TYPOLOGY OF DECEPTIVE PATTERNS PRACTICES related to data protection on social media interfaces

SKIPPING (2)

Designing the interface or user journey in such a way that **users forget** or **do not think** about all or some of the data protection aspects.

Deceptive snugness

Relying on the default effect which nudges individuals to keep a **pre-selected option**, users are unlikely to change this even if given the possibility.

Look over there

A data protection related action or information is put in **competition with another element** which can either be related to data protection or not. When users choose this distracting option, they are likely to forget about the other, even if it was their primary intent.

STIRRING (2)

Affecting the choice users would make **by appealing to their emotions** or using visual nudges.

Emotional Steering

Using wording or visual elements (such as style, colours, pictures or others) in a way that confers the information to users in either a **highly positive outlook**, making users feel good, safe or rewarded, or in a **highly negative one**, making users feel scared, guilty or punished.

Hidden in plain sight

Use a visual style or technique for information or data protection controls that **nudges users toward less restrictive** and thus more invasive options.

LEFT IN THE DARK (2)

The interface is designed in a way to **hide information** or controls related to data protection or to leave users unsure of how data is processed and what kind of controls they might have over it.

Conflicting information

Giving pieces of information to users that **conflict with** each other in some way. Users are likely to be left unsure of what they should do and about the consequences of their actions, therefore **likely not to take any** and to just keep the default settings.

Ambiguous wording or information

Using ambiguous and vague terms when giving information to users. They are likely to be left unsure of how data will be processed or how to exercise control over their personal data.

OBSTRUCTING (3)

Hindering or blocking users in their process of obtaining information or managing their data by making the action **hard or impossible** to achieve.

Dead end

While users are looking for information or a control, they end up not finding it as a redirection link is either not working or **not available at all**. Users are left unable to achieve that task.

Misleading action

A **discrepancy** between information and actions available to users nudges them to do something they do not intend to. The difference between what users expect and what they get is likely to **discourage them from going further**.

Longer than necessary

When users try to activate a control related to data protection, the user journey is made in a way that **requires more steps** from users, than the number of steps necessary for the activation of data invasive options. This is likely to discourage them from activating such control.

FICKLE (4)

The design of the interface is **inconsistent and not clear**, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing.

Lacking hierarchy

Information related to data protection lacks hierarchy, making information appear several times and being **presented in several ways**.

Decontextualising

A data protection information or control is located on a page that is **out of context**.

Inconsistent Interface

An interface is **not consistent** across different contexts or does not match users' expectations and habits.

Language discontinuity

Information related to data protection **is not provided in the official language(s)** of the country where users live, whereas the service is.

OVERLOADING (3)

Burying users under **mass of requests, information, options** or possibilities in order to deter them from going further and make them keep or accept certain data practice.

Continuous prompting

Pushing users to provide more personal data than necessary for the purpose of processing or to agree with another use of their data by **repeatedly asking** users to provide data or to consent to a new purpose of processing.

Privacy maze

When users wish to obtain certain information or use a specific control or exercise a data subject right, it is particularly difficult for them to find it as they have to **navigate through too many pages** in order to obtain the relevant information or control, without having a comprehensive and exhaustive overview available.

Too many options

Providing users with (too) many options to choose from. The **amount of choices** leaves users unable to make any choice or make them overlook some settings, especially if information is not available.

This typology is based on the **European guidelines**:

> **Guidelines on deceptive design patterns in social media platform interfaces: how to recognise and avoid them?**
> Adopted on 14 February 2023 by the European Data Protection Board (EDPB).

These guidelines aim to identify best practices related to the interpretation and application of the GDPR (General Data Protection Regulation).

Relevant GDPR principles

Each of the deceptive design patterns described in this typology infringes one or more GDPR principles related to:

- **purpose limitation**
- **consent**
- data protection **by design** and **by default**
- **transparency** and **information**
- **the exercise of data subjects' rights**

All of these practices run counter to the **principle of fairness**.