

Datastreams Platform

IN RELATION TO THE EUROPEAN UNION
GENERAL DATA PROTECTION REGULATION
(GDPR)

Overview

INTRO With the new European Union General Data Protection Regulation (GDPR) as the minimum standard for the use of customer data by organisations, privacy by design has inevitably become a leading principle of data management. The GDPR was adopted in April 2016 and is effective since May 2018.

Whether your organisation is located inside, or outside of the EU you are very likely to be impacted by the GDPR and will need to take appropriate action or risk heavy fines. Non-compliance fees are significant and have two tiers. For breaches of key GDPR provisions fines will be up to 4% of your annual global turnover or €20m whichever is the greater. For less severe breaches, such as procedural infringements, these will be up to €10m or 2%.

As a company who has worked with and delivered data management solutions for over a decade we adopted privacy by design principles https://en.wikipedia.org/wiki/Privacy_by_design at an early stage. We employ it in all aspects of our business including the scope, functionality and operations of the Privacy and Compliance module within the Datastreams Platform. To become compliant with the GDPR and more importantly, gain customer acceptance, being able to instantly manage data globally is crucial.

Why do you need a solution for the GDPR?

If you are a data controller, or processor and your data processing activities relate to the offering of goods or services (paid, or free) to, or monitoring the behaviour (within the EU) of, EU data subjects, then you need to find a solution which meets the requirements within the GDPR. Getting this right should also be an essential element of good customer service. It will put people at the centre of the relationship and can help build customer confidence and trust in your brand. This will enhance your reputation, improve levels of engagement and encourage use of new services and products. It's one way to set yourself apart from the competition.

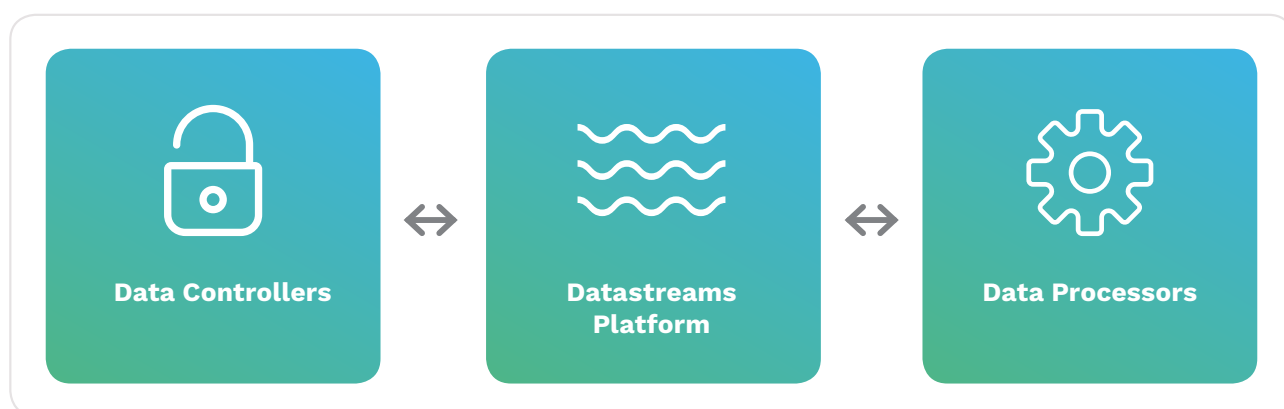


Figure 1. Instantly govern data management, globally

Are you able to meet these key data subject rights under the GDPR?

The following rights of data subjects need to be communicated (in addition to other information, such as e.g. the identity and contact details of the controller, the purposes of the processing, the period for which the personal data are stored, the existence (if applicable) of automated decision-making, etc.) at the time of collecting the personal data:

01 RIGHT OF ACCESS

Individuals have the right to obtain from you the confirmation as to whether or not personal data concerning them is being processed, and, if that's the case, have access to that personal data.

02 RIGHT OF RECTIFICATION

Individuals have the right to obtain from you the rectification of inaccurate personal data and the right to provide additional personal data to complete any incomplete personal data.

03 RIGHT TO ERASURE (“RIGHT TO BE FORGOTTEN”).

In certain cases, individuals have the right to obtain from you the erasure of their personal data.

04 RIGHT TO RESTRICTION OF PROCESSING

Individuals have the right to obtain from you restriction of processing, applicable for a certain period and/or for certain situations.

05 RIGHT TO DATA PORTABILITY

Individuals have the right to receive from you in a structured format their personal data and they have the right to (let) transmit such personal data to another controller.

06 RIGHT TO OBJECT

In certain cases, individuals have the right to object to processing of their personal data, including regards to profiling. They have the right to object to further processing of their personal data in so far as they have been collected for direct marketing purposes.

07 RIGHT TO BE NOT SUBJECT TO AUTOMATED INDIVIDUAL DECISION-MAKING

Individuals have the right to not be subject to a decision based solely on automated processing.

08 RIGHT TO FILING COMPLAINTS

Individuals have the right to file complaints about your processing of their personal data to the relevant data protection authorities.

09 RIGHT TO COMPENSATION OF DAMAGES

In case you breach applicable legislation on processing of (their) personal data, individuals have the right to claim damages from you for any damages such breach may have caused with them.

How does the Datastreams Platform help you?

Our partners use the 'Datastreams Platform' to instantly manage and govern the collection and distribution of omnichannel privacy compliant data. Developed by experts in data management, for over 10 years we have built up leading edge experience from hundreds of complex worldwide implementations in best of breed analytics solutions. We have utilised best practices and privacy by design principles then addressed these within the core of the platform. Now you can control your data across the globe and manage this throughout your organisation in a compliant way, helping you to meet with data protection and privacy legislations such as the GDPR.

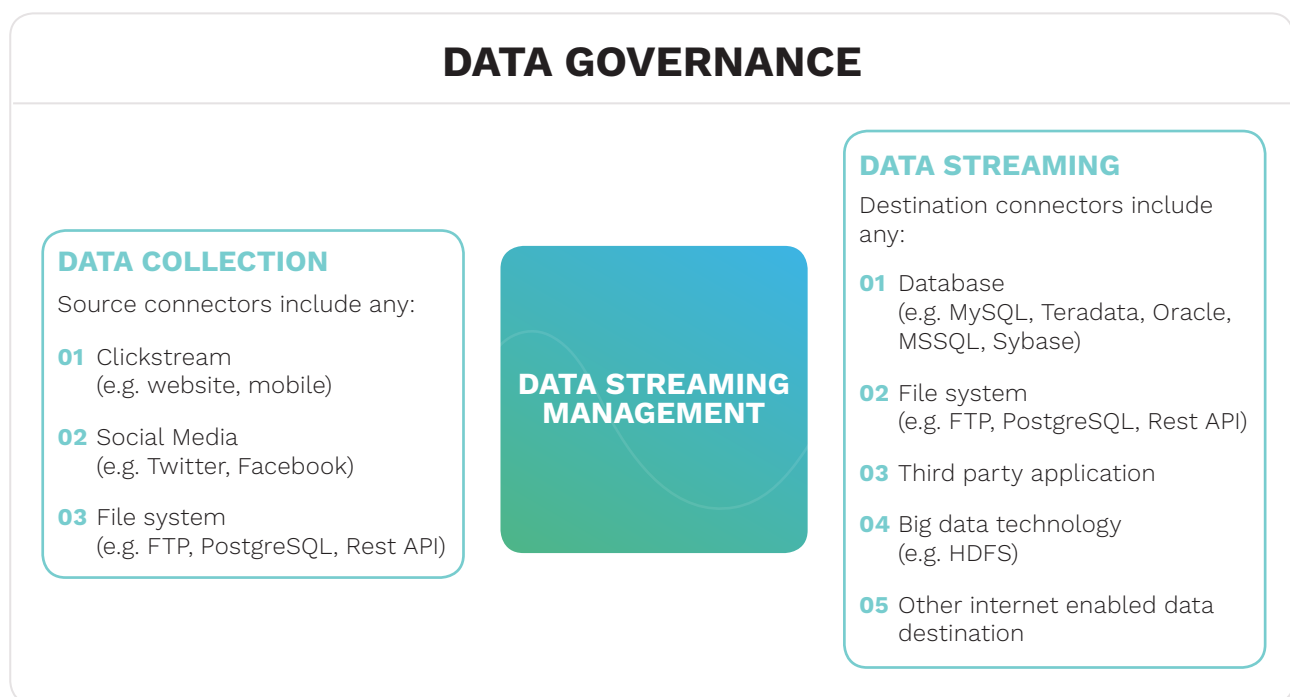


Figure 2. Datastreams Platform: Core proposition

As stated in April 2017, by the Information Commissioners Office (ICO):

- 01** The benefits of big data need not come at the cost of privacy.
- 02** Embedding privacy by design solutions into big data analytics can help to protect privacy through a range of technical and organisational measures.
- 03** Under the GDPR, privacy by design – known as 'data protection by design and by default' – will become a legal requirement.

Privacy level control	<p>Set up and manage any privacy hierarchy required and be able to manage this at a data parameter and Destination Connector level.</p> <p>Only the parameters with lower or equal level to the Destination Connector Privacy level can be mapped to a destination source.</p>
Privacy by design / default	<p>Structured approvals process. Only the data officer can publish the data stream to Go Live.</p> <p>Every Parameter requires a Privacy level to be set. Every Connector requires a Privacy level to be set.</p> <p>Only Parameters with the correct Privacy levels are available to be mapped to the Destination Connector.</p>
Transparency	<p>Shows when and who has logged and from where and what areas or modules they accessed.</p> <p>Shows any changes made to the Data Model when and by whom.</p>
Governance	<p>User & Data Management: Manage User Access Set the Privacy Levels Check Users Access Logs</p> <p>Privacy Settings: Define Privacy Levels Assign Defined Privacy level to any Parameter Assign Defined Privacy level to any Destination Connector</p> <p>Parameter Mapping: Map Parameters to the Destination Connector. Only the Parameters with lower or equal level to the Destination Connector Privacy level can be mapped.</p>

A compliant data and analytics architecture for our partners and their clients.

Our partners regularly need to deliver a privacy compliant data and analytic architecture for their clients to solve use cases via their value-added solutions and managed services. The Datastreams Platform quickly and easily provides this via a privacy by design enabled, data preparation framework for our partners, on behalf of their clients. Using the Datastreams Platform, our partners collect data from omnichannel client sources and then send this, in a privacy compliant way, for further processing, storage and utilisation.

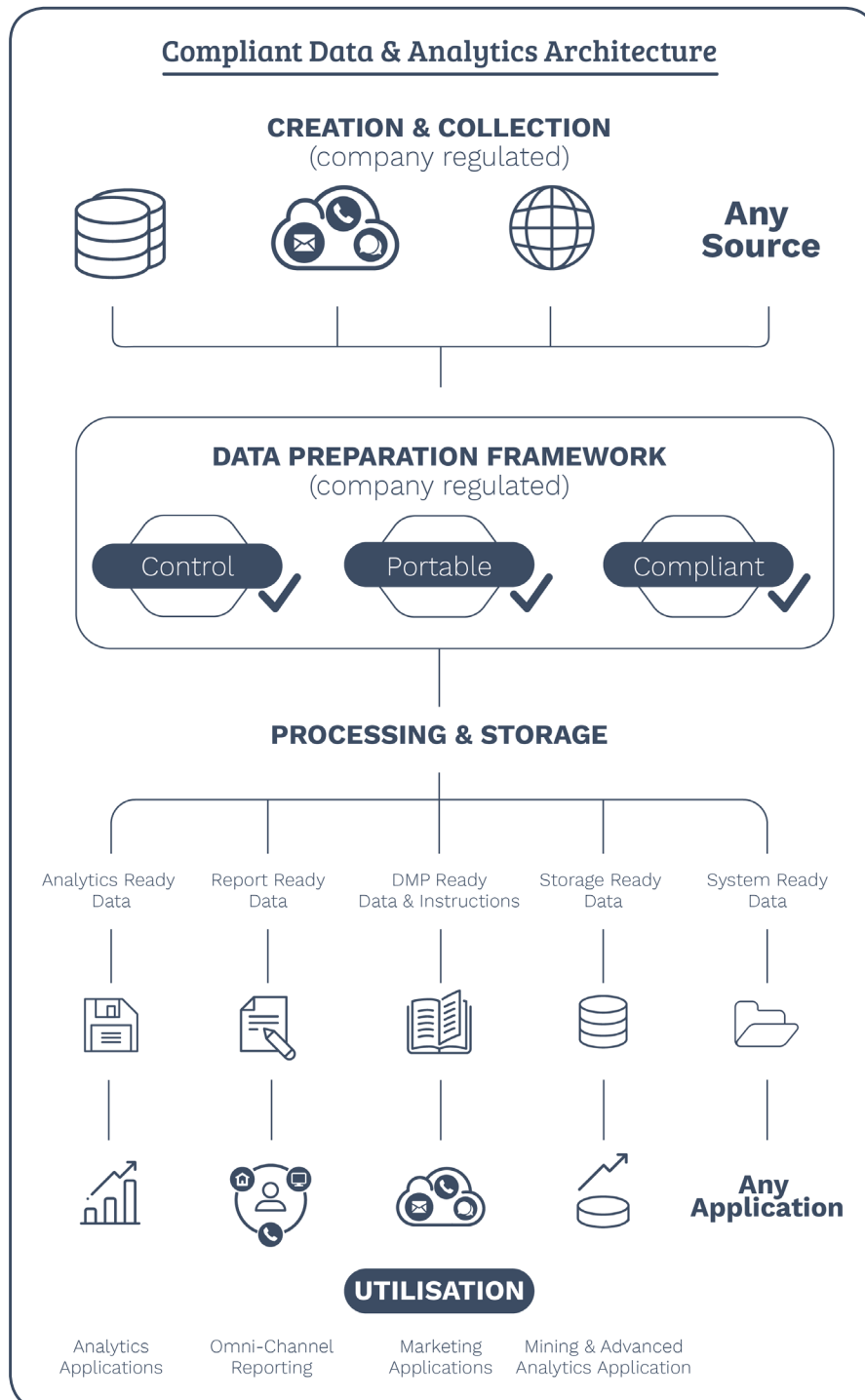


Figure 3. Compliant Data and Analytics Architecture

GDPR related features within the DSP.

01 DATA GOVERNANCE SECTION WITHIN THE MAIN MENU

Contains overview dashboards for all data streams; user administration; bespoke privacy settings and audits.

02 DATA PROTECTION OFFICER (DPO)

The DSP embeds a pivotal role for a Data Protection Officer (DPO) as also defined by the GDPR. This functionality facilitates active control of what data from which resources, are published to whom. To instantly govern data management globally for data controllers and processors, we have developed customer and partner portals. They both provide privacy information for all available data, based on different user rights and controls.

03 CONSENT MANAGEMENT & RIGHT TO BE FORGOTTEN (RTBF)

Consent management i.e. the capability to object to the use of data; and help facilitate the right to be forgotten. The building blocks for compliant data governance are built into the DSP.

04 TRANSPARANCY

Full transparency was at the heart of the DSP during its initial design and is fundamental to the current data architecture.

05 DATA MANGEMENT

Besides existing features and templates, significant configuration is possible. It is straightforward to add new functions into the DSP, e.g. monitoring data quality and applying specific rules to data that don't meet the standard. For example, incomplete records can be filtered out completely; repaired making use of predefined guidelines; or redirected to the product owner for further exploration when a critical level gets exceeded.

06 PRIVACY LEVELS

Set up and manage any privacy hierarchy required and manage this at a data Parameter and Destination Connector level. Only the parameters with lower or equal level to the Destination Connector privacy level can be mapped to a destination source.

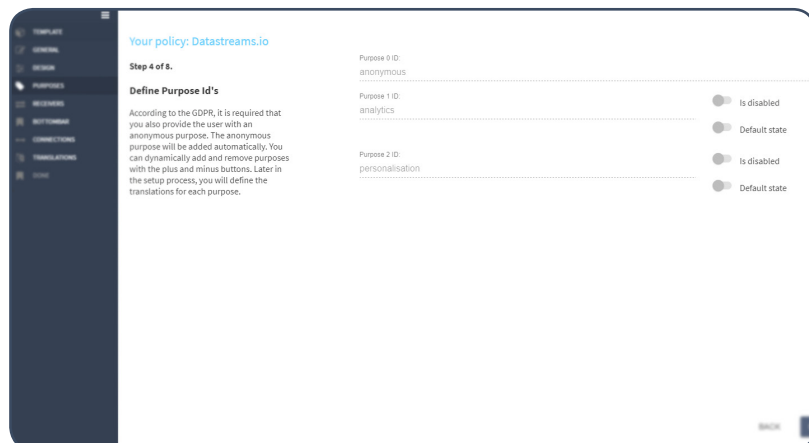
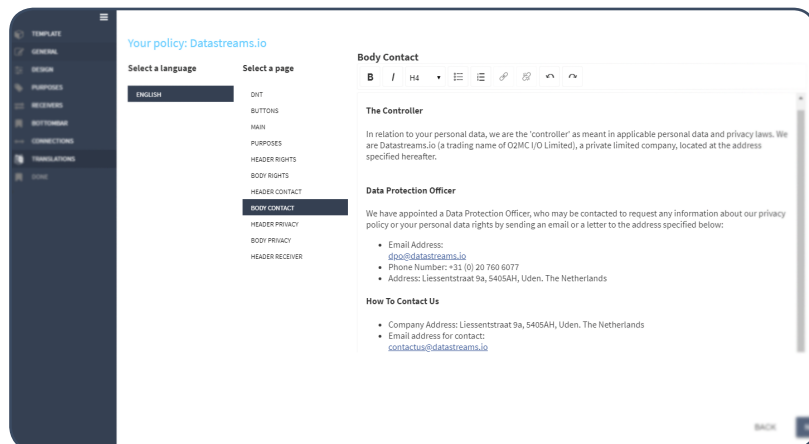
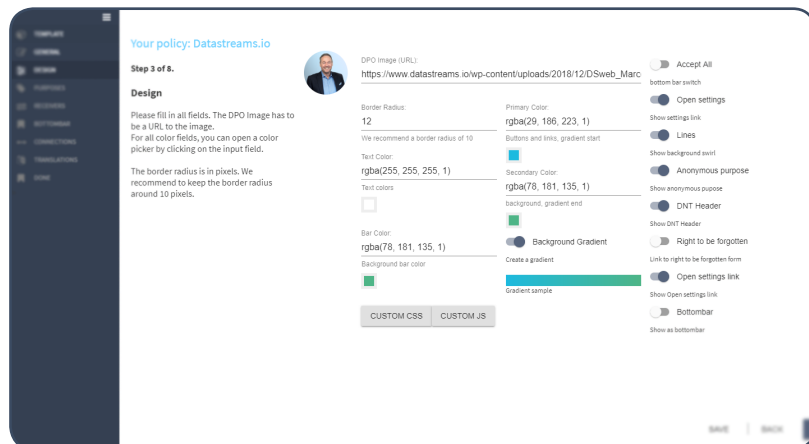
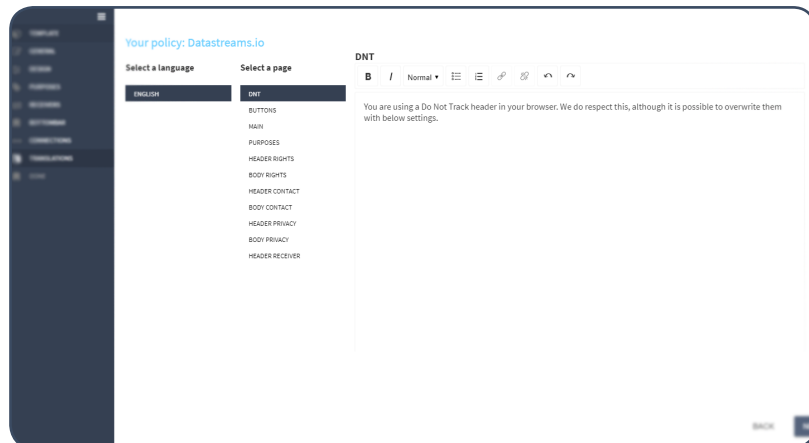


Figure 4. The Datastreams Platform: Governance user interface

More detailed DSP functionality includes.

01 EXTENSIVE DATA DESCRIPTIONS AUTOMATICALLY GENERATED

All standard data variables have a default data description, so your end-users easily understand what they are looking at. Add your own data descriptions to custom variables on the fly. You are also able to download and distribute the Data Model and all descriptions to share with other users or discuss them further within the team.

02 EXTENSIVE LOG FILES AUTOMATICALLY GENERATED

All modifications to Data Streams created with the Datastreams Platform are automatically logged to trace back any changes made by users of the Datastreams Platform.

03 IMMEDIATE ENCRYPTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) AND SENSITIVE DATA

Sensitive data such as IP addresses can be encrypted automatically to ensure no personally identifiable data exists in the data lifecycles.

04 STREAM APPROVAL FLOW FOR DATA PROTECTION OFFICERS

Publication of new data streams is controlled by the **Data Protection Officer** user role, so that no unauthorised data collection can be done by end users.

05 ADVANCED USER MANAGEMENT

Assign different user roles and rights to your users, with intuitive role definitions such as **Viewer**, **Streamer**, **Admin**, **Data Officer**, etc.

06 FLEXIBLE IN-STREAM VARIABLE ENCRYPTION

Intuitively enable encryption of captured data with the click of a button. Allow only Data Protection Officers to disable encryption of variables.

07 CUSTOMISE DATA MODELS TO MITIGATE DATA GOVERNANCE RISKS

Customise the standard data models per company, to exclude variables that introduce a privacy risk. These can be based on a company's privacy policy e.g. using an IP address.

08 BUILT IN OMNICHANNEL COOKIE CONSENT MECHANISM

Enable/disable the collection of a standard website variables based on the consent level given by a user.

09 DATA STREAM MANAGEMENT BASED ON HTTPS

Access the Datastreams Platform interface only through an SSL encrypted connection.

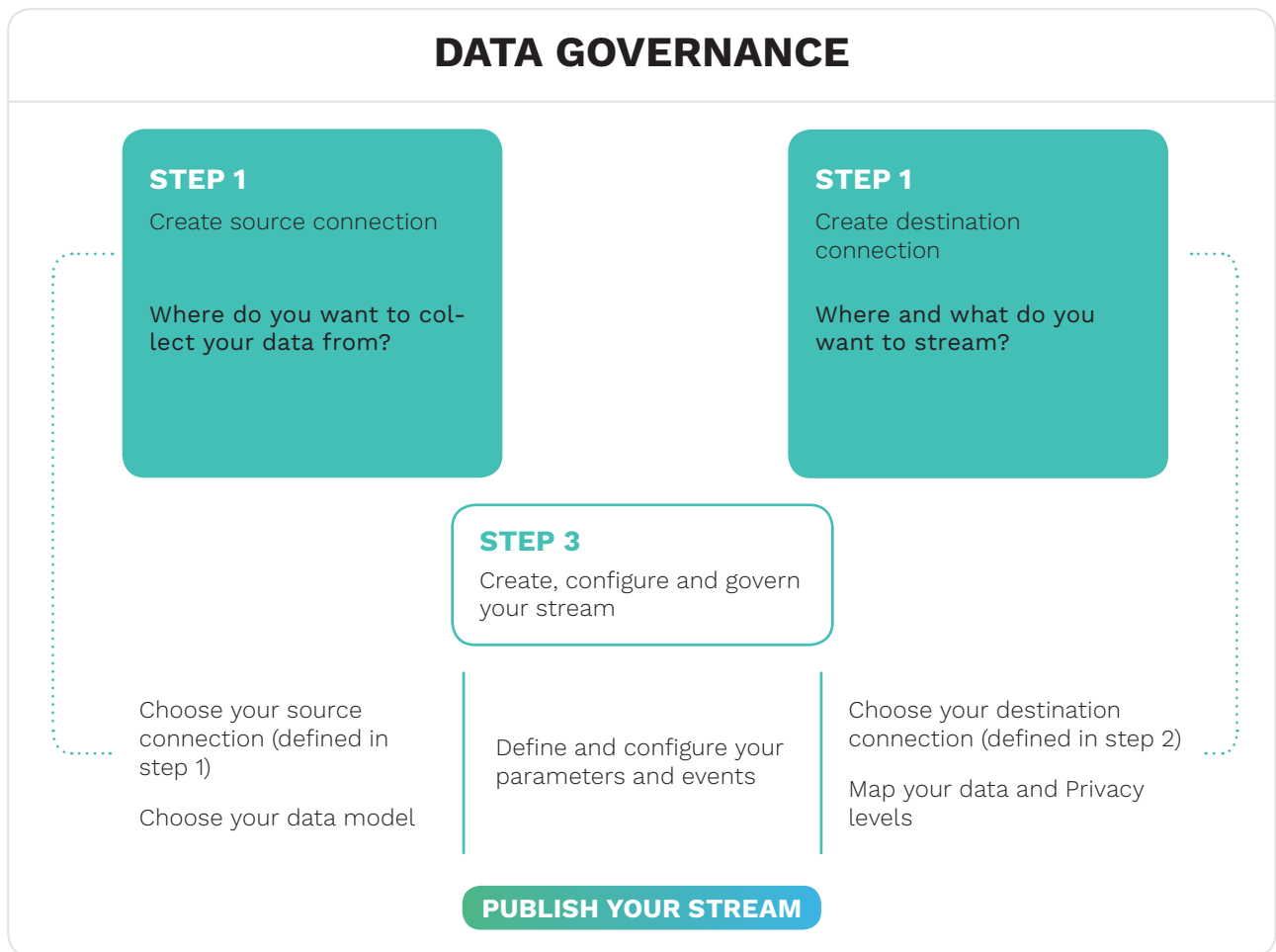


Figure 5. GDPR: data mastery in three steps

To learn more about the GDPR, see the official European Commission website:

https://ec.europa.eu/info/law/law-topic/data-protection_en

