Data Protection Guidelines

The Labour Party

Last revised Friday, 11 November 2016

Labour
labour.org.uk

1 Introduction

1 The Labour Party has legal responsibilities under the Data Protection Act (1998) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 with regard to the storage and use of all data. Failure to comply with the law in this area is likely to lead to civil enforcement or prosecution.

2 The Data Protection Act (1998) was updated in order to further protect the identity of the individual and to promote the openness and accountability of public authorities and private companies. It is largely a response to the use of personal data by companies and public sector organisations and the potential misuse of that data in ways that could adversely affect the lives of the individuals on whom data is held. For instance, information incorrectly stored may lead to people being wrongly refused credit or if data is not held securely may result in a breach of privacy.

3 It is normally an offence (there are some exceptions, for example domestic use) to process personal data without notifying (registering with) the Information Commissioner.

4 Why comply? The Following is an extract from Guidance for political parties for campaigning or promotional purposes produced for political parties by the Information Commissioner's Office.

> *"The actions of a political party come under close scrutiny from the public and the media. It is not just in your interests to act lawfully but you should also have respect for the privacy of the individuals you seek to represent by treating them fairly. Treating individuals fairly includes using their information only in a way that they would expect, while respecting any preferences they have expressed about not receiving direct marketing (subject to a candidate's right to send an election address at a parliamentary election).*
>
> *"In recent years we have investigated complaints about political parties using direct marketing and on occasion we have used our enforcement powers to prevent the party doing the same thing again. Failure to comply with an enforcement notice is a criminal offence. We will consider the nature and number of any complaints received about direct marketing by political parties with a view to using the powers at our disposal to prevent parties from making the same mistake in future.*
>
> *"The complaints we have received reveal that individuals find unwanted direct marketing, and unwanted contact from political parties in particular, to be extremely annoying. This is more likely to be the case where more intrusive means of contact are used or the individual has previously objected to marketing and where they are opposed to your views."*

5 It is imperative that data controllers must comply with the enforceable principles of the Data Protection Act – and that may mean you. Whilst it will usually be the organisation which is the data controller rather than an individual, there will be a named individual responsible for ensuring that the Labour Party, or your colleagues or department, complies with regulations, is considered the data controller. And everyone has to ensure that our policies are complied with – and if you are not sure, ask.

2 What is data?

1 Data (which includes paper records kept in organised, searchable filing systems) means information which:

- Is automatically processed, or
- forms or will form part of a relevant filing system, or
- forms part of an accessible record, or
- is held by a public authority whether or not it falls within any of the above paragraphs (the Labour Party is not a public authority)

3 Principles of the Data Protection Act (1998)

1 The Data Protection Action (1988) identifies several key principles upon which the Act is based, which set out how data should be stored and processed. An understanding of these principles is essential for a ensuring that the way we deal with personal data complies with the current legislation.

3.2 Use of personal data

1 All personal data should be fairly and lawfully 'processed'

2 'Fairly' should be taken in its everyday context. We must make it clear to data subjects (individuals upon whom we hold data) the reason we ask them to supply personal details - e.g. to keep them updated about Labour Party policy.

3 Once this boundary is set, data may not be used for any other purpose other than that for which it was supplied unless with the agreement of the data subject.

4 'Lawfully' covers a number of different situations, including that data must:

- be obtained in a proper manner (not by computer hacking etc),
- be processed only for the purpose for which it was supplied unless further permission is granted, and
- fulfil any duty of confidentiality.

5 'Processed' has been defined for this purpose as obtaining, recording or holding data and carrying out various operations which cover anything you may wish to use the data for. Altering, amending, retrieving, using and combining are just some of the definitions considered as processing.

3.3 Sensitive personal data

1 Sensitive personal data can be any of the following:

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union (within the meaning of the M1Trade Union and Labour Relations (Consolidation) Act 1992),
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission of any offence by the data subject, or
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such

2 The processing of sensitive data requires explicit consent. To use this data we must ensure that:

- completion of sensitive data on all documents (including electronic) is optional and this option is explicit
- data subjects are aware of what we may use this data for, for example, statistical analysis of our membership
- it is not disclosed to a third party without consent of the data subject
- processing is carried out in the course of the party's legitimate activities
- it may only be shared with the express prior consent of the data subject

3.4 Processed for limited purposes

1 Personal data must only be obtained for one or more specified and lawful purpose(s) which have been notified to the data subject. It must not be further processed in any manner incompatible with that purpose.

2 For example, regular mailings about local Party activity sent to a member would be compatible; the same mailings sent to a non-member would not be compatible and

would therefore require consent from the non-member to receive such a mailing. Similar principles extend to electronic communications

3 Principles applicable to all personal data on all occasions

4 Adequate, relevant and not excessive

5 There must always be a view as to how and when data may be used. Unless there is a 'foreseeable contingency' that the data will be used, the data must not be held.

3.5 Accurate

1 Personal data must be accurate and where necessary kept up to date. This is essential with all records, including all electoral register systems. Inaccurate is defined as incorrect or misleading as to any matter of fact.

2 Not kept longer than necessary

3 Data that allows or could allow identification of data subjects must not be kept for longer than is necessary for the purpose for which it was supplied. All records and files must be updated regularly; any records and files you no longer use or require must not be retained.

4 Processed in accordance with the data subject's rights

5 For example, a data subject may prevent processing where data and the processing of it, is likely to cause damage and distress.

3.6 Secure

1 Appropriate measures, both technical and organisational, must be taken against:

- unauthorised and unlawful processing of personal data
- the accidental loss of personal data
- damage to personal data

2 You must therefore take extra care when emailing or faxing sensitive data:

- avoid storing data on computer areas that are accessible to unauthorised people
- appropriate steps must be taken to secure personal information online, for example credit card details
- databases containing sensitive personal data must be protected with a password
- care must be taken when transmitting large amounts of data, for example lists of members or electors, electronically. Typically this should include the encryption and password protection of the file being transmitted and the separate deliver of necessary passwords.

3.7 Not transferred to certain countries without adequate protection

1 The countries are specified as those outside the European Economic Area (EEA) plus any other countries that have become approved. Both the data holders and the countries must have the appropriate security and data protection measures in place to ensure data is not endangered.

4 Notification as a data controller to the Information Commissioner

4.1 General

1 It is normally an offence under the 1998 Data Protection Act to process personal data without registering with the Information Commissioner (or notification in the official language).

2 Personal data is data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession or is likely to come into the possession of the data controller. It includes any expression or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.2 How to notify

1 It costs £35 per year and is carried out by contacting the Office of the Information Commissioner (OIC) notification hotline telephone on 01625 545740 or online at www.ico.org.uk. The Commission will advise if there are any queries.

2 CCTV must be included under the crime prevention and detection clause.

3 CLPs, elected representatives, Scotland and Wales National Offices must notify separately to Labour Party Head office.

4.3 Registration by CLPs

1 Each CLP must ensure it has renewed its annual notification with the Information Commissioner as a 'data controller' - an organisation that processes data on individuals.

2 CLPs do not need to be notified to use the data provided nationally in MembersCentre or Contact.Creator (as Head Office notification covers this), but, the vast majority of CLPs will need to notify if they:

- process any other computerised data on members;
- process data on electors, e.g. in locally held mailing lists etc. or make use of your entitlement to a free copy of the electronic version of the full electoral register

- hold any relevant manual filing systems that are structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible

4.4 Registration by MPs and MEPs and other elected representatives

1 Each MEP and MP must notify separately from their region or CLP. In addition to the requirements described for CLPs, data collected from constituency casework must be notified.

2 Details of data subjects collated in official 'Member' capacity may not be shared, as personal data may not be collected for one purpose and used for another without the consent of the data subject. Case work personal data must not be disclosed for party political purposes.

3 Membership lists supplied by a CLP are covered in the CLPs notification, so the Member need not notify separately. However, the Member must comply with the data protection principles when using this data.

4.5 Registration by Councillors

1 Councillors are not covered by the notification made by the local authority in respect of this data. Further information may be obtained from the Monitoring Officer of the local authority.

2 Each Councillor must notify individually for the data they collect. In addition to the requirements described for CLPs, data collected from casework must be notified.

3 Details of data subjects collated in official 'Councillor' capacity may not be shared or given, as personal data may not be collected for one purpose and used for another without the consent of the data subject. Council held personal data must not be disclosed for party political purposes.

4 Personal information collated on data subjects processed by an employee of the Council need not be notified as the Council is considered to be the Data Controller.

5 Membership lists supplied by a CLP are covered in the CLPs notification, so the Councillor need not notify separately. However, the Councillor must comply with the data protection principles when using this data.

4.6 Registration by Scottish and Welsh Offices

1 Are notified separately from the UK Head Office in addition to the UK Head Office notification.

4.7 Registration by Head Offices and the Regional Offices

1 Both Head Offices and the English Regional Offices and the Scottish and Welsh Offices are covered by one notification which is dealt with by the Compliance Unit at our London Head Office. Any changes to the types of data held must be reported to the data controller immediately.

2 We are currently covered under eleven different situations. These are:

- staff administration
- administration of membership records
- fundraising
- canvassing political support amongst the electorate
- accounts and records
- advertising, marketing and public relations
- information and databank administration
- crime prevention and prosecution of offenders
- accounting and Auditing
- advertising Marketing & Public Relations For Others
- research

5 Applications for a Subject Access request

5.1 General

1 Anyone can request that we search our files for personal data we may hold on them at any time.

2 In order to process a subject access request fully, the data controller should be aware of every information system within their organisation that they are responsible for. It should be clear to the data controller which systems hold personal data, sensitive personal data, accessible records, relevant paper-based filing systems and when each system was last amended.

3 Data controllers are advised to keep a record of all information systems within their responsibility. This will enable a quick search. Data controllers have the authority to request every departmental manager to provide a regular update of their information systems. Data processors must also be aware of their responsibilities in terms of the Act.

4 A pro forma is available from the Data Protection Officer in the Compliance Unit at Head Office as an aid to processing subject access request information. The form must be fully completed by the data subject and returned with proof of identity to the registered data controller with a cheque or postal order for £10. No data should be supplied without a written request. However the absence of our own form should not be used as a reason for not processing a subject access request. Any request which clearly identifies the subject and the data requested, and is accompanied by the proper fee should be acted upon.

5 Data subjects must supply details in order for the data controller to be satisfied as to the location of the information the data subject seeks. If a data subject is locating specific information relating to a decision made by the party that affected them, provided their personal data is included in these documents then the relevant sections and the context in which they were held in must be disclosed.

6 Once these criteria have been met, the data controller must provide all personal data to the data subject within 40 days.

5.2 What must be disclosed

1 Data controllers are required to provide:

- a description of the type of data held
- the purposes for which it is held and,
- the recipients of the data

2 Documents that make a passing reference to an individual must be disclosed. However, it may not be necessary to release a complete document. In this instance it may be reasonable to supply relevant sections of the document. The requirement to disclose applies to draft documents even if they were never published, released or supplied to third parties. If no data is found to exist, data subjects must be informed.

3 The data controller is responsible for the protection of the identity of any third parties who may be mentioned in disclosed documents. Identities should not be revealed without consent unless the data controller deems it to be reasonable to comply without consent.

4 You do not need to supply hard copy data if:

- the data subject agrees to accept the data in another form
- the supply of a copy is not possible or,
- the supply of a copy involves disproportionate effort

5 A disk may therefore be acceptable.

5.3 Where to look

1 The data controller is legally obliged to search for data in:

- Automated data storage:
- All relevant computer systems, audio tapes, video tapes etc. must be made available to search for requested data. This includes membership records, draft documents, security videos etc. Private emails may be checked in the course of this search if they are stored within our systems. All documents must be treated as if they were final versions.

2 A data subject need not be explicitly referred to in order for a document to be disclosed. It is sufficient that they may be identified by description or job title eg Leader of X Council.

3 Relevant filing systems:

4 There is an assumption that an organisation's stored manual files will be accessible with a reasonable level of file management in place, making a search relatively easy to conduct.

5 Manual files that are structured by reference to individuals for example, members, or by reference to criteria relating to individuals for example, membership number/postcode, must be searched. Files kept in storage are not exempt and may be recalled if the data contained is in a relevant filing system.

6 Other manual files include, index cards, box files, account books, schedules and calendars.

5.4 Exemptions from search

1 You are not required to look under certain circumstances, including:

- unstructured, random files containing unrelated data
- any exclusively manual files of documents that do not form a filing system structured by reference to individuals

2 Identical or similar requests from a data subject need not be acted upon unless a reasonable interval has elapsed. When considering if the interval is reasonable the data controller should consider:

- the nature of the data,
- the purpose of the processing and,
- the frequency with which the data are altered.

6 Membership lists

1 Membership lists must not be released to any third party other than those entitled to receive them (as defined in the NEC Procedural Guidelines). In such cases, the list supplied must only be used by the member for the purposes it was given. They must be informed of their data protection responsibilities using the pro-forma letter available from the Compliance Unit at Head Office. External organisations contracted by the party are supplied with this data following a confidentiality agreement, and the data must be returned or securely destroyed upon completion. Union and non-union affiliates are not entitled to receive membership lists except for the sole purpose of contacting CLP secretaries to arrange or renew affiliations. Other data sharing agreements may from time be established as allowed under the current legislation.

2 Union or non-union affiliates who wish to contact members may have their document included in a party mailing (local or national). All documents must be approved through the appropriate channels prior to mailing (Regional Director, General Secretary or Bulk Communications Manager with the agreement of the General Secretary).

7 Telephone Preference Service (TPS)

1 Information contained in the electoral register may be used for 'electoral purposes'. However, TPS is a service available to individuals if they do not wish their phone/fax number to be obtained by third parties for the purposes of direct marketing.

2 Voter ID and GOTV are not considered as direct marketing and as such we do not need to check for TPS registration.

3 TPS must be checked prior to making calls involving fundraising, recruitment, or promoting or requesting for support for a candidate or for the Labour Party's aims and ideals. When calling, callers must identify themselves and that they are calling from the Labour Party. If asked, they must provide either a valid business address or a freephone telephone number where the party can be contacted.

4 Numbers that are not supplied to us by the individual must be checked for TPS registration. Calls are not considered to be unsolicited if an individual has notified the caller that s/he does not object to receiving calls on this topic. Subsequent TPS registration does not automatically override notification of non-objection, therefore we may continue to contact these people unless they request otherwise.

8 Voter ID/GOTV (Get Out The Vote)

8.1 Voter ID scripts

1 All Labour Party scripts must adhere to/contain the following:

2 When contacting voters either by phone or in person on the doorstep, in order to secure further contact, the individual must be asked if they have any objections to the Labour Party contacting them in the future. Therefore voter id scripts must:

- state that we will use all contact details supplied to contact them; and
- allow an opt-out which, if taken, must be recorded and adhered to. So if someone asks you not to call again, make sure that is acted upon.

3 When contacting on the telephone, in addition to the above, callers must identify themselves and that they are calling from the Labour Party. If asked, they must provide either a valid business address or a freephone telephone number where the party can be contacted.

4 Questions which are acceptable to use for voter ID include:

- With which political party do you most closely identify?
- For which party will you vote for at the next general/local/Euro election?
- Which party did you vote for last time?
- Who would be your second choice?
- Do you vote at every election?

5 At any point the voter may terminate the conversation. If they ask not to be contacted again by the party this must be recorded and adhered to by adding a suppression or attribute specifying 'do not telephone', 'do not contact by mobile phone', 'do not email' or 'do not contact' to the database. Simply deleting the phone number or email address is not sufficient, since the phone number may be re-entered at a future date.

8.2 GOTV scripts

1 We are not permitted to make unsolicited calls for GOTV, therefore it is essential that we only contact those who have supplied consent.

2 However, GOTV only takes place once we have identified a voter's voter id. They have therefore given us their voter identity records. The script used to identify their voter identity record included asking them if they have any objections to the Labour Party contacting them in the future. As such, GOTV only involves calling those who have given consent to be called again.

3 When contacting voters either by phone or in person on the doorstep, in order to secure further contact, the individual must be asked if they have any objections to the Labour Party contacting them in the future. Therefore the GOTV scripts must:

- state that we will use all contact details supplied to contact them

- contain an opt-out which, if taken, must be recorded and adhered to for example 'Do you have any objections to the Party contacting you again in the future?'

4 When contacting on the telephone, in addition to the above, callers must identify themselves and that they are calling from the Labour Party. If asked, they must provide either a valid business address or a freephone telephone number where the Party can be contacted.

5 At any point the voter may terminate the conversation. If they ask not to be contacted again by the party this must be recorded and adhered to by adding a suppression or attribute specifying 'do not telephone', 'do not contact by mobile phone', 'do not email' or 'do not contact' to the database. Simply deleting the phone number or email address is not sufficient, since the phone number may be re-entered at a future date.

9 Non electronic communications

9.1 Petitions

1 All petitions must contain a statement that information supplied to us may be used to contact individuals further. By supplying their contact details, the individual has consented to receiving information on this subject. For example, the statement should read:

2 The Labour Party may contact you using the details you have supplied.

9.2 Surveys

1 All surveys must contain a statement that information supplied to us may be used to contact individuals further. They must be given the opportunity to indicate if they would prefer not to receive information. For example:

2 The Labour Party may contact you using the details you have supplied. If you do not wish to receive information from the Labour Party please tick this box..

9.3 Letters following up on petitions and surveys

1 If someone completes a petition, survey or writes regarding a specific policy, follow-up letters must acknowledge the letter is in response to the petition, survey or policy query. Either within the text, or as a 'PS', you must say that you will update them on this and other issues unless they write to the address given and request not to receive any more information. This must not be in small print.

2 All subsequent letters must contain an opt out option with a valid address for them to use in order to inform us that they do not wish to receive any more information. Examples of opt outs are shown below;

3 1st Letter in response to petition, survey or letter

4 The Labour Party may contact you with further information (on this and other issues). If you would prefer not to receive this information please write to [Joe Bloggs, 12 Station Road, Anytown AN10 1YT]

5 2nd and all subsequent letters

6 If you do not wish to receive further information from the Labour Party, please write to [Joe Bloggs, 12 Station Road, Anytown AN10 1YT]

9.4 Direct mail copy

1 If we are producing direct mail copy for use by local campaigners we must ensure that it contains an 'opt-out' statement. This allows individuals who receive the letter to indicate that they would prefer not to receive any more letters. For example, the statement should read:

2 'I think it's important for me to keep you up to date with local issues but if you would prefer not to receive such information then please let me know at the address above.'

10 Electronic communications (email, SMS etc)

1 We can only contact people electronically who have given their consent. Not objecting to being contacted does not amount to consent, it must be explicit.

2 Petitions, surveys and forms on websites or email, where an individual is invited to provide contact details, must display an opt-in statement that makes it clear that by providing their contact details, they are consenting to receiving further communications from us. For example:

- The Labour Party will contact you using the details you have supplied. If you do not wish to receive information from the Labour Party, please email Unsubscribe or contact [Joe Bloggs, 12 Station Road, Anytown AN10 1YT]

3 In the case of a web page, a tick box option is acceptable.

4 A link to the party's privacy statement must be available on the page where the individual completes their data.

10.2 Emails

1 We can only email an individual where an individual has clearly consented to receive an email from us. The party may not email an individual based on details supplied from a friend or family member. Every bulk email or email response to petitions, surveys and forms must include:

- who it is sent from, either as the sender or in the subject title

- an explicit unsubscribe facility (which must be free to the subscriber, other than cost of transmission)
- a link to the Party's privacy statement
- a valid postal address

2 When emailing groups, addresses must not be visible or accessible to others within that group, therefore we must 'blind copy' to avoid disclosure. In all cases it is preferable to use our dedicated bulk email systems which ensure that email addresses are not revealed to other recipients.

10.3 SMS - text messaging

1 We may only text where an individual has clearly consented to receive a text from us. When supplying details electronically or non-electronically it must be clear to individuals that we will contact them using the details that they have supplied.

2 Pre-advertising of the text message service must state clearly that the party will contact them using the details received, for example 'text us your views and we will keep you posted'.

3 We can only respond to the received text once and this must include:

- our identification as the 'sender'
- a valid postal address (eg LPOrgPOBox000SW1H9HP)
- Where consent is given, any subsequent text messages must include:
- our identification as the 'sender'
- a valid postal address (eg LPOrgPOBox000SW1H9HP)
- an explicit opt out (eg 2UnsubscribeTXT12345) which must be free other than normal network charges.

4 All costs must be clear in pre-advertising. If subsequent replies to/receipt of text messages will cost the subscriber, this must be clearly stated and repeated in all subsequent texts that they receive.

5 Where an individual sends the party a text message and this costs them for example, 25p plus network charges, consent to receive subsequent text messages is not absolutely necessary. Therefore, pre-advertising may say:

- Text us your views. Texts cost 25p

6 However, it is preferable that the following is used:

- Text us your views and we will keep you posted. Texts cost 25p

7 Our initial response to this text must state:

- our identification as the 'sender'
- a valid postal address (eg LPOrgPOBox000SW1H9HP)

8 All subsequent text messages must include:

- our identification as the 'sender'
- a valid postal address (eg LPOrgPOBox000SW1H9HP)
- an explicit opt out (eg 2UnsubscribeTXT12345) which must be free other than normal network charges.

9 All costs must be clear in pre-advertising. If subsequent replies to/receipt of text messages will cost the subscriber, this must be clearly stated and repeated in all subsequent texts that they receive.

10.4 Automated voice calls

1 We are not currently undertaking any automated calling following recent decisions by the Information Commissioner's Office. No future requests to use automated calling will be considered unless prior consent from the persons called has been obtained.

2 Further advice on automated calling is available from the Compliance Unit.

10.5 Member get member

1 There are two types of paper based member get member schemes the party uses:

10.5.2 Details supplied

1 Where an existing member supplies the party directly with a potential member's details, the potential member must be informed by the member that details will be passed to the party and the potential member must be given opportunity to object.

2 When contacted by the party the potential member must be given the opportunity to object to further contact from the party at which point the party may not use their contact details again.

3 The party may only contact the potential member in writing, which should contain a suitable opt out.

4 Members who are passing on details of potential members must be aware, not only of their responsibility under the Data Protection Act, but also that irresponsible disclosure of data may be a disciplinary offence under the rules of the Labour Party.

10.5.3 Details not supplied

1 Where an existing member gives a potential member a form to complete themselves and the potential member returns it to the party.

2 This is basically getting a potential member to complete an application form and it is treated in exactly the same way. If a special form is used is should contain the same data protection statements as a normal application form.

10.6 Ad hoc databases

1 Databases must be held securely and processed regularly to ensure accuracy. Once an individual contacts the database administrator (or relevant person) to ask for their or part of their details to be removed, this must be actioned immediately by flagging their data appropriately. Removing data is not recommended as it may be inadvertently added back into the database leading to unwanted communications being re-established.. Remember to check other systems where the information may be held. We are not permitted to reuse the details unless they are supplied again at a later date and agreement is given. If a complaint is made that data we are holding is not accurate we may be liable for prosecution, for example if we fail to action a request to end contact.

2 No data must be held for longer than is necessary, details such as credit/debit cards may be kept for up to a maximum of five years. You are advised to avoid storing sensitive data such as this unless it is absolutely necessary.

10.7 Opting not to receive further communications (opt outs)

1 Once an individual has informed the database administrator that they no longer wish to receive communications, this must be recorded by suppression or attribute to the database and adhered to. Simply deleting the details is not sufficient.

2 Electronic unsubscribing relates only to email contact unless the individual states otherwise.

3 If details are supplied again at a later date we may resume contact using these details.

10.8 Websites

1 Websites must have the consent of anyone quoted, pictured or referred to. A standard release form is available from the Compliance Unit. Any section that collects supporters details must follow the guidelines above (see above Petitions, surveys and forms on websites)

11 Explanation of terms

Database administrator:

Individual who holds, updates and generally administers a database

Data Controller:

As registered with the Information Commissioner - A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed

Data Processor:

Person who uses data in any form is a data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data Subject:

Natural person

Notify:

Registering with the Office of the Information Commissioner

Process:

Includes obtaining, recording or holding data as well as adapting or altering the data, and carrying out operations on this data. In addition, processing includes the organisation, adaptation or alteration of the information or data, retrieval, consultation or use of the information or data, disclosure of the information or data by transmission, dissemination or otherwise making available, or alignment, combination, blocking, erasure or destruction of the information or data.

Personal data:

Data which relate to a living individual who can be identified (a) from those data or (b) from those data and other information which is in the possession of or is likely to come into the possession of the data controller, and includes any expression or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Identification can be by reference to an identification number or it can be by reference to on eor more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity.

Relevant Filing System:

Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals

or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible

Sensitive data:

Data which may describe

- ethnic/racial information
- religious or other beliefs (e.g. political)
- physical/mental health
- trade union membership
- political opinions
- sexual life
- commission or alleged commission by data subject of any offence, proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

12 Further information from:

The Legal and Governance Unit at

Legal_queries@labour.org.uk or 0207 783 1498