UNISON
the public service union

A UNISON guide

Privacy and data protection

May 2015

1. Welcome to the Branch Data Protection Handbook

Data protection law in the UK and Europe is being strengthened. This makes it even more important, for UNISON and our members, that privacy is integrated into our day to day work. The increasing profile of the importance of protecting personal data means that the public at large, and so also both our current and potential members, are more conscious of it. We cannot afford data protection to be an afterthought.

With this in mind, this handbook has been designed to give branches an appreciation of the legal requirements that UNISON must abide by to ensure that they comply with the Data Protection Act 1998 (the DPA).

The appendices in this handbook contain further detailed information and example documentation which branches will find useful.

The content of this handbook is correct at the time that it was issued and will be updated from time to time as privacy legislation changes.

Contents

2. Introduction to the Data Protection Act

Basics of the DPA

All organisations in the UK must comply with the Data Protection Act 1998 ("DPA").

The DPA is enforced in the UK by the Information Commissioner's Office ("ICO"). The ICO has a number of powers, including the ability to fine organisations up to £500,000 per data protection breach and publicise information about data protection breaches.

Europe is currently finalising a new data protection law which will almost certainly strengthen an individual's rights in relation to their personal data - the current aim is for the new law to be finalised in 2015 and be in force by 2017/18.

The DPA applies to the **"processing"** of "personal data" by "data controllers" about "data subjects"

"Personal data" is any information about a living individual which enables them to be identified. If data is "obviously about" a person, then it is personal data. Examples of personal data in a UNISON context are:

— Date of birth
— National insurance number
— Membership number
— Bank details
— Workplace address
— Email address
— Home address
— Photograph
— Case notes

Records of opinions about an individual, or intentions towards them, are also classed as personal data.

Personal data can be held in any form on electronic media, such as USB sticks, CDs and computer drives, and hard copy files.

The majority of data UNISON branches hold regarding members is personal data

"Processing" includes:
— Obtaining and retrieving information
— Holding and storing information
— Making information available to others within or outside an organisation
— Printing, sorting, matching comparing, destroying information

Everything UNISON branches do with personal data is considered to be "processing"

A **"Data Controller"** determines how personal data will be used.

UNISON is the data controller for all personal data that branches have with one exception:
Branches are data controller for the employment records that they have about individuals they employ directly

A **"Data Processor"** is a body which processes information on behalf of a Data Controller

UNISON branches are data processors

"Data subjects" are the individuals whose personal data we hold. They include:

— Members
— Prospective members
— Employees
— Previous employees
— Prospective employees
— Agency staff
— Contractor
— Supplier

All of the membership related work which is carried out in UNISON's branches falls under the DPA.

The DPA is about striking a balance between the rights of individuals to know about and control what's happening to their personal data and the sometimes competing interests of those with legitimate reasons for using their personal data.

The eight principles of the Data Protection Act

The DPA is based on eight principles which stipulate that:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be collected for a specific purpose
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and where necessary, kept up to date
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subject
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection

Principle 1 – Personal data must be processed fairly and lawfully

There are six "fair processing" conditions for using individuals' personal data, and UNISON needs to comply with at least one of them (and one of the second set of conditions for "sensitive" personal data which are discussed later) to ensure that data is being fairly processed. The key conditions which UNISON relies on are:

— The individual must have given their **consent** for their personal data to be used by the organisation. The individual will either opt out or opt in of the activity that it is intended that their personal data will be used for. Opt-in consent is required in certain circumstances and seen as preferable in others.
— The processing is **necessary for the performance of a contract** with the individual. This condition is key for UNISON. We have a contract with our members to provide member-related services for their membership subscriptions
— The processing is **necessary to pursue the legitimate interests** of the data controller or third parties (unless it causes unwarranted damage and distress to the individual)

UNISON must publicise a fair processing notice, perhaps now more commonly called a privacy notice. This has previously been published in membership publications. For new joiners (and existing members) there is a detailed privacy policy on the UNISON website, an excerpt of which appears below:

UNISON's Privacy Policy: **https://www.unison.org.uk/privacy-policy/**

Sensitive personal data and further conditions for processing

Some personal data is classed as "sensitive" under the DPA – this data includes information relating to an individual's:

— Racial or ethnic origin
— Political opinions
— Religious beliefs
— Trade union membership
— Physical or mental health
— Sex life
— Commission of offence/s

To be able to use sensitive personal data there are further conditions (additional to those highlighted earlier) which UNISON must meet. The most common are:

— The person involved has given explicit consent for the data to be used
— The data needs to be processed by law
— The data is used to obtain legal advice and defend legal rights
— Racial, religious or health information that is collected for equalities purposes
— The data is required for detection of unlawful activities

As a trade union (personal data about trade union membership is classed as sensitive personal data). UNISON's use of personal data must meet at least one of the conditions for processing personal data and sensitive personal data.

Principle 2 – Personal data shall be collected for a specific purpose

To legally process personal data UNISON must be listed on the publicly available register which is maintained by the ICO. The process of registering is known as "notification".

Under the DPA branches are considered to be data processors, processing data on UNISON's behalf. They are covered by UNISON's registration and so do not need to notify separately. The only time when branches are considered to be a data controller is when they employ staff directly. Organisations do not need to notify if that is only purpose for which they process the personal data about their staff. If your branch is registered, please do not renew the registration.

Notifications identify several "purposes" for processing data, and these are the only activities that UNISON is legally allowed to collect and use data for. UNISON registered purposes include:

— Processing membership data
— Processing potential membership data
— Processing staff data

A copy of UNISON's registration is in Appendix 3 of this handbook.

Principle 3 – Personal data shall be adequate, relevant and not excessive

This principle is all about making sure that UNISON does not collect more information than we need to. For example, our application form used to ask potential members to state whether they were a Mason. The ICO ruled that this information was "not relevant" and instructed us to remove it from the form.

Principle 4 – Personal data shall be accurate

This principle requires UNISON to keep the personal data up to date and accurate. This is important for UNISON when corresponding with members about balloting, and key for accuracy is the use of one single membership system where data is kept up to date.

Principle 5 – Personal data shall not be kept for longer than is necessary

The DPA stipulates that personal data should not be kept longer than is necessary for the purpose it was collected. The ICO expects organisations like UNISON to have a data retention schedule which identifies the different types of document in use and how long those documents should be kept. The DPA does not set specific times for which data should be kept; organisations are expected to consider their own retention needs. However, there are some legal retention periods e.g. case files should be kept for 6 years. Other documents like membership application forms only need to be kept for a year after all the relevant data has been entered onto the membership system. An excerpt of UNISON's retention schedule is in Appendix 6 of this handbook.

Principle 6 – Personal data shall be processed in accordance with individuals' rights

People have several rights under the DPA. The following are relevant to UNISON:

— ***Be provided their personal data held by an organisation.***
These requests are called **subject access requests** (**SARs**). They cover information held in paper form and on computers. UNISON can apply exemptions to withhold some data For example, legally privileged information between UNISON and its legal advisors does not need to be disclosed and documents containing data which would be likely to prejudice our negotiations with the individual do not have to be provided in certain circumstances. As there are no hard and fast rules each request has to be treated on its merits.

— ***Request that an organisation stops processing their personal data.***
Anyone can request that a data controller, such as UNISON, stops processing their personal data if they believe that (and explain why) it causes them or someone else, substantial unwarranted damage or distress. In practice, we may stop doing whatever the person is objecting to. If, however, a member asks UNISON to stop processing their personal data, that person would no longer be able to be a

member, and if a potential member requests this, then they could not go on to become a member of UNISON.

— ***Have their personal data rectified, blocked, deleted or destroyed.***
This right is closely linked with one above because rectifying, blocking, deleting and destroying personal data are forms of "processing". We do not have to comply with the request, but if possible it is generally considered good practice to do so. If a data controller decides not to comply with a request – they think that it would be inappropriate e.g. the individual wants a formal opinion about them to be deleted – an individual can apply to a court to order the data controller to do as they requested.

— ***Stop their personal data being processed for "direct marketing".***
The request has to be acted upon and no further direct marketing material sent to the individual. The ICO defines "direct marketing" broadly – it includes the promotion of an organisation's aims, values and policies. This presents some challenges when we want to contact members with regard to policy and campaigning issues if a member has objected to the use of their email or other addresses.

— ***The right to compensation.***
An individual can claim compensation from a data controller for damage and distress caused by any breach of the DPA. Compensation for distress alone can only be claimed in extremely limited circumstances and is usually defined as a financial loss. Only a court can determine if compensation is warranted.

— ***The right to ask the ICO to assess whether the DPA has been contravened.***
If someone believes their personal data has not been processed in accordance with the DPA they can ask the ICO to make an assessment. If the DPA is found to have been breached and the matter cannot be settled informally, the ICO can take action against the data controller which could be a fine (up to £500,000). UNISON regularly receives requests for assessment from the ICO, where the data subject, who has made a SAR, does not believe that UNISON has given them all of the information they are entitled to, or that we have failed to do so within the statutory 40 calendar day deadline.

Principle 7 - Data security

The DPA requires organisations to keep personal data, whether it be in hard copy or electronic form, secure against accidental loss, damage or destruction. For electronic data e.g. that held on computers or removable media, (USB pens, CDs, etc) the ICO would expect to see password protection, encryption and virus protection, use of firewalls and data backup processes. For hard copy data examples of measures are: door security, lockable filing cabinets, secure storage areas and clear desk policies.

Principle 8 - Transferring data outside the European Economic Area

The DPA states that data is not allowed to be transferred outside of the European Economic Area ("EEA") unless that country is designated as "safe" by the European Commission.

The following countries are currently considered to have an appropriate level of protection:

EEA countries	*Safe countries*
Austria	Andorra
Belgium	Argentina
Bulgaria	Australia
Cyprus	Canada
Czech Republic	Faroe Islands
Denmark	Guernsey
Estonia	Isle of Man
Finland	Israel
France	Jersey
Germany	New Zealand
Greece	Switzerland
Hungary	Uruguay
Ireland	USA (in certain circumstances)
Italy	
Latvia	
Lichtenstein	
Lithuania	
Luxemburg	
Malta	
Netherlands	
Norway	
Poland	
Romania	
Portugal	
Slovakia	
Slovenia	
Spain	
Sweden	
Switzerland	
United Kingdom	

International transfers are not normally an issue for UNISON, but increasingly website hosting and on line services are located in non-EEA countries. It is important that this is borne in mind when using online services. Appropriate safeguards should be in place.

3. The Privacy and Electronic Communications Regulations 2003

The Privacy and Electronic Communications Regulations 2003 ("PECR") support the DPA and are specifically about electronic direct marketing communications. Examples of "electronic communications" are: email, text, fax and automated voice messages. "Direct marketing" is defined very broadly and includes the promotion of an organisations aims, values and policies.

The key requirement of the PECR is that individuals contacted by these methods must have given their prior consent other than in very limited circumstances. PECR does not consider that contacting people as a default unless they have opted out is satisfactory. They look for evidence that individuals have given their explicit consent before any communications take place. This can make contacting potential members and members tricky when it comes to information which is about educational and campaigning matters. Opt-out consent is only acceptable when the following three criteria are met:

1. The contact details were obtained from the individual during a sale or negotiation of a sale for a product or service. For UNISON this will usually be when a person is becoming a member or we are contacting an existing member; and
2. The communications relate to similar products or services; and
3. The option to opt out (or "unsubscribe") was provided when the data was collected and is included on each and every subsequent communication

The conditions are specific and so cannot be relied upon in many situations. Difficulties can arise when using a member's mobile or home telephone number to send campaigning messages if the number was not initially collected for the purpose of campaigning; instead, for example, during an employment case. It is therefore very important to know why the personal data that you have was collected in the first place.

4. The Freedom of Information Act 2000

UNISON

UNISON, although a trade union for public service workers, is not itself a public body. The Freedom of Information Act 2000 ("FOI Act") only applies to public bodies. Any FOI requests which come into the branch office should be forwarded to the regional office for review and response – the standard response is that the FOI Act does not apply to UNISON and therefore the information will not be provided.

Branch officers

Although the FOI Act does not apply to UNISON, it does apply to the majority of our members' employers. As requestors do not always appreciate this and some organisations (such as the TaxPayers' Alliance) sometimes send identical FOI requests ('round robins') - often concerning facility time, DOCAS or similar subjects - to trade unions across the whole of the UK. Notwithstanding the fact that UNISON is not subject to the FOI Act, it is important that our responses to them are consistent across branches. To ensure this please forward any such requests to the regional office. They will respond appropriately.

5. Key branch activities and data protection

5.1 Recruiting and organising

5.1.1 Collecting potential member information

Potential members' personal data can be collected as long as the people are aware their data is being recorded and retained, and they must be allowed to opt out of this data collection exercise. It is imperative that the data collected about potential members is not excessive – avoid collecting more information than is needed – and that it is stored securely and not shared with anyone who has no need to see it. A retention period should be set for this information and, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer or shredded or placed in a confidential waste bin or bag if it is in paper form.

5.1.2 New starters

It is always a good idea to contact new starters and encourage them to join UNISON. Sometimes employers can use the DPA as a barrier to passing this information on to unions. If possible, work with your employer to ensure that they make it clear - perhaps by adding into their induction materials – that, as long as the employees have been given the option to opt out, it is standard practice for new starters' names and contact details to be passed to trade union colleagues. Contact details that are obtained in this way have been collected within the confines of the DPA.

5.1.3 Mapping and monitoring in the workplace

When collecting and recording mapping data it is very likely that the information will include personal data i.e. the data could be used to identify individuals. As is highlighted in section 2 of this handbook, it is important to ensure that people are aware that their data is being collected, and that they are given the opportunity to opt out of their data being collected. If difficulties arise, and individuals decide to opt out of this exercise, the exercise should be carried out in a way to avoid collecting personal data by, for example, using anonymised data.

5.1.4 Data cleansing

This is a crucial activity in the run up to a ballot. It is important to ensure that in the process of collecting updated member data that this data is not inadvertently shared with others. This would breach the DPA and could give cause for members to complain to the ICO. It's important to ensure that a data collection method is employed which maintains individuals confidentiality. For example, do not openly circulate a spreadsheet which contains a line of information for each member; instead, send individual update sheets to individual members. Similarly, do not send out a blanket email to members without using the "blind carbon copy" (Bcc) field – some members wish to keep their membership confidential.

5.2 Storing data and information securely

5.2.1 Hard copies, file notes, incoming and outgoing letter correspondence

Under principle 7 of the DPA UNISON has a duty to ensure that data is held securely. Provisions the branch must consider putting in place include:

- Lockable filing cabinets
- Security keypad on the door of the branch office
- A file logging out and in procedure
- A clear desk policy
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin, for example

5.2.2 Electronic data

The same requirements apply to electronically held data. Provisions the branch must consider putting in place include:

- A logging process for laptop removal from the branch office
- Use storage on a network, rather than laptop or desktop computer, if possible
- Encryption of all removable media (USB pens, CDs etc).
  - If your branch uses employer-provided computers it is likely that these will have some form of encryption installed. If your branch has bought its own computer equipment, it is highly recommended that some form of encryption is considered. Further information can be found at: **http://www.pcworld.com/article/226785/encrypt_your_hard_drives.html**. A copy of the ICO's guide to information security is available on their website: http://ico.org.uk/for_organisations/data_protection/the_guide.
- Password protection on all files containing member data
- Use of RMS for processing member data (encrypted and password protected)
- Up to date antivirus and malware systems
- Adequate firewalls
- Regular offsite data backups (not needed if RMS is used)
- Secure destruction
  - It is important that when a computer is no longer required, that any data is removed in such a way that it is not recoverable. There are several organisations that will forensically clean a computer hard drive and provide a data destruction certificate to prove that it has been done.

5.2.3 Telephone and CCTV recordings

Telephone and CCTV monitoring and recording are not extensively used within UNISON, but if the branch is using these facilities, it is important to consider that these recordings contain personal data. It should be noted that the recordings would be subject to any request for access by an individual under the DPA, and should also be subject to a data retention policy and be deleted once the appropriate period has expired.

More information on CCTV and data protection is available on the ICO's website: **http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv.**

5.3 Sharing information

Personal data can be shared with third parties but it has to be done with care.

5.3.1 Using an external print/processing house

When data is passed to third parties for processing, the ICO requires organisations to choose a third party which will provide sufficient security guarantees for both its use and storage. It doesn't matter whether the information is electronic or hard copy. Examples of third party processors are:

— Mailing houses
— Website hosting
— Payroll

It is essential that a formal agreement is in place with third party processing organisations. The agreement should ensure that there is a contractual obligation on the processor to:

— Implement specific security measures
— Use the data only for the original purpose they received it
— Have trained personnel
— Disallow further sub contracting
— Grant rights of access for audit purposes

An example Data Processor Agreement is in Appendix 3 of this handbook and standard ones for use are available on SharePoint: **http://teams.unison.org.uk/groups/DPinUNISON/Forms%20and%20templates/Forms/AllItems.aspx** or in your branch. A contract containing appropriate clauses is also sufficient.

A third party is anyone except the person whose personal data it is

Misusing personal data could have serious consequences for both you personally and UNISON as a whole: you could face an investigation and disciplinary action (in certain circumstances prosecution by the ICO) while UNISON could be fined up to £500,000 and/or negative publicity and reputational damage.

5.3.2 Extracts from the membership system

Requests for extracts from the membership system should be treated with caution. Often, requests are received from other, similar organisations for data which will enable them to contact our members directly and offer them products or services or ask them to participate in a survey. Always refer these requests to the region – the principles of the DPA apply. Each request needs to be carefully reviewed to determine whether to pass the data on to the third party.

If any extracts have been taken, it is essential that the branch ensures that appropriate permissions are in place. They should ensure that the information is:

— Passed to the receiver securely;
— Not circulated widely;
— Only made available to individuals that the branch approves;
— Only used for the specific purpose for which it was extracted;
— Held securely and;
— Securely destroyed after use.

The importance of thinking before sending extracts from WARMS/RMS or any other personal data to a third party cannot be overstated. Consider what you are doing it for and check that doing it will not breach the DPA. Personal data should not be sent to personal email accounts for any reason.

Below is a table of 'dos and don'ts' which should be borne in mind when extracting information from WARMS/RMS:

Do	***Don't***
Only extract the information that is needed to complete a task. This makes sure that the data that is being used is up-to-date and accurate	Extract more than you need for a task. A lack of time is not a legitimate reason for not producing tailored reports
Only use extracts for one task. A new list should be extracted for each task	Provide information to others not involved in the task for which the data was extracted
Keep the information on systems and networks that are recognised as being acceptable for UNISON work. These may belong to an employer or the union	Email information to a personal email address or save it onto a personal device for any reason. **This is a serious breach of the Data Protection Act**
Take care when taking personal data out of the office. Only take the information if it is necessary, keep it safe and return it as soon as possible	Keep the information that you have got to use for a very similar exercise that you know you're going to do in the future
Update WARMS/RMS if a member's details etc are out of date	Leave personal data that has been taken out of the office unattended
	Put information into a normal bin use a secure disposal bin or bag. Someone else could find it and misuse it. **This is a serious breach of the Data Protection Act**
	Have and/or amend a local list. WARMS/RMS data should be the only information that you use.

5.3.3 Releasing information to prevent or detect crime; requests for disclosure under section 29 of the DPA

The police or other crime prevention/law enforcement agencies (e.g. Benefit Fraud Office and Local Authority functions) sometimes contact data controllers or data processors and request that personal data is disclosed in order to help them prevent or detect a crime. UNISON does not have to comply with these requests, but the DPA does allow organisations to release the information if they decide it is appropriate.

Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This include considering:

— The impact on the privacy of the individual/s concerned
— Any duty of confidentiality owed to the individual/s
— Whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for UNISON to release the information.

If such a request is received at a branch, please refer the requestor to the UNISON's Data Protection Officer at the UNISON Centre.

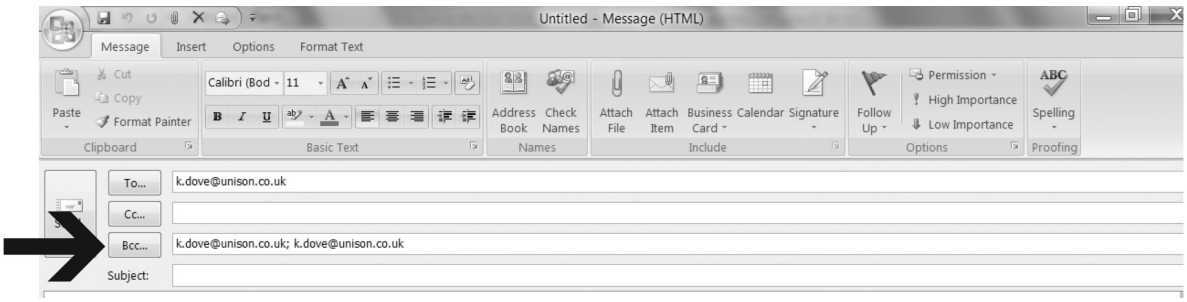
5.4 Communicating with members

As is explained in section 3 of this handbook (about the PECR), contacting members by email or text message requires opt-in consent.

5.4.1 Using email and text messaging

As well as the conditions relating to PECR, the ICO has stated that all email addresses are personal data, and as UNISON is a trade union, email addresses are sensitive personal data, requiring extra conditions to be met before the data can legally be used. It is therefore essential that when communicating with members using email and text distribution lists that the following provisions are made:

— Individuals who have opted out of mailings (apart from statutory information like ballots information) are not included in mailings or bulk text messages
— The blind carbon copy (Bcc) field on the email address line – shown below – is used.



— If a member informs the branch that they no longer wish to be contacted via email or text, their name and contact details must be removed from the distribution list, and a note made that they have not consented to receive emails or texts. The only exception to this is if the message contains statutory UNISON information and cannot be provided to the member in another way.
— An option to unsubscribe to similar communications is added to the bottom of the email or text message each time a message is sent out.

5.4.2 Sending letters to members

Some members wish their trade union membership to be confidential and request that any union related mailings are sent to their home address, rather than their workplace address. The branch should ensure that these requests are complied with. Inadvertent disclosure of an individual's trade union membership (sensitive personal data) would be a breach of the DPA.

5.5 Representing members - employment, welfare, and health & safety case files

Any information directly related to a potential or actual case is extremely sensitive and several of the DPA principles apply. Provisions that the branch need to make include:

— Secure storage for live and archived case files
— Limited access to only those officials who need to see the data
— Collection of data limited to only that which is relevant to the case in hand
— Information held in the file is accurate
— A sign in/out process if the file needs to be taken out of the branch office
— File retention policy
— Secure disposal

It is much safer to keep any case files within the branch. If this is not possible, i.e. a file needs to be taken off the premises considerable care should be taken to ensure that its whereabouts are known, and that it is always kept secure.

In order to preserve the legal privilege that exists between UNISON and its legal advisors - both our in-house legal team and external advice from Thompsons - legal advice that is sought regarding a merits assessment for a particular case, the original documentation between UNISON and the legal advisors should not be copied in full to the member. This information should be summarised before passing it to the member – this serves to protect UNISON's interests in the longer term.

5.6 Requests for an individual's own personal data (a "subject access request")

5.6.1 The right of the individual

Under the DPA an individual has a right to request all the personal data that an organisation holds about them. They also have a right to know the source of the data, the purposes that it is being held for e.g. to process an individual's membership and who it has been shared with. The individual needs to make the request in writing by letter, email, fax etc.

UNISON receives several subject access requests (SARs) each month. Individuals requesting access need to pay a standard processing fee of £10, provide some form of identification, and information about the data they are seeking. By law, once these have been received, UNISON must respond to the request within 40 calendar days of receiving it, the £10 fee and proof of identity e.g. the individual's membership number. Data we need to provide can include:

— Details held on the membership system including notes
— Case files including handwritten notes, emails, letters etc
— CCTV footage
— Photographs
— Telephone call recordings
— Records of any contact with UNISONdirect
— Complaint files

The scope of the search includes branches, regions, UNISON Centre, UNISON*direct* and any other organisation which is processing data on UNISON's behalf.

It is important to note that email and hard copy exchanges between branch officials and representatives to each other and to/from regional officers with reference to any representations or issues with members or other individuals may be have to be considered for disclosure in response to a SAR. So please:

— Keep any documented information factual
— Carry out periodic housekeeping on email and other information sources as necessary
— Keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document
— Only copy into emails those people who "need to know"
— Do not use abusive or derogatory language in emails or other documents
— Do not include any personal opinions in email or other documents
— Do not use email when a telephone call will do

5.6.2 What to do if a request for subject access arrives at the branch

If a verbal request is received the branch should inform the individual that they need to put their request in writing and that there is a £10 processing fee – details of the address they should contact are in Appendix 4 of this handbook.

If the branch receives a request in writing, it is important to forward it to the region immediately otherwise time could be lost and so fewer days available to complete the response to the request.

The branch should be prepared (but not begin) to gather all their relevant documents, including emails, as the region/UNISON Centre will soon be in contact asking for it. It is important to provide all the relevant documents, even if some are thought to be contentious. UNISON Centre's SARs team will review each piece of documentation before it is passed to the member, and will either redact, withhold or provide the data as part of the response to the SAR. Flag any documents which are considered to be contentious or sensitive in some way and don't want to be disclosed. Please explain why you are so concerned about them being released. This will help inform the response to the SAR but does not mean that the information will be able to be withheld. Information can only be withheld in response to a SAR in very limited circumstances.

5.7 What to do if there is a suspected or actual breach of the DPA

Actions to take immediately

In all cases, regardless of the level of impact contact your regional data protection contact immediately. Give them all the information that you can at that point about the breach. For example:

— The nature of the actual or suspected breach
— The type of data involved and its sensitivity – a copy of the information that has been compromised if possible
— How the breach happened
— When it happened
— When did you become aware of it
— If data has been lost or stolen in relation to a laptop or pen drive whether encryption or password protection is in place
— Has anyone tried to retrieve the data e.g. recall an email
— What the data could tell a third party about an individual, and whether there is a chance that the data could be used to cause damage or distress
— The number of people affected by the breach and whether they are aware a breach has occurred

Once a breach has been reported

The region will liaise with the branch in the first instance and may decide to refer the issue to UNISON's Data Protection Officer. The Data Protection Officer will decide how the breach should be dealt with. A summary of the breach reporting procedure for branches is in Appendix 5 of this handbook.

It is essential that breaches are looked into quickly – this helps to minimise their impact. UNISON can be fined up to £500,000 for serious breaches of the Data Protection Act.

Once a breach has been managed, it is important that any lessons learned and security improvements are put in place as soon as possible, to avoid any recurrence of the same problem.

Appendix 1 - Useful links

— Data Protection SharePoint site:
http://teams.unison.org.uk/groups/DPinUNISON/default.aspx
— Information about encryption:
http://www.pcworld.com/article/226785/encrypt_your_hard_drives.html.
— Information Commissioner's Office's Guide to information security & breach management:
http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.pdf
— Information Commissioner's guidance on CCTV and data protection:
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv
— UNISON's data protection registration:
http://ico.org.uk/esdwebpages/search - type Z9055341 in the 'registration number' field
— UNISON's privacy policy:
https://www.unison.org.uk/privacy-policy/

Appendix 2 -UNISON's data protection registration entry

Like all data controller UNISON is required, under the Data Protection Act, to register the purposes for which we use the personal data that we have. Below, for illustrative purposes, is UNISON's registration entry for 2014-15 which is available online. The entry is renewed and updated as necessary every year and the most up-to-date version can be found at: **http://ico.org.uk/esdwebpages/search** and typing Z9055341 in the 'registration number' field.

Data Protection Register - Entry Details

Registration Number: Z9055341

Date Registered: 12 May 2005 **Registration Expires:** 11 May 2015

Data Controller: UNISON

Address:

UNISON CENTRE

130 EUSTON ROAD

LONDON

NW1 2AY

This register entry describes, in very general terms, the personal data being processed by:

UNISON

Nature of work - Trade Union

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to provide a range of services to our members which may include administering membership records including the balloting of members and potential members; providing and organising activities for union members; promoting our services; supporting and managing our employees.

Type/classes of information processed

We process information relevant to the above reasons/purposes. This information may include:

— personal details
— family details
— financial details
— employment and education details
— goods and services provided

We also process sensitive classes of information that may include:

physical or mental health details
— racial or ethnic origin
— religious or other beliefs
— trade union membership
— sexual life
— political opinions
— lifestyle and social circumstances
— information about offences and alleged offences

Who the information is processed about

We process personal information about:

— members
— supporters
— enquirers, complainants
— employees

Who the information may be shared with

We sometimes need to share the personal information we process with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

— current, past or prospective employers
— suppliers and service providers
— employment and recruitment agencies
— family, associates and representatives of the person whose personal data we are processing
— educators and examining bodies
— financial organisations
— trade union and employer associations
— professional bodies
— data processors
— central government

CCTV - Crime Prevention and/or Staff Monitoring

CCTV is used for maintaining the security of property and premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the data subjects themselves, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the data protection act.

Appendix 3 - UNISON's data processor agreement for branches

Template Data Processor Agreements – including that for branches - are available on SharePoint: **http://teams.unison.org.uk/groups/DPinUNISON/Forms%20and%20templates/Forms/AllItems.aspx.**

Below is a copy of the current template for the Agreement that branches are encouraged to use

DATA PROCESSOR AGREEMENT

This Agreement is made on the [day] of [month] [year]

BETWEEN

UNISON [branch name and address] and

[Supplier name and registered address]

WHEREAS

a. UNISON [branch] wishes to engage [supplier] to process personal data on its behalf, and

b. Each time [supplier] processes personal data on behalf of UNISON [branch] the data will be processed on the terms and conditions laid out in this Agreement.

IT IS HEREBY AGREED THAT

Interpretation

The following terms:

"Data"

"Data Controller"

"Data Processor"

"Personal Data"

"Processing"

have the meanings given in Section 1(1) of the Data Protection Act 1998.

"Data Controller" means UNISON, UNISON Centre, 130 Euston Road, London, NW1 2AY

"Confidential information" means UNISON [branch's] and the Data Controller's secrets and confidential information and extends to all knowledge or information relating to both, their organisation, finances, processes and membership information held by UNISON [branch.

Data Processing

1. The terms of this Agreement shall apply whenever [supplier] processes data on behalf of UNISON [branch]
2. [Supplier], as a data processor, will:

2.1 Act only on instructions from UNISON [branch]

2.2 Comply with the obligations set out in the Seventh Principle of the Data Protection Act 1998 by taking:

- appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and
- reasonable steps to ensure the reliability of any of its employees who have access to the personal data

Confidentiality

3. [Supplier] shall both during this Agreement and after its termination (without limit in time) keep confidential and not (except as authorised or required by the purposes of this Agreement) use or disclose or attempt to use or disclose any confidential information supplied by UNISON [branch] or its members.

4. Confidential information will only be made available by the parties to those of their staff and agents who have a reasonable need to know of it. The documents or other materials and data or other information or copies thereof will not be made available to any third parties except for professional advisers in confidence or if required by law,

5. [Supplier] shall not under any circumstances subcontract the processing of UNISON [branch's] data without prior written permission from UNISON [branch] to do so.

6. Either party is entitled to demand the return of any documents or other material or data or other information supplied to the other party under this Agreement within one month of giving the other party written notice.

7. On the cessation or earlier termination of this Agreement, each party shall return to the other all documents or other material containing confidential information and destroy any surplus copies.

8. Paragraph 7 of this Agreement shall not apply to documents, other materials, data or other information which are already in the public domain at the time when they were provided by either party or if at any time the information becomes public knowledge through no fault of the other party.

9. Both parties undertake that any information which is received from the other party under this Agreement will only be used for the purposes of this Agreement.

Requests for information

10. [Supplier] must inform UNISON [branch] immediately (within 2 working days) of any requests it receives for copies of UNISON [branch] data, and only respond to any such request as directed by UNISON [branch] or the Data Controller. [Supplier] shall also co-operate fully with any reasonable requests made by UNISON [branch] or Data Controller in relation to any such requests.

Inspection

11. The Data Controller may, on reasonable notice and during business hours inspect [supplier]'s data processing facilities, data files and relevant documentation.

Indemnity

12. [Supplier] shall indemnify the Data Controller, against any loss or damage it sustains or incurs as a result of any loss, theft or un-reparable damage to UNISON [branch]'s data or any other failure by [supplier] to comply with its obligations under this Agreement, including any regulatory fine imposed on the Data Controller because of [supplier]'s action or omission.

Governing Law

13. This Agreement is subject to English Law and the parties submit to the non-exclusive jurisdiction of the English Courts.

Signed …….. Name……..

For and on behalf of UNISON [branch]

Signed …….. Name……..

For and on behalf of [supplier]

Appendix 4 – Subject access requests: address details

Potential subject access requests

If you receive a verbal subject access request i.e. asks for their own personal data, or asks how to place one, you should tell them to write to:

Data Protection Officer

UNISON

UNISON Centre

130 Euston Road

London

NW1 2AY

Individuals requesting subject access should write to the above, enclosing:
— proof of identity (membership number, NI number etc)
— a £10 processing fee
— details of the information they are seeking

Receiving a formal subject access request or any other request for personal data

Forward any requests for information that you receive to your regional data protection contact immediately

For subject access requests you should be prepared to:
— gather all the relevant documentation, including hard copies of emails – region/ head office will be requesting these
— provide all information, even if contentious

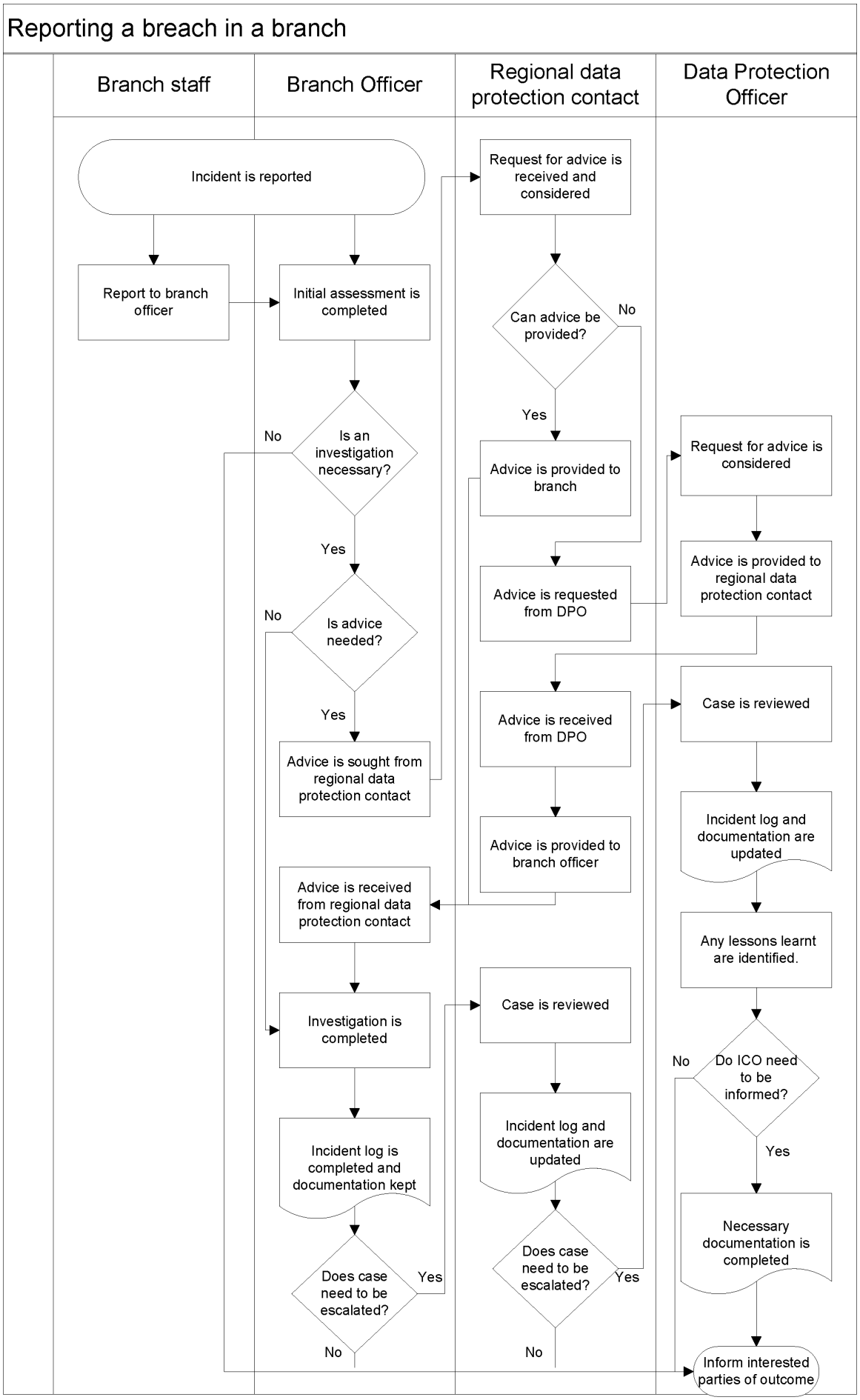
The SAR team will review each document and decide whether to redact, withhold or provide.

Appendix 5 – Branch data protection breach reporting procedure

A flowchart showing the process for reporting breaches is in the appendix. Please use it if you either think or know that the Data Protection Act has beem breached.

More detailed information on managing breaches – including flowchart is available in the 'Managing breaches' section of the Data Protection SharePoint site: **http://teams.unison.org.uk/groups/DPinUNISON/Knowledge%20%20Learning%20Resources/Forms/By%20Category.aspx.**

The log and other forms and templates are available in the 'Breaches' section: **http://teams.unison.org.uk/groups/DPinUNISON/Forms%20and%20templates/Forms/By%20Category.aspx.**


Reporting a breach in a branch
Branch staff
Branch Officer
Regional data protection contact
Data Protection Officer
Incident is reported
Report to branch officer
Initial assessment is completed
Is an investigation necessary?
No
Yes
Is advice needed?
No
Yes
Advice is sought from regional data protection contact
Advice is received from regional data protection contact
Investigation is completed
Incident log is completed and documentation kept
Does case need to be escalated?
Yes
No
Request for advice is received and considered
Can advice be provided?
No
Yes
Advice is provided to branch
Advice is requested from DPO
Advice is received from DPO
Advice is provided to branch officer
Case is reviewed
Incident log and documentation are updated
Does case need to be escalated?
Yes
No
Request for advice is considered
Advice is provided to regional data protection contact
Case is reviewed
Incident log and documentation are updated
Any lessons learnt are identified.
Do ICO need to be informed?
No
Yes
Necessary documentation is completed
Inform interested parties of outcome

Appendix 6 – Retention schedule

UNISON's retention schedule is available on SharePoint at: http://teams.unison.org.uk/groups/DPinUNISON/Data%20Protection%20Policies%20and%20Procedures/Forms/AllItems.aspx.

An example is:

Record category	Description	Examples	Start of retention period	Retention period	Action
Case Files	Documents generated during the course of representation of members from initial stages through to resolution.	Completed CASE form Meeting notes Email exchanges Compromise agreements General Communication from/to member	Closure of case	6 years	Secure destruction
Membership Information	Manual membership forms	Membership form Direct debit forms/ bank details	Membership accepted and all details transferred to RMS	1 year	Secure destruction

UNISON
the public service union

Designed and produced by UNISON Communications Unit. Published by UNISON, UNISON Centre, 130 Euston Road London NW1 2AY

CU/MARCH2015/22957