Privacy Canvas

## About the Privacy Canvas

The Privacy Canvas is a tool that can be used by a business or on a project basis to help address privacy and data protection concerns during the innovation stages of that business/project. The Privacy Canvas has been modelled on the Business Model Canvas (Osterwalder & Pigneur, 2010), and can be used to help incorporate privacy by design early in that project or business’ growth. The Canvas will help people understand GDPR and help them protect their business/project by starting the discussion on it, even if the business or project owners have limited knowledge of GDPR. The Privacy Canvas could be used similarly to a “Data Protection Impact Assessment (DPIA)” except for non high-risk projects. It is intended that the Privacy Canvas be developed alongside the creation of a Business Model Canvas and possibly an Ethics Canvas (Online Ethics Canvas, 2017), and could be further developed iteratively with the Business Model Canvas.

A main motivation for this project is to consider the impact of the new “General Data Protection Regulation”, which came into effect in May 2018. This project is also Maurice Buckley’s final year project for his fourth year as a Computer Science student at Trinity College Dublin.

## How It Works

The Canvas has been divided into blocks 1-9 which each hold a particular purpose, described below:

**Blocks 1-3:** These blocks are about the data subjects and the data that is being stored.

**Blocks 4-6:** How the business/project cooperates with the data subjects.

**Blocks 7-8:** Privacy and how the data is being protected.

**Block 9:** Preparation for a data breach.

## About Each Block

**1. Data Group(s)**

What type of people do you hold personal data on? Employees/Customers/Adults/Children etc?

**2. Data Type**

What type of data do you hold? Children data? Sensitive data? Biometric data(data that could identify a person)?

**3. Purpose and Accuracy**

What is the purpose of keeping this data? Is the data being updated to uphold its accuracy? Is there a time limitation on the storage of the data? Is the data only being used for the initial required use?

**4. Consent**

Has consent been asked for data collection or will it be asked? Is it presented clearly? Is consent revocable?

**5. Transparency**

Is there transparency in the processing and use of the data? I.e: Info notices, paper trails etc.

**6. Data Rights**

Can data subjects access their data on request? Can the data be erased? Can data subjects object to certain types of use of the data eg: direct marketing? Will data subjects be notified on a data breach?

**7. Storage**

Is there a storage time limitation? What technical measures have been taken to protect personal data from un-authorised access? What level of security is needed?

**8. Data Governance**

What measures have been implemented/completed to reduce the risk/impact of a breach? Eg: Data Protection Impact Assessment (DPIA), audits, policy reviews, data protection officer, privacy canvas, certifications.

**9. Breach**

What happens after a data breach? Who is notified? Do you maintain an internal breach register? Possibility of administration fines.