Join Together Data Protection Compliance Factsheet

Purpose

Join Together (JT) has produced this factsheet to provide trade unions which are considering using JT to manage members' registration with information concerning data protection legislation, how it applies to the services provided by JT, which processing activities are involved, and how they are carried out by JT.

This document is merely intended to easily make available for trade unions information related to JT's compliance standing and efforts, and it does not constitute legal or compliance advice in any way.

What is data protection law and why is it important?

Data Protection law is a set of regulations – in the UK it mainly includes the UK GDPR (General Data Protection Regulation, set out in the Data Protection Act 2018) and the PECR (Privacy and Electronic Communications Regulations 2003) – which relate to the processing of personal data[1]. The aim is to ensure that the processing of personal data is carried out respecting the rights and interests of the persons to whom the data relates to (the data subjects).

Data Protection compliance requires that entities processing personal data (data controllers and data processors) should adhere to certain principles and be accountable to supervisory authorities and, most importantly, to data subjects, so that individuals are aware of the "Who, What, When, Where, Why, and How" of such processing, and can exercise or assert control over it.

What does this mean in practice?

It means that, when processing personal data, organisations are required to have appropriate processes and policies in place to comply with the applicable data protection laws.

At JT, we offer a SaaS product to simplify trade unions' members registration. We provide this service, as a data processor. This means that we will process personal data on your behalf. We are required by law to enter into an agreement with you, which regulates how we will process personal data on your behalf. Trade unions are responsible for fulfilling their own obligations as a data controller. These include ensuring, for example that:

- you have a suitable legal basis to process the data managed through JT's platform;
- where you process any special category personal data or sensitive data (such as relating to race, political views, religion, disability and trade union membership) that you comply with the specific requirements in the applicable data protection laws in this regard;
- you comply with any laws relating to marketing in the event that you intend to send electronic marketing communications to any individuals who express interest in registering;
- any consent request, including its wording, complies with UK GDPR and EPCR requirements;
- JT's data processing is reflected in your privacy policy and the privacy policy is provided to data subjects before their information is collected;
- you comply with all applicable data protection laws.

In case you have any doubt as to your obligations as a data controller, you should seek advice from experts in data protection law.

What kind of personal data does the JT platform collect, and how do we process it?

We will collect and send to you information such as, for example, the names and contact details, employment information, diversity information, payment data of prospective members, and any other personal data you might need to register them as a member.

JT has implemented best practices to ensure a high level of protection for personal data and integrated data protection into its processes and products by default. This means that we try to collect as little data as possible and we use it

only for the strictly necessary needs related to service delivery. For example, we only use essential cookies to operate securely during the application process and we do not use cookies for analytics. We also offer to unions privacy-preserving features as a default in our services (see below).

Should you wish to change any such defaults, that is of course possible, providing that we do not believe the desired feature or setting violates a data protection provision (this is something we will discuss with you).

Concerning our data protection obligations, we have implemented the following:

- **Records of processing activities:** JT established and regularly keeps up to date two records of processing activities: one related to the processing carried out as a data processor for trade unions, and the other to document our own data processing, which includes also the processing of personal data of your employees, carried out to provide our services to you;
- **Privacy notice:** as data controller, we have published on our website a detailed notice about how we process the personal data of website users, as well as prospective and existing customers: https://jointogether.online/privacy-policy. As data processor, we can provide you with as much information as you might need to comply with your own transparency obligations but it is ultimately your responsibility to ensure that you are being transparent with data subjects about how their information is processed (including your use of the JT platform). This is because you are a data controller.
- **Data protection policies:** we have implemented the following data protection policies: Record of Processing Inventory, Privacy Policy, Data Processing Agreements and this Factsheet.
- **Data protection by design and by default**
    - As we collect prospective members' applications to join unions, we ensure that personal data is correctly formatted.
    - Data is either transmitted onwards automatically to the your membership systems via secure and encrypted APIs, or stored on our servers where your team can securely download it to processes the applications.

- By default we redact all user-submitted personal data in incomplete or unsubmitted applications after 14 days. All user-submitted personal data in submitted applications is redacted 60 days after you have retrieved them for processing. If you feel that these retention periods do not suit you, you can choose to change them at any time.
- Your team will be able to access personal data via a secure login. Each person that needs access will be able to assigned a user profile and you will be able to revoke access when it is no longer required. All access to personal data will be logged for security purposes. We can optionally restrict this access to specific IP addresses if required and two-factor authentication is on our near-term roadmap.
- All data is encrypted at rest in our databases with AES-256 block-level storage encryption and encrypted during transmission with 256bit SSL encryption.
- The personal data you process through our platform will be stored in the EU instances of Heroku, our hosting provider, which are located in Dublin, Ireland.

- **Payment data:** we collect bank information only for the purposes of setting up Direct Debits on your behalf, as the trade union.
- **Data subject rights:** if you require our assistance in relation to any data subject rights requests you have received, you can contact us at privacy@jointogether.online.