

Liberal Democrat Data Protection Rules – Plain English Version

© The Liberal Democrats  
September 2018

### Contents

1. Background
2. Data Security
3. Data Collection
4. Data Use
5. Data Subjects Rights

### 1 Background

The Federal Party is legally in charge of all personal data collected, stored and used by all areas of the party. This includes Specified Associated Organisations (SAO) and Associated Organisations (AO).

You may have been elected to public office. For example, Councillors, Parliamentarians, Assembly Members, Police Commissioners and Mayors. You must keep personal data collected as an elected official separate from any data collected for the Party. You are responsible for any data you collect for your work as an elected officials.

You must only use personal data collected by the Party. If you get data from a source outside of the party, we must have a legal right to use it. Or if the source outside of the party can show they have received consent to give us the personal data.

The Party will appoint a Data Protection Officer (DPO). You must use specific wording whenever you collect personal data. This is called a Fair Processing Notice. The DPO will keep a list of these Fair Processing Notices (FPNs) for use in different situations. The DPO will also keep an up to date list of approved suppliers and a list of approved software.

### 2 Data Security

Personal data must only be stored on computers or other devices owned by the party. Otherwise that computer, device or the data must be encrypted.

You must send passwords for encrypted data using a different method than the data itself. For example, if you send the data by email, then send the password text message or phone call, but not by another email.

Personal Data must not be used on devices that belong to non-party members. Once exception to this is where the person, service or company is on the list of approved suppliers. Staff members may use their own device or computer where permitted.

Personal Data must not be used for longer than the time stated in the privacy policy. The Privacy Policy is at <https://www.libdems.org.uk/privacy>.

You should only use software and systems that are on either the approved software or supplier lists.

Encrypt any computers and servers owned by party organisations that store personal data.

If any data gets deleted or destroyed by accident, you must report it to the DPO within 24 hours, in writing. You can email [data.protection@libdems.org.uk](mailto:data.protection@libdems.org.uk) or phone HQ on 020 7022 0988.

Make sure that you use, store and throw away any printouts and paper forms with personal data securely.

If any of these rules are broken, you must report the breach in writing to the Party's Data Protection Officer, within 24 hours.

### 3 Data Collection

Personal data must be collected in line with the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (UKDPA).

When collecting data from a form, then make sure you show a readable, current Fair Processing Notice near to the form.

If you collect Personal Data on a telephone call, then the person giving their data must be asked to consent to us using it. You must also inform them of how their data will be used and how long the party will keep it.

If you collect personal data face to face, then you must hand over a leaflet with the current Fair Processing Notice. The person must also be asked to consent to us using their data.

If the personal data comes from a third party, i.e., not the person themselves, then you must not record the data or use it. You can record and use third party data if there is consent from that person or there is another legal reason for doing so.

You must record any consent for collecting personal data in one of the databases in the approved software list. This record will include who, when and what they consented to. It will also include which Fair Processing Notice they were given at the time.

A member of staff who breaks any of these rules will be subject to the relevant Staff disciplinary procedure.

A member of the party who breaks any of these rules will be subject to the relevant party disciplinary procedure.

### 4 Data Use

Personal Data must not be used unless there is a lawful reason to do so. For example, the individual has given consent for us to use the data. We can also use personal data for running the Party, if the individual is a member of the Party, an SAO or an AO.

You can also use the data if it is necessary for complying with another law, or it is allowed by another law.

If an individual gives consent, then it has to be received to the standards set in the Data Protection Act. More information on this is available at <https://libdems.org.uk/gdpr>.

Members of the public may be contacted with leaflets or mail without a name or address. You can also send them addressed mail if they are on the electoral register, unless they have opted out of receiving mail. You can also send addressed mail where they have given consent.

You can contact members of the party by mail, email, telephone, text message, social media and apps, unless they have requested not to be contacted. You can also contact members of SAOs or AOs by those methods, unless they have requested not to be contacted.

Non-members who have consented can be contacted by electronic means. They must have consented to the specific method of contact whether that is Email, Telephone, Text message, Social Media or using apps.

You must record any consent for collecting personal data in one of the databases in the approved software list. This record will include who, when and what they consented to. It will also include which Fair Processing Notice they were given at the time.

If an individual withdraws consent, then that must be recorded in the database in the approved software list.

Consent is only valid if it was freely given. Consent must not be linked to any other matter. The individual must be given information how their data will be used. This is the Fair Processing Notice. This must be easily readable and easily accessible. This must also be in clear and plain language.

Personal data may only be given to suppliers that are on the list of approved suppliers.

Above all, personal data must not be used if the individual has instructed us that they do not want to have their data used.

### 5 **Data Subjects Rights**

Individuals have privacy rights under GDPR and UKPDA. For example, the right to be forgotten, the right to restrict the use of their data, and the right to correct the data we hold on them. Also they have the right to ask for a copy of all the data we hold on them (a Subject Access Request).

You must forward any request from an individual using their Privacy Rights to the DPO within 24 hours. Email [data.protection@libdems.org.uk](mailto:data.protection@libdems.org.uk) or phone HQ on 020 7022 0988. Only the DPO can legally respond to these requests.