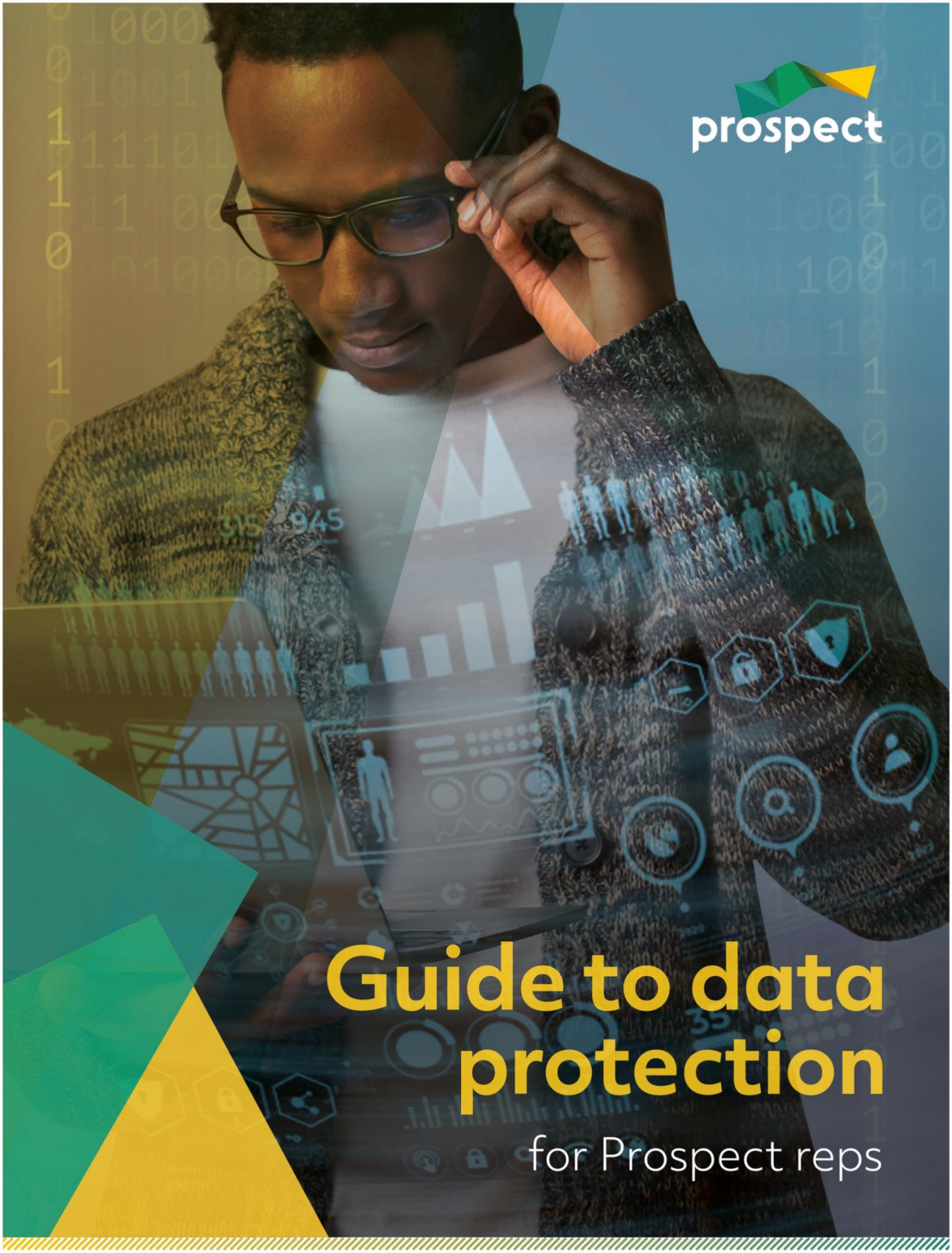


prospect

Guide to data protection

for Prospect reps

prospect.org.uk

Guide to data protection for Prospect reps

Contents

Introduction

Prospect has a responsibility to keep its membership information secure and to use it in a way that members would expect and think fair. All members must be able to trust that when they provide us with their personal information it will be kept safe.

It is also a legal requirement, as trade union membership is classed as ‘special category’ by the legislation and requires a higher level of protection.

This guide is designed to help you as a union representative to comply with data protection legislation and help to make the handing of personal data as easy and secure as possible.

Background

The legislation that protects personal data:

The Data Protection Act 2018 (DPA)

This Act sets out the data protection framework in the UK and sits alongside and supplements the UK GDPR. It also covers areas not in the UK GDPR including data relating to crime and the security services.

The UK General Data Protection Regulations 2021 (UK GDPR)

This sets out the key principles, rights, and obligations for the processing of personal data in the UK (previously known as the GDPR 2018)

Protection of Electronic Communications Act 2003 (PECR)

This legislation gives specific privacy rights in relation to electronic communications. The relevant areas are:

- Marketing by electronic means including email, text, and fax
- The use of cookies on websites

UK General Data Protection Regulations

What does the UK GDPR apply to?

- Any organisation/individual who collects personal information about individuals for any business or other non-household purpose.
- Any personal data you use in connection with union work; either stored electronically on computers, smart phones or in paper files.

What does UK GDPR not apply to?

- Only applies to living individuals.
- Does not cover information, which is not, or is not intended to be, part of a 'filing system'. Therefore, information kept in notebooks will not be covered.
- The legislation does not apply to personal data that has been anonymised.

Remember: data collected by employers about staff are also subject to these regulations.

Trade union data

Under data protection law trade union data is defined as 'special category' (Article 9 UK GDPR). This category of data means it is highly sensitive and extra rules apply to use this type of data.

Prospect is the data controller for all union data which includes all personal data processed by union reps.

Remember: Disclosing information about an individual that reveals their trade union membership or non-membership is a breach of the regulations if you do not have permission to do so.

The seven principles of data protection (Article 5)

The seven principles of the UK GDPR set out how personal data should be processed:

- **Lawfulness, fairness and transparency** – Personal data shall be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation** – Personal data shall be collected for a specific, explicit, and legitimate purpose and not further processed in a manner that is incompatible with that purpose.
- **Data minimisation** – Personal data shall be adequate, relevant, and not excessive for the purpose of the processing.
- **Accuracy** – Personal data shall be accurate and, where necessary, kept up to date.
- **Storage limitation** – Personal data shall not be kept for longer than is necessary for the purposes of the processing.
- **Integrity and confidentiality** – Personal data shall be processed in a manner that ensures appropriate security of the personal data.

Accountability is the seventh principle, which relates to the requirement for data controllers to be able to demonstrate they are complying with the legislation.

1. Personal data must be processed fairly and lawfully and in a transparent manner.

In order to process personal data, there must be a lawful basis to do so. There are six lawful conditions (as set out in Article 6), and at least one must be identified for Prospect to comply with the above principle. These are:

1. Consent
2. Performance of a contract
3. Legal obligation
4. Vital interest
5. Public interest
6. Legitimate interest

However, for special category data, which includes the following, there must be an additional lawful basis:

- Trade union membership
- Race and ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Genetic data
- Biometric data (this includes photographs, fingerprints, audio recordings)
- Health (including disability)
- Sex life or sexual orientation
- Criminal convictions and offences

Processing of this data is prohibited unless one of the following applies (Article 9):

- Explicit consent
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or individual in the field of employment, social security, and social protection law
- Processing is necessary to protect the vital interests of the individual
- Processing is carried out during its legitimate activities, with appropriate safeguards for trade union aims, and relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and the personal data is not disclosed outside the body without the consent of the data subjects
- Processing relates to personal data manifestly made public by the individual
- Processing is necessary for the establishment, exercise or defence of legal claims
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for arching purposes in the public interest, scientific or historical research purposes or statistical purposes

To ensure transparency, Prospect must communicate to its members how it will process their personal data. This is done by:

- Publishing a privacy notice that explains how we process personal data. This is located on the Prospect and Bectu websites, and all members should be aware of this. https://prospect.org.uk/privacy/
- When personal data is collected, be clear to members and non-members how their data will be used.

Please refer to the Prospect privacy notice to see the lawful basis for our processing.

The lawful basis for the majority of our trade union work will be contract (6.1.b), as we offer services to members as part of their membership and in the course of our Legitimate trade union activities (9.2.d). However, we may use others depending on the specifics of the processing.

Under the Data Protection Act, special category data on race, religion or health can be used for equalities purposes.

2. Purpose limitation

Personal data should only be collected for the purpose it is designed for. This means you shouldn't use personal data for something the individual wouldn't have expected when it was provided.

The categories we collect data for and are legally allowed to use are:

- To meet our obligations as set out in the union rule book
- To deliver and manage services to members
- To recruit members
- To provide advice and assistance to members

- To conduct elections and ballots
- To provide training opportunities for members and non-members
- To communicate with members including providing information about campaigns, benefits, and services
- To manage our website, and social media platforms
- To manage staff who deliver those services
- To manage our statutory obligations
- To manage the finances of the union
- To promote and deliver equality and diversity
- To investigate complaints
- To prevent and detect crime and fraud
- To aid in case of a medical emergency

3. Data minimisation

Only collect the data you need. Don't collect more data than is necessary to achieve your purpose.

4. Accuracy

This principle requires Prospect to ensure it keeps data accurate and has processes in place to keep data up to date. This would include:

- Encouraging members to up-date their details via the Prospect website
- Checking members details when they contact us directly
- Checking members details during industrial ballots and elections

Representatives are encouraged to use the E-branch system on the website, as this is the best way to ensure data is accurate.

5. Storage limitation

Personal data should not be kept for longer than is necessary for the purposes of the data processing.

To meet this requirement Prospect has a data retention schedule for the data it holds. Organisations can set their own time limits to meet their own requirements. However, there are some legal retention periods that need to be met. (See Appendix 3)

6. Integrity and confidentiality

This principle is to ensure that appropriate security is put in place to keep personal data safe, and secure against accidental loss, damage, or destruction. Examples include:

- Password protection
- Virus protection
- Secure storage
- Clear desk policy

Individual rights

All members and non-members whose personal data we process have the following rights under the regulations.

Right to be informed

Individuals have the right to be provided with information about how their personal data is being processed. This is usually done in the form of a privacy notice either provided in writing or by other means including publishing on websites.

Right of access

Individuals have the right to obtain confirmation that their personal data is being processed and to be provided with a copy of that data.

If you receive a request, it should be forwarded to Prospect to the Data Protection Compliance Officer on datacompliance@prospect.org.uk. We have a month to respond from the date the request is received, so it's important a request is forwarded as soon as possible.

Right to rectification

Individuals have the right to correct information held about them if they believe it is factually incorrect. They also have the right to have incomplete personal data completed by means of providing a supplementary statement.

Right to erasure

This is also known as 'the right to be forgotten'. In certain circumstances it allows individuals to ask for their personal data to be deleted or removed.

If you receive an erasure request, it should be forwarded to Prospect to the Data Protection Compliance Officer on datacompliance@prospect.org.uk. We have a month to respond from the date the request is received, again it's important a request is forwarded as soon as possible.

Right to restrict processing

In certain circumstances individuals have the right to stop us processing their personal data. The data can be stored but cannot be used until a dispute is resolved.

Right of data portability

This is a new right that allows individuals to access and move their personal data for their own benefit across different services. This only applies to data provided electronically by automated means.

Right to object

Individuals have the right to object the processing of their personal data, on grounds relating to their particular situation. Therefore, we must stop the processing unless we have a legitimate reason to continue to use the data.

Right to opt out of direct marketing

Members have the right to opt out of receiving direct marketing. See the section of Privacy of Electronic Communications Regulations.

Exemptions

The DPA 2018 sets out exemptions to these rights in certain circumstances. For example, if you collect data for journalistic, academic, artistic, and literary purposes you will be exempt from most provisions of UK GDPR including subject access requests, and from providing a privacy notice when collecting data.

Right to complain to the Information Commissioner Office (ICO)

The ICO is the regulator for data protection and an individual has the right to complain if they believe their personal data has not been processed in accordance with data protection regulations.

If Prospect is found to be in breach of the regulations the ICO can take action against us, including issuing fines up to 4% of our annual turnover and for breaches of PECR £500,000.

Data breaches

A data breach is the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples of breaches:

- Lost paperwork
- Mobile devices lost or stolen containing union data
- Spreadsheets of members data not password protected sent by email
- Emails to branch members not blind copied
- Personal data sent to the wrong person by email or post
- Documents not disposed of properly
- Cyber-attacks

The first thing to remember is don't panic, mistakes happen. As soon as you realise a breach has happened, try to rectify the situation, if possible. For example:

- Wipe data from mobile devices if lost or stolen
- Request deletion of emails if sent to the wrong person

Report a breach of union data to the Data Protection Compliance Officer (DPCO) at Prospect as soon as possible on datacompliance@prospect.org.uk.

When reporting the breach, please include the following information:

- The nature of the actual or suspected breach
- The type of data involved, including a copy of the information, if possible
- How the breach happened
- How many individuals involved
- When it happened
- When you became aware of it
- Action taken to rectify the situation

Serious high-risk incidents must be reported to the ICO, and Prospect has only 72 hours to assess the breach and report, so early reporting is essential. (See Appendix 2).

Once reported, you may be asked to complete an incident report form.

The DPCO, will investigate the incident. Depending on what has happened, if there is a serious risk to individuals then it will be reported to the ICO.

Other incidents will be investigated and logged.

The DPCO will inform the official for the branch of the incident.

Once the investigation is complete the DPCO will report back on the results of the investigation, and any action that needs to be taken to ensure it cannot happen again.

Subject access requests

Individuals have the right to make a request to any organisation for confirmation that their personal data is being used, and where this is the case, access to the personal data, and a privacy statement about the data being used.

It is important for reps to remember that when keeping processing personal data and communicating about individuals that you shouldn't write anything you wouldn't want that individual to see.

A request can be made in writing or verbally and even via social media. An individual does not have to use specific words or refer to the legislation or direct the request to a specific individual for it to be a legitimate request.

Any request to access personal data should be referred to the DPCO on datacompliance@prospect.org.uk

When information is kept on workplace or private computer systems the DPCO will contact the relevant individuals to ask for copies of the information.

Reps may also be asked to supply information when the employer receive a request. However, if the request would involve trade union data, then this request should be forwarded to Prospect's DPCO, and the employer should be informed that as Prospect is the data controller for union data, we will deal with this aspect of the request.

Data Protection Impact Assessments (DPIA)

The UK GDPR requires organisations who plan to use new technologies, special category data or data on a large scale to undertake a risk assessment known as a DPIA. As part of this process the organisation should consult all interested parties before the introduction of the new technology or before any change to the use of staff data.

Examples of new technology include:

- Tracking software – GPS and digital tracking
- Fingerprint access systems
- Surveillance software – on phones/laptops
- Keystroke monitoring – on what you are typing, and speed
- Shift allocation systems – scheduling your work shifts
- Feedback systems – incorporating client or customer “ratings” into employee records
- Task management systems - app based software to allocate tasks, set times and monitor how you are working
- Performance management – rating workers, on promotions, bonuses
- Facial/emotional recognition – cameras used to check on workers
- Recruitment software

If new technology is going to be introduced or staff data is going to be used in a new way ie fingerprint entry systems, staff monitoring. Ensure you are included in discussions or ask for a copy of the DPIA.

Some key questions that can and should be raised with employers include:

- How is the data going to be used?
- Why is the personal data being collected?
- What are the sources of these data?
- How have you identified risks arising from the use of individual personal data and the rights/ freedoms of the collective group of employees?
- What are these risks and how can they be reduced?
- If you have decided not to consult with union reps, can you disclose the reasons why?
- What will be the review process?
- How will data breaches be shared with the union?
- If employer has decided not to undertake a DPIA, what are their reasons why?

Other issues that should be considered include:

- Processors - Is the data being collected and processed by another organisation on behalf of the employer? The employer should then have a processing agreement with that company, and staff need to be informed about their identity in the privacy notice.
- International data transfers - Is the data being transferred overseas, eg via cloud storage? A transfer of personal data to a third country or international organisation shall only take place subject to specific provisions set out in the regulations, including agreements and risk assessments.

Branch activities and data protection

The employer as processor

An employer is the data controller for employee personal data. However, when union reps are using employers' computer systems to process documents or communicate with members and non-members, this makes the employer a processor because the union is using their computer systems.

Therefore, it is good practice to have an agreement in place with the employer, which would cover the responsibilities of each data controller, including data sharing, data breaches and subject access requests. This type of agreement could also be part of any facilities agreement or the recognition agreement.

Check agreements to see what arrangements are already in place for

- data sharing – information on new staff members
- using internal computer systems for union work
- Using email to contact staff

Transparency

All branch reps should be transparent about their activities when using membership data, especially when organising and contacting non-members.

- Wherever possible highlight Prospect's data privacy notice and include a link in any communication when you contact individuals on union business.
- Always inform members and non-members whenever possible about the information you are collecting or using and why you are doing so.

Recruitment and organising

Data processing in branch

The role of branch representatives involves the following:

- Organising the branch
- Recruiting members
- Representing members
- Negotiating with management
- Consulting with members

All these activities involve the use of personal data of both members and non-members, including:

- Handling membership forms
- Mapping the membership
- Organising and running meetings
- Amending or deleting membership details
- Running membership reports
- Communicating with members
- Dealing with personal cases

When completing these activities:

- Do ensure spreadsheets and lists of members and non-members are password protected.
- Do lock your computer screen when away from your desk
- Do ensure files are kept in lockable cupboards.
- Don’t leave paper copies of membership details on your desk.
- Do encourage members to up-date their records as soon as possible.
- Do shred membership information when it is no longer required.
- Do use the E-branch system on the Prospect website.

Collecting potential member information

Purpose

When collect persona data reps should be clear with colleagues about exactly why you need the data. The data collected should only be enough to undertake the organising work you need to do.

Reps should be able to explain why they are processing the data, if you can't then don't use it.

Data needs to be relevant to your organising activities. If you have data that you want to use for a purpose not connected to organising, then you would need the consent of the individual.

For example, if a non-member provides information about a personal situation at work which you want to pass onto an official you would need their consent to do this, and this consent should be confirmed by email.

New starters

Employers often use data protection legislation to refuse to share information on new starters or insist on using employees consent before sharing the data. Try to work with the employer to ensure data about staff is shared with the union.

- In recognised workplaces have a data sharing agreement in place or include data sharing in the recognition, facilities agreement.
- Employers ask new employees to consent to share their data with the union. If consent is not given this can make it difficult to identify new members.
- By using the lawful basis of legitimate interest employees can be given the option to opt-out, this makes it easier for details to be passed to trade union reps in compliance with data protection regulations.
- Alternatively, ensure union reps are part of the induction process, get union information into induction materials for new staff, or on the staff intranet.
  (The Employment Practices Code, ICO, covers the sharing of data between employer and a trade union).

Publicly available material

Personal data about non-members that is publicly available can be processed, eg information located on a workplace website or intranet. However, you will need to provide individuals with access to a privacy notice when you first make contact.

Workplace contact details can be used to make contact, if individuals are made aware that this is taking place, and they can opt out of further communications.

- Don't collect excessive amounts of information keep it to a minimum that is needed.
- Do keep the information secure, ideally password protected.
- Don't share with anyone who does not need to see it.
- Do establish a retention period for this information, and once this time period has elapsed dispose of the information.
- Keep a 'Don't Contact' list so you don't contact colleagues who have opted out.
- Do dispose of information securely ie delete from a computer or shred paper documents.

Mapping the workplace

Mapping is the process of obtaining accurate and relevant information about the workplace, and can be used for recruitment, communication, develop activists and campaigning. However, this process involves using personal data and is therefore subject to data protection regulations.

Our legal right to collect this data, is legitimate interest and processing is carried out during our legitimate trade union activity.

The process of mapping and creating tables of information will include the collection of personal data, for example:

- Identifying workplace colleagues: name
- Workplace structure – departments/buildings
- Working patterns – full or part-time/contract, rotas
- Membership – identifying union membership, attitude to union membership
- Identifying teams – names
- Issues – concerns and workplace complaints
- Identifying where staff socialise/eat - habits, routine, vegetarian/vegan

The best way to proceed in mapping non-members:

- Have a clear purpose which the mapping exercise is linked to ie recruiting more members by holding an event, or talking to them individually, surveying non-members on a workplace issue, involvement in a specific workplace campaign.
- Purpose should involve contacting non-members that have been mapped. This should be done as soon as possible, or at least within one month of collecting the data.
- When you contact a member, provide them with access to Prospect's privacy notice, and seek permission to contact them further.
- If you don't get consent, then the data should be removed to a do not contact list.
- Anonymise data if you don't plan to contact members. If individuals are not identifiable then it is not personal data, eg:
    - how many workers in a department
    - how many workers are on a permanent or fixed term contract.

Data sharing

Reps may wish to share mapping data relating to members and non-members with other members and officials.

- Don't let other members see data if there is no reason to do so, eg if the data relates to one department only share with members in that department, unless members will be involved with recruitment in other departments.
- Ensure that all mapping information is kept secure.

Data security

- Do tell staff that you are collecting data about them.
- Do be careful on what you write, as individuals have the right to see their personal data, and opinions about an individual can be personal data.
- Don't say anything you wouldn't want anyone to see.
- Anonymise the data by removing the names, eg only identify individuals by their role.
- Pseudonymise data if you still need to identify individuals by keeping a separate list of names.
- Do keep lists containing member and non-member personal data password protected.
- Don't keep lists for longer than needed.
- Do securely destroy documents when no longer needed.

Data cleansing

- It is important that any personal data is accurate, as this is one of the principles of the legislation.
- Do encourage members to contact membership if they need to up-date their details.
- Do encourage members to log into the Prospect website to manage their records.
- If you become aware of changes to a member's details from a third party, check with them first before asking membership to up-date their record.
- Don't keep old copies of membership records, as the personal data may have been on the main database.

When seeking to update information:

- Don't circulate a spreadsheet with information and ask for corrections, send individual up-date sheets or a questionnaire to individual members.
- Don't send out blanket email to members without using the 'blind carbon copy' (Bcc) field

Secure data storage

All personal data must be kept safe and secure.

Paper data

- When dealing with paper eg, file notes, correspondence, reports, consider putting the following in place:
- Lockable filing cabinets
- Lockable door of branch office
- A clear desk policy
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin.

Electronic data

This covers computers, laptops, cloud computing, removable media (USB, CDs etc).

If using employer systems, much of the items listed below will be covered. If you are using your own equipment, especially portable equipment, then you need to ensure it is adequately protected.

- Back up your data and ensure it is kept separate from your computer.
- Store data on a network rather than a laptop or desktop computer.
- Keep data on an external hard drive – password protected.
- Cloud storage - ensure data is encrypted.
- Protect your computer from virus/malware attacks by installing and turning on antivirus software, and ensure it is kept up to date.
- Avoid downloading apps unless from manufacturer approved sites.
- Keep all your IT equipment up to date.
- Turn on or install adequate firewalls.
- Ensure mobile equipment can be locked, password protected and remotely wiped if lost.
- If equipment containing union data is lost or stolen it should be reported to Prospect as soon as possible on datacompliance@prospect.org.uk.
- Don’t connect to unknown wi-fi hotspots.
- Once a computer is no longer required ensure all data is removed and is not recoverable.

Mobile technology - smartphones and tablets, need the same amount of protection

Password Protect equipment and individual documents, as necessary. It is recommended that you use strong passwords:

- Use a minimum of eight digits.
- Avoid using commonly used words, for example, birthdays, family names etc.

- Use special characters – % $ &.
- Use letter and upper-case characters and numbers.

Membership data

Membership data should not be shared with any other organisation. If you receive a request from an outside organisation this must be referred to a union official.

However, there will be occasions when you will need to share data because we are either legally required to do so or when there is a legitimate interest to do so. This may involve using on-line tools, like Snap surveys.

- Balloting for industrial action
- Redundancy procedures
- TUPE transfers
- Grievance/Disciplinary procedures
- Personal case details shared with legal advisors
- Membership surveys
- Mapping the workplace

Membership information

- Do send documents securely.
- Do keep data secure including password protecting membership lists.
- Do only supply membership data to individuals who need to see it.
- Don't use for a purpose it was not intend for.
- Don't keep duplicate copies of information.
- Do securely destroy copies once no longer needed.
- Create a secure, password protected folder for union work, if using the employer's network, to ensure the employer cannot access the data.

Sharing data in an emergency

There may be an emergency where you may need to share members personal data, for example contact details to:

- prevent serious physical harm to a person
- prevent loss of human life

If possible, refer the request to Prospect Head Office.

If this is not possible, ask yourself:

- Is it unfair to the individual to disclose their information?
- Would they expect their data to be shared in an emergency?
- Are you acting for their benefit?

- Do I know who is asking for this information ie emergency services, employer, relative?

The specifics of any situation will obviously define your answer and how you respond.

Releasing information to prevent or detect crime

Any request from the police or law enforcement agencies should be referred to the Data Protection Compliance Officer on **datacompliance@prospect.org.uk.**

Communicating with members

Email addresses are personal data and communicating with members and non-members will be regulated by both PECR and UK GDPR.

Remember when using your work email accounts, computer network for union business, the employer will be the controller and therefore will be able to access these systems.

Secure use of email

- Ensure no one else can access your email.
- When sending an email to a member on a personal case always put private & confidential in the subject line.
- If emailing more than one person always use the BCC field if the recipients do not need to see who has been copied into the email, especially when corresponding with branch members.
- When forwarding emails, take care that it contains no information that should not be shared, especially if it is a long email chain. Ideally, start a new message.
- Always password protect spreadsheets, or any document containing members details and send the password separately.
- Only use a member's preferred email address, using a workplace address when they have expressed a preference for the personal address, would be a breach of the regulations.
- Please use Prospects secure free E-branch system, available via Prospect website. https://members.prospect.org.uk/resources/ebranches
- Ensure you are sending to the right person especially when using auto insert for email addresses. Ideally turn off auto-insert.
- When organising a meeting Outlook does not allow you to blind copy addresses when organising a meeting through the calendar. Email addresses should be put in the optional section.

Workplace communications

- Union recognition agreements – can set out what access reps have to internal computer/email systems to contact staff.
- The language of messages should be considered carefully when making contact ie keep it about workplace issues (see the section on PECR).
- Get individuals consent to contact them further.
- If you collect data to create a mailing list, then this will be subject to UK GDPR and the union will then become the data controller.
- If non-member opts out of receiving emails. Keep record of this so you don't contact them again.
- When appropriate use Prospect's E-branch to contact branch members as this ensures you are using the correct details and is secure.
- If you are using different communication software ie Slack, to communicate all these points still apply.

Workplace issues

Under Trade Union and Labour Relations (Consolidation) Act 1992 unions have the right to negotiate on the following areas. Therefore, these are issues that can be legitimately communicated to members and to non-members.

- Terms and conditions
- Physical conditions
- Engagement, non-engagement, termination, suspension of employment, duties of employment, allocation of workplace duties
- Discipline
- Employees membership or non-membership of a trade union
- Facilities for a trade union
- Machinery for negotiation
- Recognition

Representing members

Information related to a potential or actual case will be extremely sensitive and branch reps need to ensure:

- Files are stored securely.
- Access to files should only be given to those who need to see the data.
- Collection of data is limited to only what is relevant to the case.
- Information on file is accurate.
- Obtain written consent from the member in order to start representing them.
- Always inform the member on the progress of the case.
- Files should be retained for 7 years, once closed.
- Archive files securely when no longer required.
- Remember opinions can be personal data.
- Individuals have the right of access to see information held about them.
- The union has a duty of confidentiality to its members when handling personal cases.

Privacy and Electronic Communications Regulations 2003 (PECR)

PECR applies if the union is sending unsolicited direct marketing messages by electronic means. This includes emails, texts, picture messages, video messages, voicemails, or any type of electronic message.

- Direct marketing is the communication (by whatever means) of advertising or marketing material which is directed to a particular individual.
- This includes the promotion of an organisations aims, values and policies. This would cover the recruitment of members and any campaigning activities by the union.
- Under PECR, organisations must not send marketing texts or emails to individuals without their specific consent.
- Marketing not directed at individuals, for example: leaflets, magazine inserts, advertising are not covered by PECR.
- PECR requires that individuals have given prior consent to be contacted electronically. This must be a positive action ie ticking a box, responding to an email. Failure to respond to an email or not ticking a box does not count as consent.
- All individuals have the right to opt-out of direct marketing at any time.
- Corporate email addresses using the company name and @ org, co, com or gov are not covered by PECR, but are still subject to UK GDPR rules.
- Individuals using corporate emails have the right to opt-out from receiving marketing material. But you don’t need prior consent to contact them.
- Keep records of consent to receive emails and keep lists of those who have opted-out, so they are not used in any further communications. Important to remember these lists are covered by UK GDPR rules, so should be kept secure.

Contacting non-members

When sending emails to non-members in the workplace, for the first time, it should include the following:

- Clearly identify the sender – Prospect's contact details
- Clear information about how their data will be used for example to send further emails
- A clear statement informing them that if they reply to the email this will be taken as consent to receive further communications. **For example:**

  If you are interested in receiving more information about the work of Prospect, and want to be kept informed about workplace issues, please reply to this email with the following: I consent to receiving further information from Prospect and understand this consent can be withdrawn at any time.
- A link to the Prospect privacy notice
- Clear information about how to opt out of further communications

Social media

As reps you may also be using different types of on-line communications systems to keep in contact with members and non-members. This could include Facebook, WhatsApp, Signal, Twitter, Instagram.

There is an exemption in the Data Protection Act for the use of personal data for domestic purposes. However, this does not cover an individual or organisation's use of social media and all the requirements of data protection legislation will apply.

When a site is clearly being used for the purposes of promoting Prospect or to allow members to communicate with each other regarding union issues, then the legislation will apply.

The legislation will apply:

- When you post personal data on your own site or a third party's site.
- When you download and use personal data from a third party's site.
- When an organisation or individual runs a social media site which allows third parties to add comments or posts about individuals.

Data controller

A data controller is an individual or organisations which determines the purposes and means of processing personal data. In relation to social media contact information or other personal information the site processes about its own users or subscribers will mean that the administrator will be the data controller for the site.

This means Prospect will be the data processor for our website and other on-line sites we clearly administer and set the rules for.

However, if social media sites are set up by reps or members, and they determine their own purpose and set their own terms and conditions. Then the person setting up the site (the administrator) will be the data controller and will therefore be responsible for meeting the requirements of the legislation, including the following.

Accuracy

Ensuring that information on sites is accurate. Only reasonable steps need to be taken you do not have to monitor and check every post. Individuals posting opinions do not need to be checked for accuracy, but they may be subject to other legislation.

Measures which should be in place, include:

- Clear and prominent policies for users about acceptable posts.
- Procedures for individuals to dispute posts and to ask them to be removed.
- Respond to complaints from individuals who believe that their personal data may have been processed unfairly or unlawfully because they have been the subject of derogatory, threatening, or abusive on-line postings by third parties.
- Respond to disputes quickly and have procedures to remove or suspend access to content.

Subject Access Request

An individual can make a subject access request which can include social media, and they have a right to a copy of their data.

Data breaches

The data controller will also be responsible for any breaches of personal data, including:

- Posting information without the consent of the individual.
- Taking screen shots and sending to third parties without permission
- Personal data hacked from sites because of poor security.

If you are running an on-line site on behalf of Prospect, please inform the DPCO so that it can be logged in the processing register

Other legislation that may be relevant in respect of opinions expressed, may have serious legal consequences for Prospect as the data controller and for individuals making the posts.

Protection from Harassment Act 1997

Communications Act 2003 – Section 127

Malicious Communications Act 1988

Common law contempt of court and the Contempt of Court Act 1981

Section 4A of the Public Order Act 1986

Common law of defamation and the Defamation Acts, 1952, 1996 and 2013 (note that section 5 of the 2013 Act deals specifically with website operators).

Further information

If you require further information or advice, please contact the Data Protection Compliance Officer on datacompliance@prospect.org.uk.

Links

Information Commissioner's Officer

https://ico.org.uk/

https://ico.org.uk/for-organisations/data-sharing-information-hub/

National Cyber Security Centre

https://www.ncsc.gov.uk/collection/10-steps/data-security

Documents

Prospect Digital Technology Guide for Reps.

Appendix 1: Data protection terms you need to know

Controller: A Data Controller is the body which determines how and why personal data is processed including how it is stored, kept secure and transferred.

Processors: A 'processor' is an organisation/individual which processes personal data on behalf of a data controller, for example a recruitment agency, payroll company, and on-line companies like Eventbrite.

Processing: The processing of personal data covers anything that you do with personal data, and including the following:

- keeping branch records
- creating lists of members/non-members
- communicating with members
- social media
- administration of personal cases documentation
- transferring personal information
- disposing of information

Personal Data: Information **relating to** a living person (often known as a **data subject**); which enables them to be identified, directly or indirectly.

Some examples of personal data are:

- name (email address)
- an identification number (membership number, national insurance number, passport number)
- location data (home address, postcode, GPS)
- an online identifier - (IP address, cookie identifiers, social media 'handle', device fingerprints)
- or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person – (health, religion, occupation, bank details, photographs)

Meaning of 'relating to'

Information must relate to the individual involved to be personal data. A name by itself is not necessarily personal data. It must do more than simply identify them, it must concern the individual in some way, and you must be able to distinguish them from another individual.

> **Example**:
>
> *John Smith works at company A. If there is only one John Smith, this is enough information to identify him.*
>
> *However, there are three individuals called John Smith who work at the company in different departments. Therefore, to identify the correct individual you need further information, such as: John Smith, Head of Accounts, who works in the Finance department.*

Therefore, any information that can be used to identify someone can make it personal data.

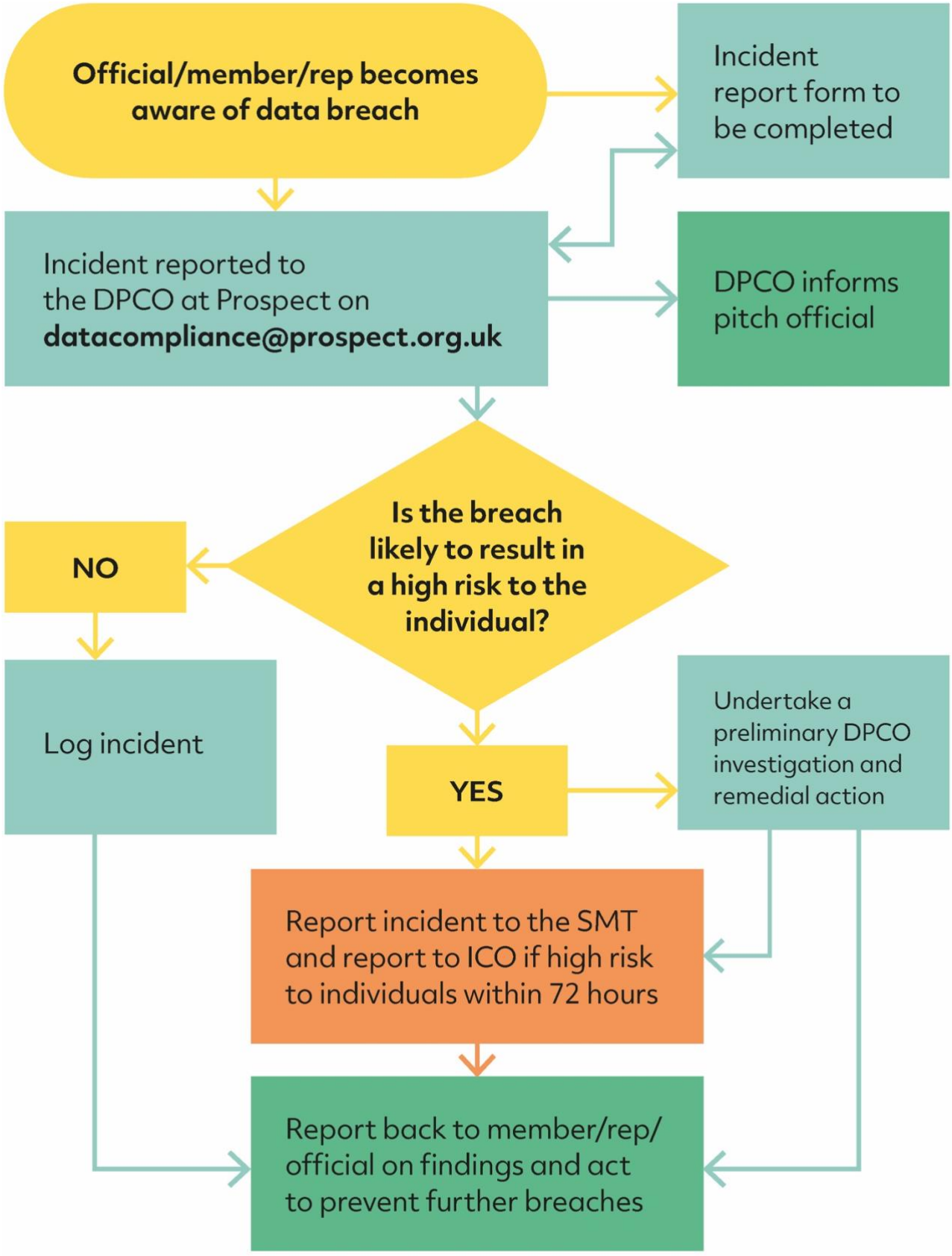
- Opinions about individuals are also classed as personal data.
- Information about a deceased person is not personal data.
- Information about a company or public authority is not personal data.
- Information about individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable, and the information relates to them as individuals then this may be personal data.

Data subject examples

These are examples of data subjects:

- Members
- Non-members
- Former members
- Contractors
- Suppliers
- Employees

Appendix 2: Reporting a data breach



DPCO – Data Protection Compliance Officer; **ICO** – Information Commissioner's Office; **SMT** – Senior Management Team

Appendix 3: Prospect retention schedule

Description	Document types	Retention trigger	Retention period	Reason for retention
Industrial relations	Branch activities Agreements Publicity	Completion	3 years	Trade Union & Labour Relations (consolidation) Act 1992 Limitation Act 1980
Meeting administration	Agendas/Minutes Branch committee Branch meetings AGM meetings	Completion	3 years	Operational requirement
Branch records	Contact information Branch membership lists Diaries Telephone messages	No longer needed	1 year	Occupational requirement
Statutory ballot for industrial action	Membership lists Ballot papers Campaign material Ballot result report Supporting paperwork	Ballot closed	1 year	Legal Trade Union & Labour Relations (consolidation) Act 1992
Non-statutory ballot – consultative ballots	Supporting paperwork Ballot papers	Ballot closed	1 year	Operational requirement
Recognition	Collective agreements	Date of agreement	Permanently	Operational requirement
Personal cases	Correspondence Documents Minutes Reports Legal opinions Instructions Forms	Completion of case	7 years	Limitation Act 1980, GDPR 2018 Civil Evidence Act 1995 Prescription & Limitation (Scotland) 1973

Appendix 4: Processing agreement with employer template

This template agreement can be amended as necessary and can form the basis for negotiation with the employer.

EMPLOYER AGREEMENT BETWEEN PROSPECT & [the company]

Parties to the agreement

1. This agreement is made between Prospect and [the company]. By this agreement [the company] is the Controller of their staff intranet, internet, email system and computer systems, including storage, security, and office productivity tools, and for the purposes of this agreement [the company] is the Processor and Prospect is the Controller of union members' personal data.
2. By this agreement [the company] agrees to process data on behalf of Prospect by providing data processing services as set out in Annex 1.
3. Prospect and [the company] have agreed that they are Controllers in their own right as defined under Article 24 of UK GDPR.

Purpose of the agreement

4. This agreement is made for the purposes of ensuring compliance with the obligations as set out in UK General Data Protection Regulations (UK GDPR), and the Data Protection Act 2018.
5. Prospect is, within the meaning of the UK GDPR, the Controller of certain types of personal data for purposes connected with [the company] activities and/or persons who work for [the company], and wishes to use the services provided by the processor described in Annex 1 for the processing of personal data connected to its trade union activities.

Personal data to be processed

6. Prospect undertakes data processing for the purposes of providing trade union services to its members. The following types of personal data may be processed under this joint data controller agreement:
    - Personal details
    - Contact details
    - Employment details
    - Education details
    - Finance details
    - **Special category data**: Trade union membership; Physical or mental health details; Racial or ethnic origin; Religious or other beliefs; Sexual orientation; Political opinions; Offences or alleged offences.
7. The categories of data subjects whose personal data is processed is likely to include union members; prospective union members; [the company] staff.

8. The type of processing undertaken under this joint data controller agreement:
    - Trade union activities, including advice and assistance
    - Collective negotiations, including redundancy procedures, and TUPE
    - Personal case work, including grievance, and disciplinary
    - Health and safety issues
    - Industrial relations activities
    - Union communications
    - Recruitment campaigns
    - Maintenance of accounts and records
    - Surveys/ballots

Lawful basis

9. UK GDPR provides explicit protection for trade unions to process their membership data in respect of trade union activities under Article 6(a), 6(b), 6(c) and Article 6(f) Article 9(a), 9(b) Article 9(d), Article 9(f) and Article 9(h).

10. There is a legal requirement on the union to process members' data for a range of legitimate trade union activities and to exercise rights in employment law.

11. Personal data gathered is held in the individual's membership file and/or case file (in hard copy or electronic format, or both), and on [the company] computer systems. The periods for which the Prospect holds personal data are contained in its privacy notices to individuals which can be viewed on Prospect's website.

12. In addition, Article 9(h) provides protection for the work of trade union safety representatives. This is to ensure compliance with the Health and Safety at Work Act 1974.

13. Trade unions also provide training and certification to both members and non-members and in this case, as provided for in Article 6(b).

14. In some cases, Prospect may seek consent from members to enable the union to process personal data for one or more specified purposes, such as promotion of member benefits and services or the use of trusted partners.

Duration and retention of data after termination

15. This agreement takes effect immediately upon the first use of the Services by Prospect (or Prospect's employees or representatives).

16. This agreement will remain in force until terminated by one party by giving to the other a minimum of 28 days' written notice.

17. In the event that this contract is terminated under clause 16, [the company] will allow access to any data which is held on behalf of Prospect for the period of one month beginning with the date of expiry of the notice given under clause 16, after which the data will be deleted. [The company] will notify Prospect in writing before deleting the data.

Processing instructions

18. Subject to clause 20, in providing the services to Prospect, the [the company] will act only on the written instructions of Prospect, either as set out in this Agreement or after notifying the Prospect in accordance with clause 34 that different action is required.

19. Both parties undertake to provide each other with whatever information it needs to ensure that both parties are meeting their Article 28 obligations.

20. The [the company] will not be bound by clause 18 if required by law to act without instructions. In these circumstances, the [the company] will inform Prospect before processing the data, unless that is itself prohibited by law.

Confidentiality

21. The [the company] will ensure that all staff who process personal data on behalf of Prospect are subject to a duty of confidence, through their terms and conditions of employment or engagement.

Data security

22. [the company] acknowledges that, in providing the Services, it is subject to the same requirements as Prospect to keep the personal data that it is processing securely, as set out in Article 32 of the UK GDPR. The [the company] will take all appropriate technical and organisational measures to ensure that its processing complies with Article 32.

Data subject rights

23. Taking into account the nature of the processing both parties shall assist the other by implementing appropriate technical and organisational measures, insofar as this is possible, in order to assist with each parties' obligations to respond to requests to exercise Data Subject rights under UK GDPR.

24. In the event that either party receives a request by a data subject to access their data or to exercise another right under the UK GDPR, each party will provide all reasonable assistance to the other in complying with that request.

Personal data breach

25. Both parties to this agreement will inform the other without undue delay on becoming aware of a data breach affecting their personal data. Each party will assist the other, if necessary, to undertake an investigation and to meet any obligations to report or inform data subjects of the data breach.

Other assistance

26. Both parties to this agreement will provide reasonable assistance with any data protection impact assessments, taking into account the nature of processing and the information available, which is each party reasonably considers to be required in order to meet its obligations under UK GDPR articles 35 or 36.

27. [The company] will provide such co-operation as is reasonable with any audit or inspection into its provision of the Services which may be carried out by Prospect or by an auditor appointed by Prospect. The conduct and scope of any audit or inspection shall be agreed in advance between the parties in writing.

28. [The company] will provide Prospect with whatever information held by [the company] that Prospect needs and is reasonable for [the company] to provide, to ensure that both parties are meeting their obligations under Article 28 of the UK GDPR.

29. The [the company] will immediately inform Prospect if the [the company] is asked to do something infringing the UK GDPR or other data protection law of the United Kingdom.

Other

30. This agreement constitutes the entire agreement between the parties relating to the provision of the Services as listed in the Annex for the purposes of Article 28 of the UK GDPR. This agreement supersedes all prior negotiations, representations, and undertakings, whether written or oral, specifically about the provision of the Services for those purposes. For the avoidance of doubt, the User Responsibilities (as amended from time-to-time) for computer and telecommunications equipment and services, provided by [the company] to persons who work in or for the company, does not form part of, and remains unaffected by, this agreement.

31. [The company] will give written notice to Prospect of any intention to change the terms of this agreement, including any change to the service description, or to take different action under clause 18, or to engage a sub- processor as mentioned in clause 24. Prospect will be deemed to have agreed to the changes to the terms of the agreement, to the different action or (as the case may be) to the engagement of a sub-processor upon the first use of the Services by Prospect (or by Prospect's employees or agents) after the expiry of seven days from any such notice being given.

32. For the purposes of this agreement, a notice shall be deemed to be in writing if it is in electronic form contained in or attached to an email message; and any such notice sent by email shall be deemed to have been given—

    a) in the case of a notice given by [the company] to Prospect, at the time it is transmitted to [the company] email address; and

    b) in the case of a notice given by Prospect to [the company], at the time it is transmitted to this email address: email address

33. This agreement will be governed by and interpreted in accordance with the law of England and Wales and shall be subject to the jurisdiction of the courts of England and Wales.

34. The provisions of clauses 17, 33, 35, 36 and this clause 37 will survive the expiry or prior termination of this agreement.

Signed for and on behalf of [the company]:

Name: ……

Signature: …….. Dated: ……

Signed for and on behalf of Prospect:

Name: ……..

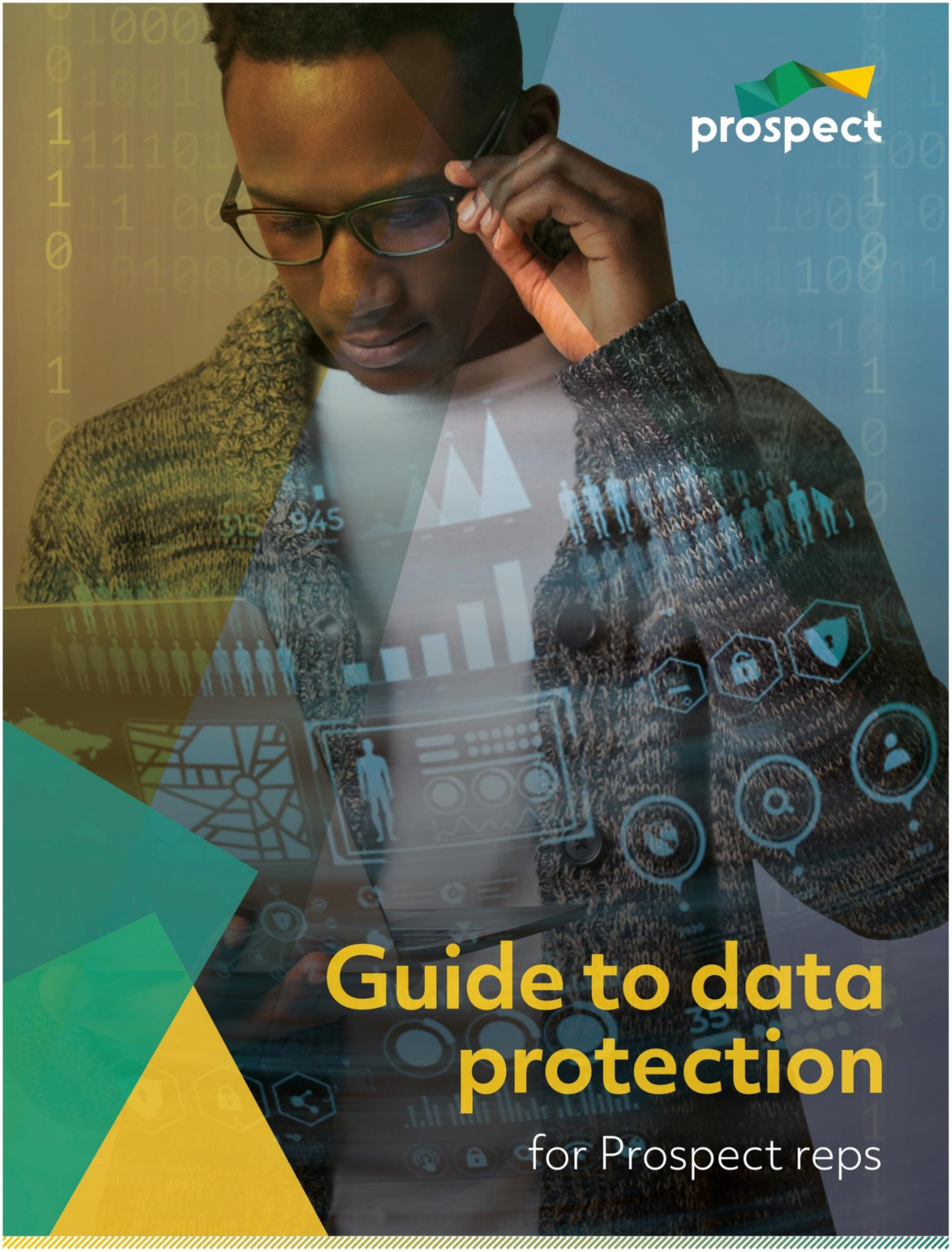
Signature: …….. Dated: ……

Annex 1: Data processing services provided by [the company] to Prospect

The following table shows the data processing services carried out by [the company] on behalf of Prospect for purposes relating to Prospect's trade union workplace activities.

Please amend this schedule as necessary

Service	Description
Office productivity tools	*List the office software you use ie Microsoft Office 365*
Email, calendaring and communication tools	*List the email system used.*
Personal file storage	*List how files are stored ie file server maintained by the company*
Shared file storage	*List shared file storage*
Cyber-security	*Amend as necessary.* *In order to protect its systems, the [the company] uses a range of cyber-security tools including intrusion detection and prevention tools; anti-malware tools; and email filters. The [the company] carries out scans for vulnerabilities and weak passwords and conducts investigations.*
IT support	*Amend as necessary.* *The [the company] provides IT support services and may use tools to backup and migrate data. These services also include the secure destruction of IT equipment.*



prospect

Guide to data protection

for Prospect reps

prospect.org.uk