sdt

How to deal with data management and protection during a project?

A useful framework made of actionable guidelines
and tips for designers struggling with data-related projects.

Tutorial + Framework

00 Introduction

Data Privacy is a human right. It refers to the right to privacy of personal information that people provide to public or private organizations to get the services and products they need.
Today, in the era of massive digitization, where emerging technologies (such as the Internet of Things, Artificial Intelligence, Machine Learning and Analytics, Blockchain, etc...) are increasingly used both in public and private sectors, the topic of privacy is becoming particularly relevant.
And while extensive data collection facilitates global surveillance, dilemmas arise for innovators and designers.

On the one hand, regulators around the world are reviewing laws and norms to consider the peculiarities of rapidly evolving emerging technologies and protect human rights. But, as we know, regulations are often rigid, slow to be adapted and adopted, and they do not always encompass the ethical perspective. Moreover, it happens that regulations regarding data protection conflict between different countries, together with other challenges that designers need to be aware of.
For example, organizations might use technologies to set up experiments by collecting private behavioral data (e.g. Pokemon Go). No one knows when and how the results of these experiments will be used. Or data collectors don't take responsibility for the use of data by the third parties with whom they're sharing the data (infinite loop). Or again, personal data can be used by politicians, marketers, etc. to target/nudge people to perform certain actions without fully realizing the reasons for and consequences of their actions (e.g. Cambridge Analytica scandal).

As designers we cannot avoid taking into account the protection of our users' privacy when envisioning new solutions for products and services, both enhancing the comprehension of privacy-related processes, and giving them the chance to express their privacy preferences and maintain the control on their experiences.

As a designer, have you ever thought of your responsibility in the protection of others' personal data? Do you know that there are different types of data that require different treatment?

** This toolkit was developed by students of the VII edition of the Specializing Master in Service Design of POLI.design - Politecnico di Milano within a didactic activity, with the support of service designers with expertise in data privacy. No validation process has been undertaken to verify its usability and efficacy. If you have the chance to use it please send us a feedback at* ***info@servicedesigntools.org****. Your case study could be included into the platform as a reference to support further applications.*

Since data management and protection is such a big and complicated topic, we developed the Data Management Framework for Service design*, which includes suggestions and tools to be used at different stages of the design process. Some are associated with legal issues, some others are more technical and can facilitate the collaboration between designers and engineers/technologists, or aim at facilitating the communication with the users and operationalizing certain ethical concepts. A synthetic and designer-friendly reference frame that can help a design team to manage data-related issues into everyday practice.

Resources

Deloitte (2016), Reimagining customer privacy for the digital age: Going beyond compliance in financial services. https://www2.deloitte.com/content/dam/Deloitte/br/Documents/-financial-services/Deloitte-reimagining-consumer-privacy-for-digital-age.pdf

Soffer, T., & Cohen, A. (2014) Privacy Perception of Adolescents in a Digital World. Bulletin of Science, Technology & Society, 34(5-6), 145–158.

Vitale, J., Tonkin, M., Herse, S., Ojha, S., Clark, J., Williams, M. A., Whang X. & Judge, W. (2018, February). Be more transparent and users will like you: A robot privacy and user experience design experiment. In Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction (pp. 379-387)

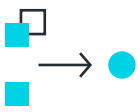
Sapere research group & Covec (2015) Data Driven Innovation in New Zealand, https://srgexpert.com/wp-content/uploads/2017/11/Data-_Innovation_Report_WEB.pdf

Fletcher J., 2017, Data as an economic growth factor and currency: Personal API's, data management, and the emerging data economy. Raft. https://raftcollective.com/media/Raft-Data_as_an_economic_growth_factor_and_currency.pdf

DATA MANAGEMENT FRAMEWORK FOR SERVICE DESIGN

A useful framework made of actionable guidelines and tips for designers struggling with data-related projects.

01



Clarify the purpose for data collection

WHAT

- Identify the purpose for data usage.

- Understand the service ecosystem with all the actors involved in the process.

- Define each stakeholder group's responsibilities in data privacy protection.

- Check every data-related issue is under control.

WHEN

At the beginning of the design process or as soon as the need for data collection arises (either it being related to user research or UX design).

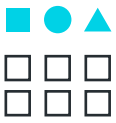
HOW

• The decision matrix - Canvas 1

• Define and understand public benefic and user need - Data Ethics Framework

• Digital security and Privacy Protection UX Checklist

02



Identify the type of data you need

WHAT

- Understand the types of data you need to gather.

- Check up the laws and the regulation in force in your country regarding data processing.

- Classify data based on its sensitivity level and come up with different conditions for data sharing depending on the sensitivity.

- Prepare the data collection permissions according to the different data types you are willing to collect.

- Identify and plan for potential data quality issues and biases.

WHEN

As soon as the data collection planning starts, and anytime new types of data need to be collected during the process.

HOW

• The Data Spectrum

• Information and data sensitivity classification - Data responsibility guidelines

• Consent for data use

03

Understand how the data flows

WHAT

- Describe the information journey specifying inputs, outputs, where data is stored, and where it travels.

- Identify and plan for potential limitations that might come from data misuse or missing data.

- Identify and plan for potential limitations in terms of algorithmic and human biases.

WHEN

Throughout the process of envisioning and prototyping new solutions.

HOW

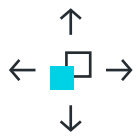
• Data flow diagram

• Data Map Template - The Privacy toolkit

• Mapping the system - IDEO's AI ethics cards

• Data Responsibility plan template - Data responsibility guidelines

04



Be aware of data impact

WHAT

- Provide all stakeholders with clear and comprehensible information for data sharing.

- Educate users to be always aware of their rights and potential threats.

- Consider all aspects of user experience and plan for transparent communication.

- Identify and communicate potential data impacts for each stakeholder group.

- Come up with measuring and treatment mechanisms for these impacts.

WHEN

After the new solution is tested and launched, at the evaluation stage.

HOW

• Information sharing protocol - template - Data responsibility guidelines

• Personas for privacy and security

• Pillars for data handling - Raft framework

• Privacy statement

• Personal data breaches - Guide to the general data protection regulation (GDPR)

01 Clarify the purpose of data collection

Before starting to work on a data-related project, it's important to align everybody's vision of the project and the role data might have. This initial alignment will provide a solid basis for later decisions on data processing, sharing, communication and so on.

The purpose for data collection can apply to the user research conducted to elaborate the service solution, to data gathering through digital platforms as part of the solution itself.
Concerning the first case, the availability of digital research methods and the enhancements of the use of these methods in commercial settings have brought new dimensions to the privacy discussions within the context of user research. In fact, user researchers have the ethical responsibility to collect information properly, firstly allowing participants to give informed consent, and then processing data in the right way when research is finished, considering the type, the scope, the circumstances and the purpose of the processing along with connected risks.
Similarly, concerning data gathering through digital platforms, purposes can be manyfold. Some examples: retailers might use sales data and cloud-based point-of-sale software to understand the popularity of different products and ensure that they have the right levels of stock at the right times. Insurance might use claims registers to assess the validity of a claim and/or decide whether or not to offer cover, or to detect insurance fraud. Frontline health providers might collect data to proactively determine the treatment needs of their patients and work to prevent the need for more costly and traumatic treatments. Logistics and transport operators might use data on road and traffic conditions to optimize their operations and routes. And so on...

TIPS

- Identify the purpose for data collection and usage by answering questions as those you can find in the The decision matrix - Canvas 1 by Nesta, or the Data Ethics Framework - Define and understand public benefic and user need by UK Government Digital Service;
- Understand the service ecosystem with all the actors involved in the process to clarify the different roles and responsibilities of each actor in data collection and processing and data privacy protection . System maps can help doing the job.
- Check you have considered (or will consider) all the data-related critical aspects throughout the different phases of data management by building a checklist or opting for something like the Digital security and Privacy Protection UX Checklist

02

Identify the type of data you need

Once the purpose for data collection is clear and shared within the team, the need for data responsibility arises: a set of processes and procedures that allow the safe management of personal data during the different phases of the project.

First of all, while users involved in your research are asked to agree the request for consent for data collection, when it comes to data that are readily available (e.g. online reports, tweets, google trends,...), do not forget about the necessity to ask for permission to use them as well, or to follow and respect the terms of use of each online platform you are searching on.
Typically, designers have to deal with various types of personal data collected, from self-reported information to digital exhaust (the information that users generate during their daily digital lives). Within this context, you not only need to understand the legal requirements to meet privacy regulations, but also which treatments to put in place according to the sensitivity of that type of data.
In fact, while personal identifiers (such as names and surnames) are considered sensitive by definition, there are also nuanced categories of sensitive information that should be treated with attention by designers and their teams.
When thinking about how data will be managed and shared in your project, it's important to first understand the characteristics of data and classify them by sensitivity levels, then you can determine which are the set of rules for each of those levels.

TIPS

- Understand the types of data you need to gather referring to common classification as that you can find in The Data Spectrum by Open Data Institute;
- Check up the regulations in force in your country regarding data processing (e.g GDPR in Europe). If you're serving international clients, you should be even more careful to adapt your solutions to different and sometimes conflicting regulations;
- Prepare and submit the required data collection informed consents according to the different data types you are willing to collect, such as the Consent for Data Use suggested by Digital Impact
- Classify data based on their sensitivity level and come up with different conditions for data sharing depending on the sensitivity. You can use the Data Classification Matrix developed by The United Nations Office of The Humanitarian Affairs (OCHA).
- Identify and plan for potential data quality issues and biases, checking the documentations of your sources (or asking the collectors to specify the details).

03 Understand how data flows

When working on data-related projects, it is useful to understand how data flows, how different algorithms process them and how they are shared. Understanding the mechanisms of data processing you could better protect your users' privacy and achieve fairer and more well-functioning design solutions.
When an algorithm is designed to process data and make predictions on them, you need to consider the consistency of data with the kind of outcome you expect. For example, you cannot predict users' creditworthiness based on their addresses. Designers should be conscious of these biases and participate in the design of the datasets to support analysts through their perspective on user experience.
Concerning data flows, you must also consider the possibility of data breach (when your database is accessed by third-parties without authorization). This security accident can hurt businesses or its users in serious ways. Even though designers are not necessarily responsible for such technicalities, it's crucial to be aware of the issue and work with technicians to come up with preventative and recovery mechanisms for unwanted exposure of confidential, sensitive data.

TIPS

- Describe the data journey specifying inputs, outputs, where data is stored, and where it travels compiling a Data flow diagram as that proposed by Lucidchart or the Data Map Template you can find in The Privacy Toolkit by Hewlett Packard Enterprise;
- Identify and plan for potential risks that might come from data misuse or missing data, building your Data Responsibility Plan. You can start from the template you can find in the Data Responsibility Guidelines developed by The United Nations Office of The Humanitarian Affairs (OCHA);
- Identify and plan for potential limitations in terms of algorithmic and human biases, for example following the principles suggested by IDEO's AI ethics cards.

04 Be aware of data impact

The need to think critically about data privacy doesn't end when the project is successfully launched. It is important to continue assessing the impact of data collection and processing on different stakeholders, and also remain updated with the rapidly changing legal and ethical regulations.
When sharing data with colleagues, clients and 3rd parties, you should know that not everyone has the same awareness about data privacy. Similarly, even if aware of their responsibilities, not everyone has the same level of training to share data in a safe and respectful way. It's not required to become a legal expert, but it's necessary to clarify under which conditions we can share data and which measures or methods we can adopt.
On the other hand, most users are not always aware of their privacy rights and of certain potential threats as they don't have full access to the service dynamics. By monitoring data journeys and sharing them transparently, designers can continue protecting users' rights, build long-term relationships with them, and act ethically.
When assessing the positive and negative impact on different stakeholder groups, you should first define these impacts (e.g. what will happen in case of data breach?) and then develop standardized metrics to evaluate them over time. It is also recommended to develop a systematic way to communicate these impacts so that stakeholders can act upon it.
This could be part of the designer's responsibilities as well, firstly to help make sure that visualized/analyzed data is interpreted in an ethical way, and then to communicate the impact of data collection to users and stakeholders as part of the design solutions.

TIPS

- Provide all stakeholders with clear and comprehensible information for data sharing filling an Information sharing protocol as the one you can find in the Data Responsibility Guidelines developed by The United Nations Office of The Humanitarian Affairs (OCHA);
- Educate users to be always aware of their rights and potential threats while building trustful long-term relationships for your client organizations. You might consider using Personas for privacy and security to highlight the knowledge and awareness gaps of different user types in terms of their data privacy rights and take punctual actions to improve user experience in order to fill the gaps. Or you can look at the Pillars for data handling elaborated by Raft Collective;

- Identify and communicate potential data impacts for each stakeholder group (e.g. inform users about third party data sharing or terms of services and make sure they have control over their information). You can look at the Privacy statement by Visual Contracts as a good example to follow;
- Come up with measuring and treatment mechanisms for these impacts.
To prevent data breaches you can look at the Guide to the general data protection regulation (GDPR) by the UK Information Commissioner's Office. Make sure to get creative with the metrics and to not miss the qualitative impacts.

Other useful links:

- https://datasociety.net
- https://simplysecure.org
- https://www.ryerson.ca/pbdce/
- https://responsibledata.io
- https://privacyinternational.org
- https://digitalimpact.io/toolkit/
- https://privacyinternational.org/taxonomy/term/512