacy" should always be present.

Users should also be educated that data forms our personal identity and so should be careful in how they control it.

3.3.8 Minimise the capture and display of data

Refrain from collecting more personal data than is required and minimise the personal data displayed through the interface.

A lot of personal information is collected through the user interface, often through the use of forms, where users are presented with pre-defined fields to complete. When designing forms and considering the fields that will be presented to the user it is important to consider if the information being captured is required and/or being captured in the most privacy-preserving format.

As an example, instead of requiring the full date of birth to verify the age of the user, consider only requiring the year of birth. In some cases the exact age of the user is crucial in order to determine the validity of given consent and to process the data in a lawful way taking into account the measures prescribed by the GDPR, Art. 8[50]. In these cases the full date of birth could be erased or obscured when it is no longer necessary for the data processing (pursuing the data minimization principle and the data storage limitation principle).

Consider if the display of data could inadvertently reveal more information about a person than intended. A few years ago, some police forces advised cyclists to change privacy settings or not start and end rides at their home address after a rise in bike theft that they believed could be linked to sharing data on ride sharing apps.[51] [52] Strava offer a feature to do this 'Privacy Zones', included in appendix B. Another common example

[50] "General Data Protection Regulation - European Commission." 4 May, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 18 Oct. 2017.

[51] "Police renew appeal for cyclists to protect personal information on ride ...." 13 Oct. 2015, http://www.cyclingweekly.com/news/latest-news/police-renew-appeal-for-cyclists-to-protect-personal-information-on-ride-sharing-sites-195381. Accessed 21 Nov. 2017.

[52] "Police warn cyclists of thieves using GPS apps to steal bikes - Cycling ...." 15 Nov. 2014, http://www.cyclingweekly.com/news/latest-news/police-warn-cyclists-thieves-using-gps-apps-steal-bikes-144820. Accessed 21 Nov. 2017.

when data is redacted is credit card numbers. After the initial entry of the credit card number, only the last 4 numbers are displayed on the interface subsequently.

3.4 Summary of Considerations

User-Focused

Design and develop user interfaces with the user front of mind. Understand and consider the user's goals and motivations, test with users often, and iterate designs based on user feedback.

User Control

The interface should provide users with the information and mechanisms to exercise control over their personal data. It should aim to make privacy information and controls easy to find and simple to use, empowering the user to control their personal data. Privacy should be the default setting.

Information and Device Context

Be aware of the context in which users will be presented with privacy information and choices, both within the interface and external influences such as the device being used.

Consent

Consent should be informed and captured in a clear, unambiguous way. Users should be able to withdraw consent as easily as giving it.

Clarity and Understandability

Present privacy information and choices in a clear, accessible and easy to understand manner.

- *Use clear and easy to understand language, appropriate for audience*
- *Be aware of technical jargon*
- *Adhere to accessibility standards*

Inform

'Provide data subjects with adequate information about which personal data is processed, howit is processed, and for what purpose.'[53]

Educate

Educate users about their personal data, where and how it is stored, protected and accessed, and raise awareness about data privacy issues and technology in general.

Minimise the capture and display of data

Refrain from collecting more personal data than is required and minimise the personal data displayed through the interface.

[53] Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora..., - "Privacy Design Strategies for the DECODE Architecture" June 2017

4.0 Conclusion and Next Steps

A key objective of DECODE is to put the user in control of their personal data. In conjunction with the technical architecture, the interface design supports the privacy preserving aspects of DECODE. This document outlined considerations that will be taken into account when designing privacy interfaces for DECODE.

A number of specific design challenges have been identified relating to privacy and DECODE that will be addressed during the course of the project. These will evolve as the project progresses and our knowledge and understanding increases.

- Privacy Information: Defining the line between the pilot applications and the DECODE platform in terms of privacy information. For example, privacy policies, information about settings, how data will be used.
- Localisation and internationalisation: DECODE has pilots in two cities in different countries with different languages and cultures. There is also the possibility for DECODE to be used in other countries in the future.
- Working across different industry sectors: Applications built on DECODE will have different user bases in different industry sectors and will have their own branding.
- Reducing the User Experience Friction: Reducing the friction in the user journey between pilot applications and the DECODE interfaces. An example of this may be the user experience going from the application to the DECODE wallet.
- Education: DECODE uses state of the art technology and complex cryptographic methods. The design challenge is to educate users about how their data is being stored in an easy to understand way. DECODE is 'inverting' the model of consent by putting the user in control of the consent mechanism (entitlements). This emphasises the need to inform and educate users that they are in control of their data and consent that they have given.
- Data entitlements awareness: DECODE will implement entitlements (see section 2.0 - DECODE Context for a description of entitlements) using smart rules. The technical implementation of smart rules needs to be translated to an easy to use interface for users to control their personal data. The key challenge here is finding ways to inform users about who has access to their data and how it is being used.

Appendix A - Useful Resources

Many organisations are doing work in the area of privacy and user experience and interface design. Below are a few external examples and resources that have focused specifically on privacy and topics related to GDPR. Many of these provide good ideas and examples of how privacy can be included into interface design.

Data Transparency Lab

http://datatransparencylab.org/

The Data Transparency Lab is an inter-institutional collaboration, seeking to create a global community of technologists, researchers, policymakers and industry representatives working to advance online personal data transparency through scientific research, innovation and design.

Projects by IF

https://projectsbyif.com/

Projects by IF have been doing a lot of work in the area of privacy and data protection and they have a number of ideas and resources on their website including:

- Data Permissions Catalogue -A catalogue of different design patterns for data sharing (https://catalogue.projectsbyif.com/)
- Designing for Digital Rights - a set of sketches and prototypes looking at GDPR (https://projectsbyif.com/blog/designing-for-new-digital-rights)

Digital Catapult

https://www.digitalcatapultcentre.org.uk/project/pd-receipt/

Digital Catapult Centre has been researching and trialling the use of personal data receipts (see example in appendix B)

privacypatterns.org

https://privacypatterns.org/

A collection of design solutions to privacy problems. Some are technical solutions but also contains interface design patterns such as layered policy design.

Legal Tech Design

http://www.legaltechdesign.com/communication-design/

A team based at Standford's Law School and d.school have looked at how legal information is presented. Although the site does not focus solely on privacy, it contains a lot of great examples of different ways privacy information could be presented.

Surveys conducted into attitudes to Privacy

European Commission Eurobarometer 431 - Data Protection

http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2075

A 2015 survey conducted for the European Commission into opinions on data protection across Europe. It also contains country specific factsheets.

European Commission Eurobarometer 443 - ePrivacy

http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124

A 2016 survey conducted for the European Commission into opinions on key issues around online privacy. It also contains country specific factsheets.

KPMG Report - Crossing the line

https://home.kpmg.com/uk/en/home/insights/2016/11/crossing-the-line.html

KPMG conducted research with almost 7000 people across the works to understandard the line between 'creepy vs. cool' and how consumers felt about the use of their personal data.

Other examples of Privacy Guidelines

GSMA Mobile Privacy Guidelines

https://www.gsma.com/publicpolicy/mobile-privacy-principles

The GSMA have developed a set of privacy principles specifically for mobile users, many of their principles overlap with the principles outlined in this document.

Design My Privacy - Tijmen Schep (Book, published 2017)

https://www.tijmenschep.com/design-my-privacy/

Referenced in places in this document, this book contains 8 principles for privacy design. It was created as part of an initiative by the MOTI design museum and contains a lot of examples.

Privacy by Design

https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

The 7 foundational principles of Privacy by Design. Also related to this is another report looking at Privacy by Design and User Interfaces (https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces_Yahoo.pdf)

Resources for GDPR

Information Commissioner's Office - Guide to GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The UK Information Commissioner's Office has put together a good guide to GDPR.

ICO Consent Guidance Consultation

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/consent/ and

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/gdpr-consent-guidance/

The Information Commissioner's Office in the United Kingdom recently held an ICO and stakeholder consultation entitled' GDPR consent guidance'. The results of this are being analysed and are estimated to be published in December 2017.

IAPP - 'The UX Guide to Getting Consent'

https://iapp.org/media/pdf/resource_center/UX_FINAL.pdf

The International Association of Privacy Professionals (IAPP) have published a guide 'The UX Guide to Getting Consent' based on the GDPR regulations. It includes a number of examples and more detailed considerations for designing consent mechanisms.

ICO - Privacy Notice Information

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

GDPR provide specific requirements for privacy notices and the ICO provides information about this.

EConsultancy - GDPR - How to create best practice privacy notices with examples

https://www.econsultancy.com/blog/69256-gdpr-how-to-create-best-practice-privacy-notices-with-examples

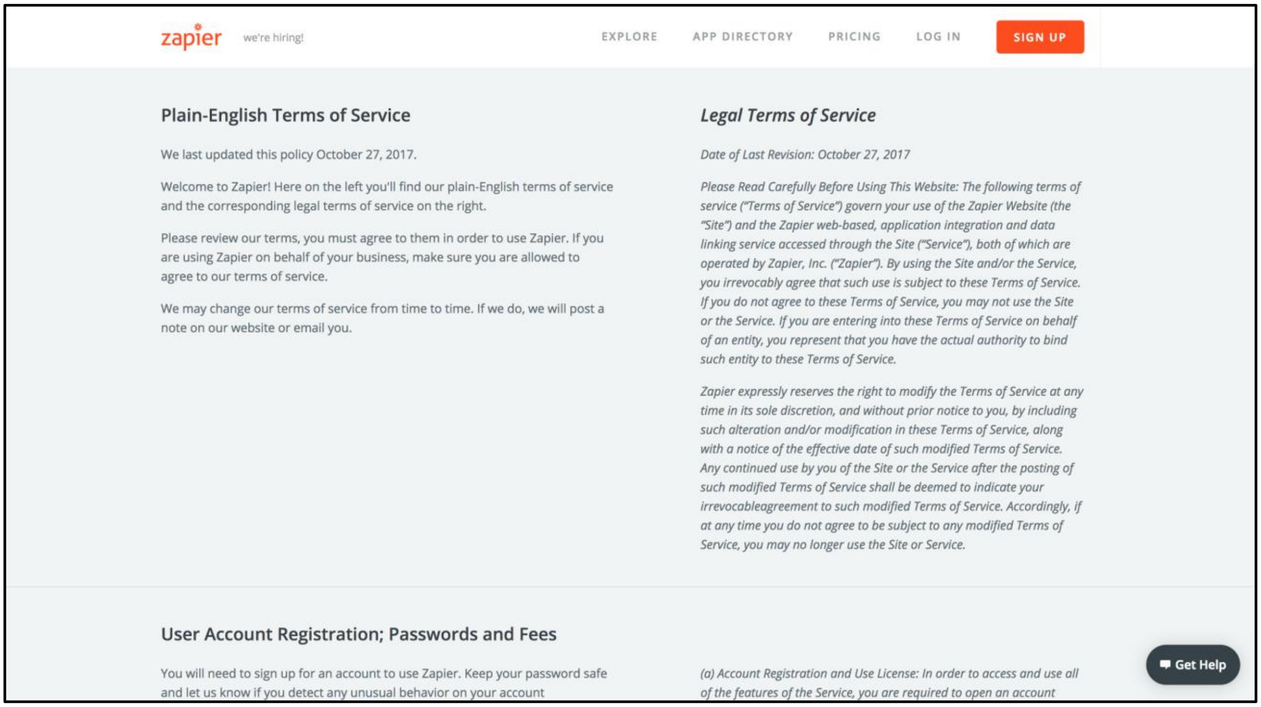
Appendix B - Examples

Included below are some examples of privacy information and controls from websites and research projects.

Zapier

https://zapier.com/terms/

Zapier have displayed the legal version of their terms and condition side by side with a plain English version.



Plain-English Terms of Service

We last updated this policy October 27, 2017.

Welcome to Zapier! Here on the left you'll find our plain-English terms of service and the corresponding legal terms of service on the right.

Please review our terms, you must agree to them in order to use Zapier. If you are using Zapier on behalf of your business, make sure you are allowed to agree to our terms of service.

We may change our terms of service from time to time. If we do, we will post a note on our website or email you.

Legal Terms of Service

Date of Last Revision: October 27, 2017

Please Read Carefully Before Using This Website: The following terms of service ("Terms of Service") govern your use of the Zapier Website (the "Site") and the Zapier web-based, application integration and data linking service accessed through the Site ("Service"), both of which are operated by Zapier, Inc. ("Zapier"). By using the Site and/or the Service, you irrevocably agree that such use is subject to these Terms of Service. If you do not agree to these Terms of Service, you may not use the Site or the Service. If you are entering into these Terms of Service on behalf of an entity, you represent that you have the actual authority to bind such entity to these Terms of Service.

Zapier expressly reserves the right to modify the Terms of Service at any time in its sole discretion, and without prior notice to you, by including such alteration and/or modification in these Terms of Service, along with a notice of the effective date of such modified Terms of Service. Any continued use by you of the Site or the Service after the posting of such modified Terms of Service shall be deemed to indicate your irrevocableagreement to such modified Terms of Service. Accordingly, if at any time you do not agree to be subject to any modified Terms of Service, you may no longer use the Site or Service.

User Account Registration; Passwords and Fees

You will need to sign up for an account to use Zapier. Keep your password safe and let us know if you detect any unusual behavior on your account

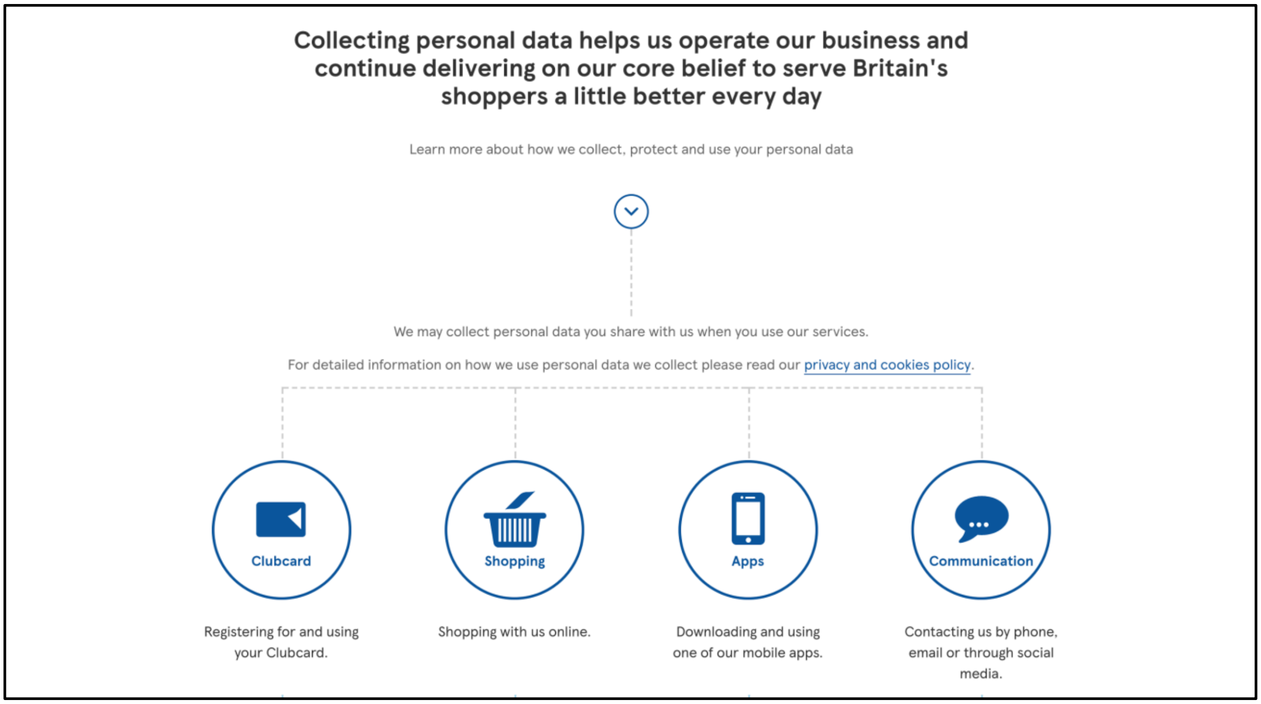
(a) Account Registration and Use License: In order to access and use all of the features of the Service, you are required to open an account

From Zapier (https://zapier.com/terms/)

Tesco

https://www.tesco.com/help/privacy-and-cookies/privacy-centre/

Tesco have a user-friendly privacy centre in which, among other things, they detail a customer's data journey including the types of data that may be accessible to third parties.



Collecting personal data helps us operate our business and continue delivering on our core belief to serve Britain's shoppers a little better every day

Learn more about how we collect, protect and use your personal data

We may collect personal data you share with us when you use our services.

For detailed information on how we use personal data we collect please read our privacy and cookies policy.

Clubcard — Registering for and using your Clubcard.

Shopping — Shopping with us online.

Apps — Downloading and using one of our mobile apps.

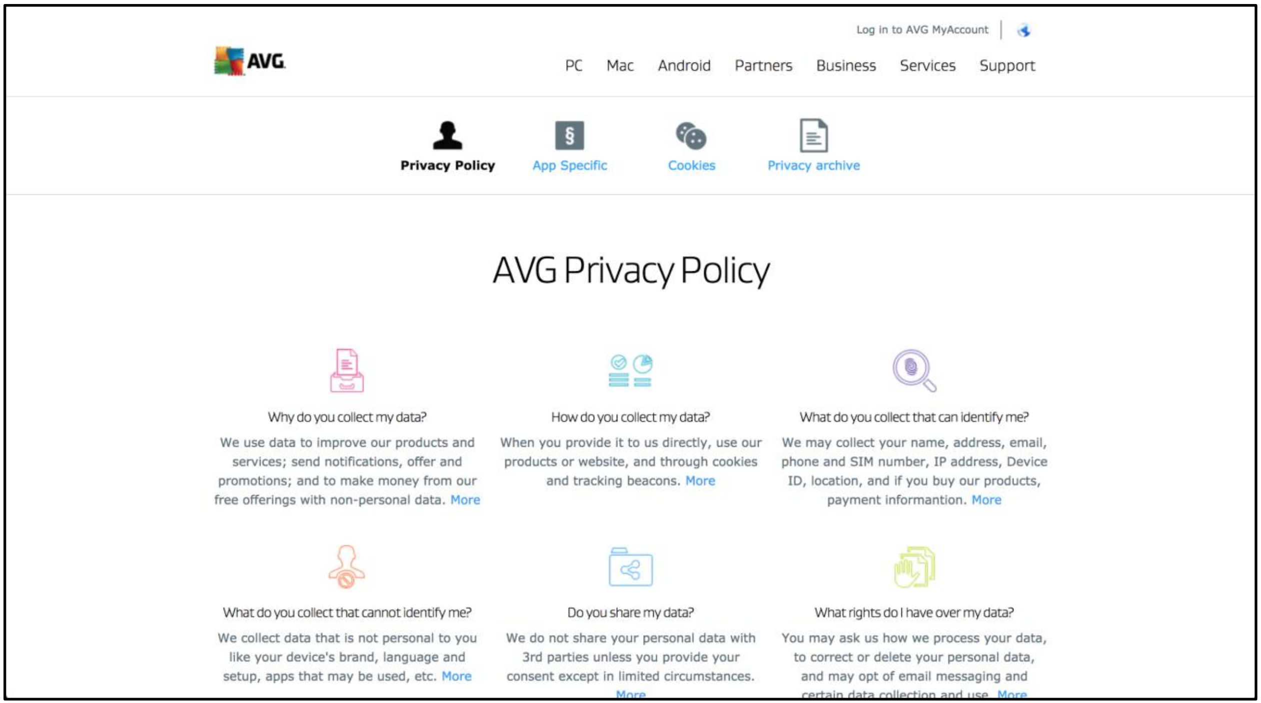
Communication — Contacting us by phone, email or through social media.

From 'Your data journey' in Tesco Privacy Centre - https://www.tesco.com/help/privacy-and-cookies/privacy-centre/tesco-and-your-data/your-data-journey/

AVG

https://www.avg.com/en-ww/privacy

AVG’s privacy policy is clear and simple to navigate. It uses clear language to explain how data is collected and used and what information can identify the user and what information cannot.



AVG Privacy Policy

Why do you collect my data?

We use data to improve our products and services; send notifications, offer and promotions; and to make money from our free offerings with non-personal data. More

How do you collect my data?

When you provide it to us directly, use our products or website, and through cookies and tracking beacons. More

What do you collect that can identify me?

We may collect your name, address, email, phone and SIM number, IP address, Device ID, location, and if you buy our products, payment informantion. More

What do you collect that cannot identify me?

We collect data that is not personal to you like your device's brand, language and setup, apps that may be used, etc. More

Do you share my data?

We do not share your personal data with 3rd parties unless you provide your consent except in limited circumstances. More

What rights do I have over my data?

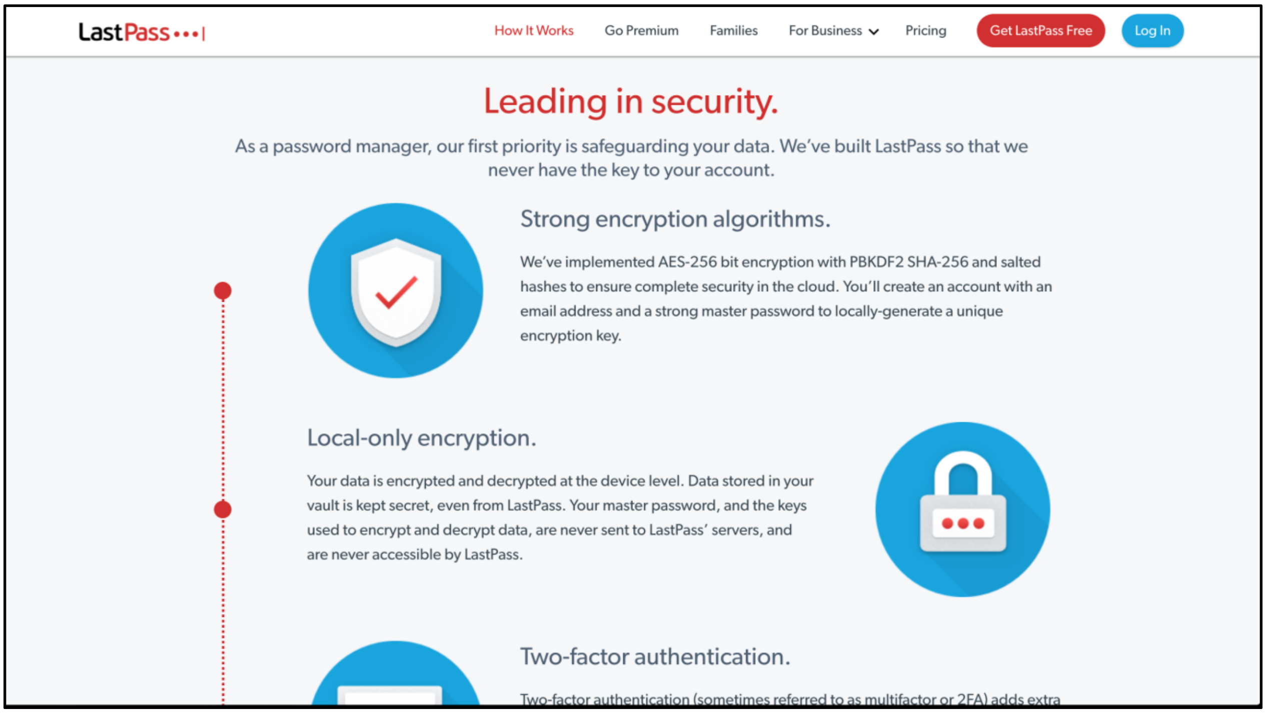
You may ask us how we process your data, to correct or delete your personal data, and may opt of email messaging and certain data collection and use. More

From AVG Privacy Policy (https://www.avg.com/en-ww/privacy)

LastPass

https://www.lastpass.com/how-it-works

LastPass contains an explanation on how and where data is encrypted.



Leading in security.

As a password manager, our first priority is safeguarding your data. We've built LastPass so that we never have the key to your account.

Strong encryption algorithms.

We've implemented AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes to ensure complete security in the cloud. You'll create an account with an email address and a strong master password to locally-generate a unique encryption key.

Local-only encryption.

Your data is encrypted and decrypted at the device level. Data stored in your vault is kept secret, even from LastPass. Your master password, and the keys used to encrypt and decrypt data, are never sent to LastPass' servers, and are never accessible by LastPass.

Two-factor authentication.

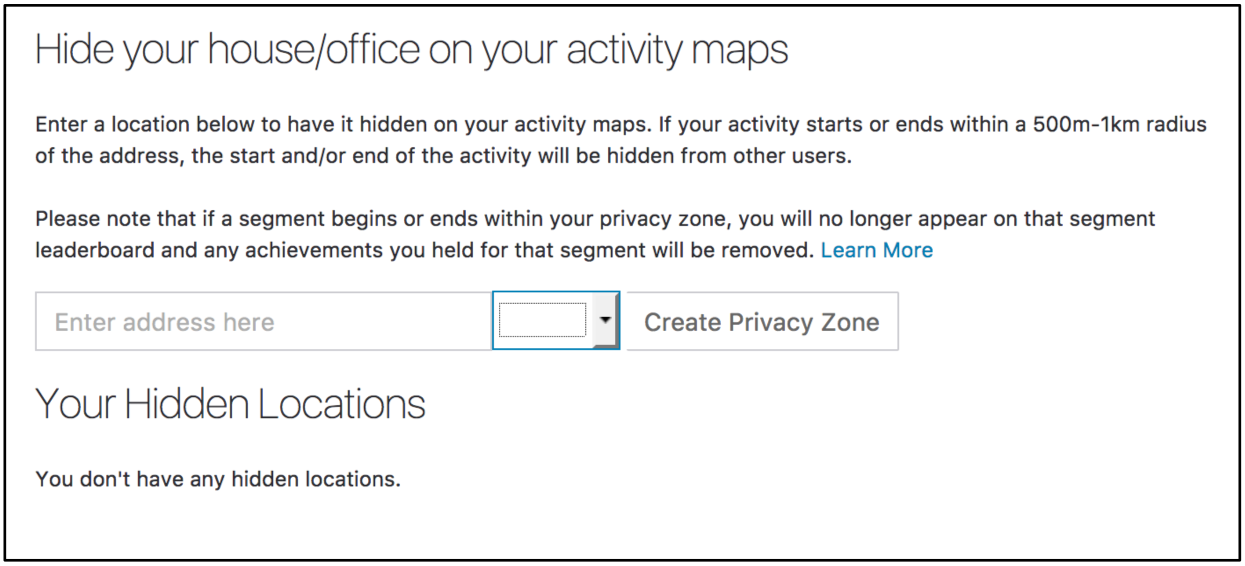
Two-factor authentication (sometimes referred to as multifactor or 2FA) adds extra

From LastPass how it works (https://www.lastpass.com/how-it-works)

Strava Privacy Zones

https://support.strava.com/hc/en-us/articles/115000173384-Privacy-Zones

Users of the Strava application are able to hide activity that takes place near certain addresses, for example a home address via Privacy Zones. By entering an address and a radius, if a user's activity starts or ends in this zone, the activity will be hidden from other users.



Hide your house/office on your activity maps

Enter a location below to have it hidden on your activity maps. If your activity starts or ends within a 500m-1km radius of the address, the start and/or end of the activity will be hidden from other users.

Please note that if a segment begins or ends within your privacy zone, you will no longer appear on that segment leaderboard and any achievements you held for that segment will be removed. Learn More

Your Hidden Locations

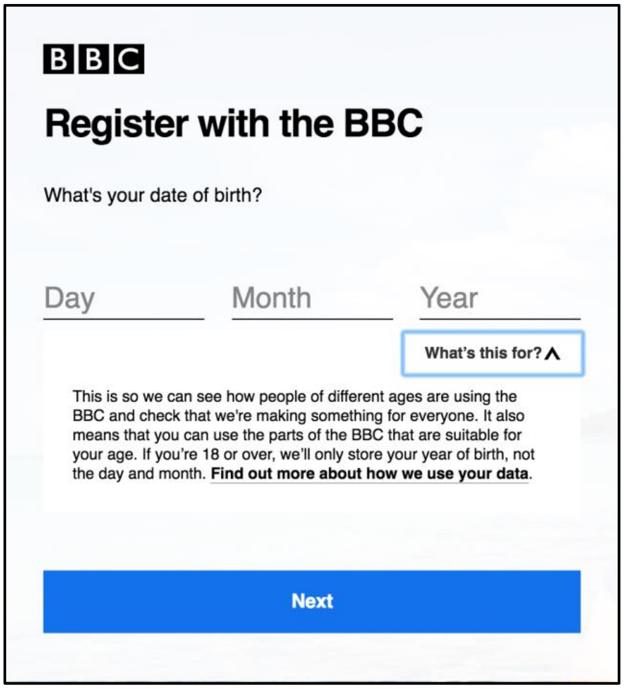
You don't have any hidden locations.

From Strava Privacy Zones (https://support.strava.com/hc/en-us/articles/115000173384-Privacy-Zones)

BBC Sign Up Process

https://account.bbc.com/register

An example of only storing required data is in the BBC sign up process. During this a user is asked to provide their date of birth to regulate which parts of the BBC the user is able to access. For users over 18, they inform the user that they will only store the year of birth and not the day and month.



BBC

Register with the BBC

What's your date of birth?

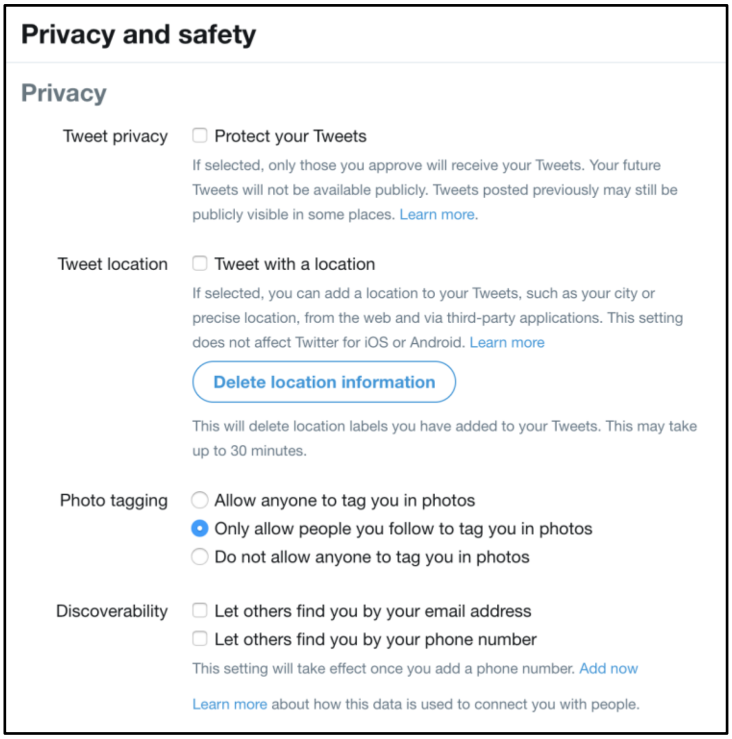
This is so we can see how people of different ages are using the BBC and check that we're making something for everyone. It also means that you can use the parts of the BBC that are suitable for your age. If you're 18 or over, we'll only store your year of birth, not the day and month. **Find out more about how we use your data**.

From BBC Sign Up Process (https://account.bbc.com/register)

Twitter Privacy Settings

https://twitter.com/settings/safety

Twitter have provided detailed options and controls for their privacy settings with clear explanations.



Privacy and safety

Privacy

Tweet privacy

□ Protect your Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location

□ Tweet with a location

If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging

○ Allow anyone to tag you in photos
● Only allow people you follow to tag you in photos
○ Do not allow anyone to tag you in photos

Discoverability

□ Let others find you by your email address
□ Let others find you by your phone number

This setting will take effect once you add a phone number. Add now

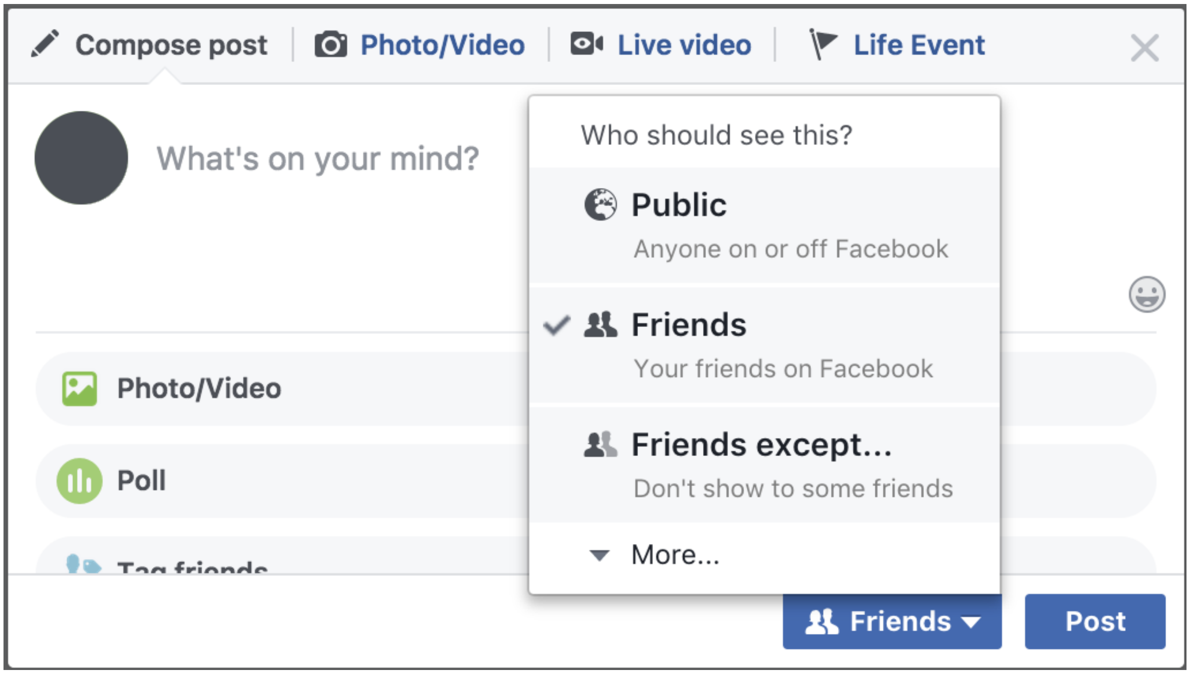
Learn more about how this data is used to connect you with people.

A portion of Twitter's privacy options (https://twitter.com/settings/safety)

Facebook Post Privacy Settings

https://www.facebook.com

Facebook gives people control over the audience of their social media posts. At the point of creating a new post the user is given the option to change the audience. The options have a concise and clear explanation of who will be able to view the post.



Selecting the audience for a post on Facebook (www.facebook.com)

Pagefair

https://pagefair.com/blog/2017/gdpr-consent/

Pagefair have created sketches of possible GDPR consent dialog.

Projects by IF

https://projectsbyif.com/blog/user-centred-consent-at-mozfest

Project by IF recently ran a workshop at MozFest looking at how to design user centered consent.

Privacy Icons

https://wiki.mozilla.org/Privacy_Icons

A project that designed icons to convey privacy information.

Privacy Nutrition Labels

https://cups.cs.cmu.edu/privacyLabel/

A 2010 project by Carnegie Mellon University looked at applying the principles of nutrition labels to privacy.

References

1, 6, 8, 22, 23, 43 - Bassi, Eleonora (Politecnico di Torino), Ciurcina, Marco (Politecnico di Torino), De Martin, Juan Carlos (Politecnico di Torino)… "D1.8 Legal frameworks for digital commons DECODE OS and legal guidelines" Oct 2017.

2, 14, 18 - Danezis, George. Bano, Shehar. Al Bassam, Mustafa… "D1.4 - First version of the DECODE architecture.' Oct. 2017 https://decodeproject.eu/publications/decode-architecture-first-version Accessed 23 Nov. 2017

3, 9 - Symons, Tom. Bass, Theo. "Me, my data and I:The future of the personal data economy | DECODE." 18 Sep. 2017, https://decodeproject.eu/publications/me-my-data-and-ithe-future-personal-data-economy. Accessed 21 Nov. 2017.

4, 10 - Irving, Jill, Barritt, James... "Pilot Scenarios and Requirements | DECODE." 27 Sep. 2017, https://www.decodeproject.eu/publications/pilot-scenarios-and-requirements. Accessed 21 Nov. 2017.

5, 13, 16 - DECODE Proposal: ICT-12-2016 DECODE

15 - Alexander Grech, Anthony F. Camilleri - "Blockchain for education" http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf Accessed 22 Nov. 2017

7, 44, 45, 46 - Hoepman, Jaap-Henk. Bano, Shehar, Bassi, Eleonora..., - "Privacy Design Strategies for the DECODE Architecture" June 2017

11, 28 - van Kranenburg, Rob. Bonelli, Federico. Veldman, Jennifer "Co-creation framework, methodologies and templates" Jul. 2017

12, 19 - Roio, Dennis, "DECODE language design patterns" Nov. 2017

17 - Al-Bassam, Mustafa, Bano, Shehar, Danezis, George… "D3.1 - Survey of Technologies for ABC, Entitlements and Blockchains" June 2017

20, 21, 25, 31,47, 50 - "General Data Protection Regulation - European Commission." 4 May, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Accessed 18 Oct. 2017.

24 - "Guide to the General Data Protection Regulation (GDPR) | ICO." https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr. Accessed 22 Nov. 2017.

26, 27- "The Distribution of Users' Computer Skills: Worse Than You Think." 13 Nov. 2016, https://www.nngroup.com/articles/computer-skill-levels/. Accessed 24 Nov. 2017.

29, 34 - Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles - Information and ...." https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Accessed 21 Nov. 2017.

30 - Cavoukian, Ann. Weiss, Justin B. "Privacy by Design and User Interfaces - Information and Privacy ...." 1 Jun. 2012, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces_Yahoo.pdf. Accessed 21 Nov. 2017.

32 - Patry, W., 2009. Moral Panics and the Copyright Wars. Oxford University Press

33 - "GDPR: A Step Towards a User-centric Internet? | Intereconomics." https://archive.intereconomics.eu/year/2017/4/gdpr-a-step-towards-a-user-centric-internet/. Accessed 23 Nov. 2017.

35 - "Desktop vs Mobile vs Tablet Market Share Europe | StatCounter ...." http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe. Accessed 24 Nov. 2017.

36 - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), see http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

37 - Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

38 - “Consent | ICO." https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/consent/. Accessed 23 Nov. 2017.

39 - “Data controllers and data processors: what the difference is and what the governance implications are”, Data Protection Act, https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

40 - “Consultation: GDPR consent guidance”, https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

41 - “WCAG Overview | Web Content Accessibility Guidelines Overview”, https://www.w3.org/WAI/intro/wcag. Accessed 21 Nov. 2017.

42 - "Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines ...." 26 Feb. 2015, https://www.w3.org/TR/mobile-accessibility-mapping/. Accessed 24 Nov. 2017.

48 - Schep, Tijmen “Design My Privacy” BIS, 2017

49 - "Mobile Privacy Principles - GSMA." http://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf. Accessed 22 Nov. 2017.

51 - "Police renew appeal for cyclists to protect personal information on ride ...." 13 Oct. 2015, http://www.cyclingweekly.com/news/latest-news/police-renew-appeal-for-cyclists-to-protect-personal-information-on-ride-sharing-sites-195381. Accessed 21 Nov. 2017.

52 - "Police warn cyclists of thieves using GPS apps to steal bikes - Cycling ...." 15 Nov. 2014, http://www.cyclingweekly.com/news/latest-news/police-warn-cyclists-thieves-using-gps-apps-steal-bikes-144820. Accessed 21 Nov. 2017.