Leader
by ecanvasser

Helping you to be **GDPR compliant**

01 Privacy Compliance Dashboard

Your campaign **Privacy Compliance Dashboard** is a **transparent view** where you identify the **contact information** for both your **Data Controller** and **Data Protection Officer**.
Within this dashboard, you can **map the individual personal data fields** with the **legitimate**, **lawful purpose** for processing that information, in compliance with **Article 13 section 2**.

02 Subject Access Requests

Under the **new regulation**, individuals have the r**ight to see what information you hold** about that person. In response to a **Subject Access Request**, you can share all personal information that you hold about that individual by viewing that persons data record on the **People Page**.
Individuals have the **right** to have their **data updated** or **removed**, which you can do through editing or deleting that person's record, again from the People Page.

03 Data breaches

Data breaches will happen over time and **it is important to be ready to deal** with them. Leader provides **activity logs** for team activity as well as a **data export history**. The majority of data breaches occur when **passwords are broken or stolen**.
Leader gives you the ability to c**hange passwords regularly** and to build password **'best-practice' into your team training**.
In this way you will **avoid the most likely route to a data breach**.
Our mobile phone **signup process** with authentication code is a **very secure onboarding system**. In the event of a data breach you can request to see the login credentials that might be connected to the breach.

04 Obtaining Consent

The new **e-signature consent** feature is available through the **Ecanvasser apps**.
You can **capture a person's consent** along with their **e-signature** as evidence of consent should you need to contact a person in the future for a specific purpose. There are, of course, **Unsubscribe functionality** built into email contacts and No Contact status option in the main database.
The **consent statement** needs to be a **clear and unambiguous message**, which provides individuals with 4 options of consent:

1. To be **contacted** regarding **ongoing issue(s)** which the individual has reported
2. To receive **updates regarding this campaign** for the duration of the campaign
3. To receive **news updates** regarding this candidate
4. To receive **information** regarding **volunteer** events

*Custom options are available

05 Field Canvassing

Face-to-face canvassing can be done in the community to capture **non-personally identifiable data** on voters. **Anonymised data** from this canvassing work is **displayed in raw and aggregated form**. Field canvassing also allows for consent to be captured and subsequently **personally identifiable data** such as **email, name, address and social media** handles.

06 Email

When you are using **individual email** or **email marketing** functionality on Leader you will need certain functionality to comply with **GDPR legislation**. Leader provides **advanced database filtering** capabilities on the range of data points that you hold on voters. You also have filtering based on the consent settings you have collected from people. All emails can contain **unsubscribe functionality** so that i**ndividuals can opt-out of future contact**. **Email statistics** and **open rates** are included in email analytics.

DATABASE

- Secure Database
- Data Minimization
- Auto Log- Out
- Anonymised Data in DB
- Encrypted EU Server
- Activity Logs/ Timestamps

COMPLIANCE

- Permission Levels
- Data Breach Reportline
- Consent to Contact Settings
- Unscribe + No Contact
- E-signature Capability
- Subject Access Requests
- Privacy Dashboard

TERMINATION

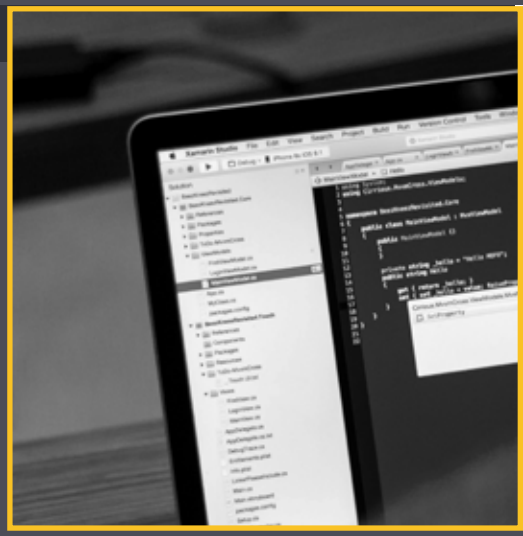
- Data Deletion
- Export Functionality

07 Deletion

Data deletion is a necessary part of database management and we have **permanent deletion functionality** for all data points in Leader. Retention settings at the backend will hold deleted data for a period of **one month** as a **backup**.
Your data retention policy is a key document in your GDPR compliance so the **protocols** you have identified there can **easily be built** into team training on the system.

08 Permission levels

Permission levels are assigned to **all new team members** and can **be changed at any time** by a senior member of the team. Permission levels **control access to database** and the **functionality of the product**. Controlling the number of people with full access to your database is a **key ability in managing your data protection**.



09 Data Minimization

With **GDPR**, you need to ensure the **personal data** that you capture is **adequate**, **relevant** and **limited**. You need to ensure that **you are only storing the minimum amount of data required for your purpose**, this is Data Minimization.
We recommend that you **review all your Custom Fields**, and remove any fields that do not meet this requirement.

10 Storage Limitations

All of your campaign data is **securely stored** in an **encrypted cloud-based database** for the duration of your contract.
You can **remove any information** which you no longer require including **people**, **houses** and **imported files** by deleting these from the dashboard.
This will be **removed instantly** from the dashboard and app, and permanently **removed from the database within 30 days**.

Obtaining Consent

1. Centralised and **secure database**
2. **Data encryption** and **EU** based **servers**
3. **E-signature** capability
4. **Activity logs** and **timestamps**
5. **Permission levels** for team members
6. **Data deletion** and **data retention** settings
7. Unsubscribe and "**no contact**" functionality
8. **Subject access request** data-extraction
9. **Data breach** reporting functionality
10. Consent to contact settings
11. Ability to collect **anonymised data**
12. **Privacy dashboard** to identify **legal basis** for each data point collected
13. Ability to **minimize data quickly**