Module 4 – Data Protection

As recruiters you collect, process, manipulate and transfer data about people in the course of your jobs. This means you have to comply with the law about the processing of personal data as set out in the UK Data Protection Act 1998. It doesn't matter whether you are a sole trader with all your participants on a card file index or a multi-national company with thousands of records on a digital database, the Data Protection Act applies to everyone! There is an independent authority in the UK responsible for regulating the Data Protection Act, this is the Information Commissioner's Office, known as the ICO.

In this module we will look at what is in the Act, explain the terms used and the principles in the Act. This guidance will help you understand your obligations and inform you on the kinds of steps you should be taking in order to be compliant with the legislation when you collect and retain personal data about your staff or your participants. It is advisable for you, whatever the size of your business, to have a Data Protection Policy and to keep it updated. If you don't have a Data Protection Policy already, or want to update your existing one, there is information in Module 6, The Recruiter Toolkit, on how to make one for your business.

The information contained in these modules is not legal advice. It aims to give awareness of the Data Protection Act 1998 with specific reference to market and social qualitative research recruiters, to highlight significant areas and illustrate industry best practice. For specific queries you are advised to seek advice from the Market Research Society (MRS), the ICO or obtain independent legal advice. Useful websites and telephone numbers can be found at the end of this module.

Direct quotations from the Data Protection Act are in italics.

The Data Protection Act 1998

The Data Protection Act 1998 is an Act of Parliament which defines UK law on the processing of personal data on identifiable living people. The Data Protection Act controls how personal information is used by organisations, businesses or the government.

There is a new EU regulation on data protection coming into force in May 2018. This is the European Union General Data Protection Regulation (EU GDPR). The UK will still be part of the EU at this time and will have to comply with this regulation. The exact implications of this for research are being determined by the MRS in consultation with the ICO. The Fair Data website has guidance on what you can do now to prepare for the EU GDPR www.fairdata.org.uk The MRS will also keep their website updated with advice www.mrs.org.uk

Key Definitions used in the Data Protection Act

Before we go through the principles and rules which govern the collection and retention of personal data it is useful to understand the terms that are used in the Act.

These terms refer to the people who obtain the data and to those whom the data is about:

Data Controller - *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. The Data Controller is required to take appropriate steps, both technical and organisational, to protect personal data from accidental or unlawful destruction or accidental loss, alteration or disclosure.*

You are the data controller if you collect and/or keep identifiable data on participants including, but not exclusively, names, email addresses, telephone numbers and determine the purposes for which and the manner in which personal data is processed.

The Data Protection Act 1998 requires every data controller (e.g. organisation, sole trader) who is processing personal information to register with the ICO, unless they are exempt. Recruiters are not exempt from registration. Registration can be completed online via: https://ico.org.uk/for-organisations/register . It is very straightforward and costs £35 per year (correct at June 2016.)

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.*

For instance you would be the data processor if you were recruiting from a client database/customer list and were not gathering or using any client data for your own purposes.

Data Subject - *means a living individual who is the subject of personal data.*

For market and social research purposes this is anybody who is identifiable from data which you hold irrespective of whether individuals have participated in research or not. Any employees that you have will also be data subjects under the Act as you will hold identifiable personal data about them.

These terms refer to how you store and process data:

Data (information on an individual is data under the Data Protection Act if any of the following apply):

(a) it is being processed by means of equipment operating automatically in response to instructions given for that purpose,

For instance databases where you can generate lists of participants to contact.

(b) is recorded with the intention that it should be processed by means of such equipment,

For instance collecting information on the street which is later entered on to a computer.

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

A relevant filing system means 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.

For instance a list of participants organised by their biographical and/or social geodemographic details - age, sex, occupations, health conditions etc.

Processing - *in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—*

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

These terms refer to the nature of the data held:

Personal Data - *means 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 of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

For you as a recruiter this means all the day-to-day data that might be held on a database (digital or paper) or sent on profiles to clients e.g. participant names, addresses, telephone numbers, email addresses, customer numbers, plus any other data which might identify individuals and this would include opinions you have noted down about the participant.

Sensitive Personal Data - *in this Act "sensitive personal data" means personal data consisting of information as to—*

(a) the racial or ethnic origin of the data subject,

(b) his/her political opinions,

(c) his/her religious beliefs or other beliefs of a similar nature,

(d) whether he/she is a member of a trade union,

(e) his/her physical or mental health or condition,

(f) his/her sexual life,

(g) the commission or alleged commission by him/her of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act does not include financial data within the legal definition of sensitive personal data. However, personal financial details will be perceived as sensitive data by individuals as well as being high risk data which is vulnerable to illegal activities such as identity fraud. As such financial data must be collected sensitively and processed and handled confidentially and securely.

The rules for using personal data in the Data Protection Act 1998

The Act has eight principles whose purpose is to protect the interests of the individuals whose personal data is being processed and not to cause them any harm.

1. *Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.*
   You should always recruit participants on the basis of getting their informed consent to take part in the research. A full description of informed consent is given further on.
2. *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.*
   For instance if you are using personal data from a client supplied list you cannot use the data for any other purpose, such as adding to your own database or creating lists of participants for use elsewhere.
3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
   For instance a client cannot ask you to gather information that is not relevant to the current project just in case they may need it later.
4. *Personal data shall be accurate and, where necessary, kept up to date.*
   This principle sounds straightforward enough but the law does recognise that it may not be practical to double-check the accuracy of every item of personal data that you receive. To be compliant with this principle consider the following four steps: have you taken reasonable steps to make sure that the personal data you receive is accurate; do you know where the personal data has been sourced from; could anyone challenge the accuracy of the information; is it necessary to update the information?
5. *Personal data shall not be kept for longer than is necessary for that purpose or those purposes.*
   There is no specific minimum or maximum length of time stated in the Act but it is advisable to establish your own standard retention time. Data should be securely deleted if it is out of date or no longer required.
6. *Personal data shall be processed in accordance with the rights of data subjects under the Act.*
   It is a requirement to have a contract in place with your client on how the data will be used. The data subject has the right to see what information is held about them.
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*
   If you have a data security breach it may cause embarrassment to a participant or real harm such as identity theft. Make sure that you and/or company has a culture of data security and that staff and/or suppliers who have access to data are trained in data protection.
8. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*
   Before you start working for an overseas client on a project involving EU nationals you need to check what personal data you are allowed to transfer to them. This applies even if the

research is taking place within the EU/EEA. This is a complicated area so please refer to the MRS or ICO or get independent legal advice for specific projects. You can find the list of EU/EEA members via: https://www.gov.uk/**eu-eea**

Informed Consent

For recruiters the first two principles of the Data Protection Act are primarily about getting informed consent from research participants. You need to be transparent during recruitment ensuring that individuals approached to participate in research have a clear and unambiguous understanding of the purpose(s) for collecting the data and how it will be used. At the time that the data is collected, individuals must give their consent to their data being collected, for what purpose and also at this time, have the opportunity to opt out of any subsequent uses of the data. Consent should be recorded in a verifiable format. Data collected should only then be used in accordance with the permissions gained during data collection.

You should always have the following information from clients so that a participant can decide whether they want to take part in the research:

The purpose of the recruitment
The location, time and duration of the activity
The type of client research e.g. group, depth, paired depth, in-home interview etc
The monitoring, observation or recording arrangements
The incentives and how and when they will be paid
Any other activity involved in the research eg pre- or post-task
Any re-contact arrangements which can be for the purposes of that project only
You must not disclose the identity of a client or any confidential information about a client without the client's permission, unless there is a legal obligation to do so. However, if you are recruiting from a file of identifiable individuals e.g. a client database/list then the source of the personal data must be revealed at an appropriate point, if requested by participants. This overrides the right to client anonymity.

Recording Calls

It is legal to record calls as long as certain criteria are met. Where you are able to identify either party involved in the call you must do the following: inform the other party that recording is planned and how the recording will be used; obtain their permission for the call to be recorded; and ensure that any recorded participant data is kept in a secure location and is retrievable and accessible if requested by a data subject.

A schedule for deleting recorded calls should be part of your data security procedures.

Client Supplied Databases/Customer Lists

If you are working from a sample provided by a client (also called client supplied databases or client customer lists) there are other considerations that need to be taken into account.

In this situation the clients will be the data controller and the recruiter will usually be the data processor. There must be a written contract with the client that all people on the client database have consented to being contacted e.g. any individuals that have requested not to be contacted for research purposes are excluded from the list. The data controller - the client in this instance - is

responsible for ensuring that recruiters use the data in accordance with the terms under which it was collected. You may be required to sign a legal contract with the client often called a "Sub-processor Data Handling Contract". Recruiters must also ensure that client supplied data is retained and stored securely. The data controller - clients which supply customer lists - must be registered with the ICO and within client notifications it must state that customer data will be used for research purposes. Information on registered data controllers is publicly available on the ICO website.

The Data Protection Act does not specify a length of time to keep data. Principle 5 states that it *"shall not be kept longer than is necessary for that purpose or those purposes".* As part of the contract between the data controller and the data processor it is advisable that a timescale for keeping any database/list is specified and adhered to. Once the list is no longer required it should be securely deleted.

Only data that is necessary for the project must be collected during recruitment. The client is not allowed to collect extra data just in case they need it at some future point. The participant should be advised that they will not be contacted for any other reason than for the purpose of that particular research project.

As you call through a list you should annotate it after each call. Clients are not allowed to use market and social research recruitment as an opportunity to update their records. In practice this means that you should record information relevant to the call but not expand upon it. For instance you should record if you find out that someone has died; if someone has moved house you should record "no longer at this address" but you cannot provide details of the new address. It is the responsibility of data controllers to collect up-to-date customer information, using any data screening protocols which they may have in place.

Clients can request that you report details of specific complaints or dissatisfactions for investigation. Participants must first give consent for feedback to be passed to the client before the information can be given to the client.

It is advisable that you have a standard list of annotations that you can use on a list and always keep to that format e.g. not at this address, declined to be interviewed, interviewed but didn't fit criteria, no answer, telephone number not recognised, recruited etc. Then the list can easily be sorted and the client updated with how many people have been contacted and what the results of that contact were. You cannot give clients the individual names of people who have refused to participate or didn't fit the criteria for a project. You can only give the numbers e.g. - 10 not at this address, 9 declined to be interviewed, 8 didn't fit the criteria etc.

You cannot retain any data for your own use e.g. adding client customer names to your own database.

Client databases can contain very sensitive information so always make sure that you identify the person you are talking to. It is advisable not to leave messages that can be picked up by others e.g. "Message for Sue. If you are interested in doing market research about your Swiss bank account please ring this number".

Children

When you recruit children there are special requirements. Children are classed as individuals under 16 years of age. Young people are aged 16 and 17. The consent of a parent, or responsible adult (in loco parentis), must be obtained before speaking to or interviewing a child. Parents, or responsible adults, must be given sufficient information about the nature of any research project to enable them

to provide informed consent for their child to be interviewed and to take part in the research. The child or young person must have their own opportunity to decline to take part in the research. Parents, or responsible adults, must also be fully informed of any products or stimulus material which the child may be asked to try or use. Verifiable consent must be given by parents/the responsible adults before any research takes place. A parental consent form will usually be supplied by a researcher to be signed before any research takes place. If the research is to be conducted without parents/responsible adults being present then this should be part of the instruction at the time consent is gathered from the responsible adults.

It is illegal to conduct research on behalf of manufacturers, or providers of products or services, where the product or service is illegal for the age group involved in the research e.g. buying alcohol for under 18s or gambling for under 16s.

Subject Access Requests

All data subjects have the right of access to the personal data that you hold about them. They are entitled to the following information: whether any personal data is being processed; a description of the personal data; the reasons it is being processed; whether it will be given to any other organisation or people; and finally the source of the data. They have a right to copies of all personal data that is held by the data controller e.g. a printout of their database account or copies of any email correspondence. It is an offence to deliberately edit or destroy any of these once a subject access request has been received. Be aware that personal data is not just referring to the data subject's biographical data but also refers to any opinions that you may have recorded.

The data subject must make a subject access request in writing for it to be valid – this includes letters, email and also social media. If the data subject is physically unable to make the request in writing then an exception can be made to accept a verbal request under the Disability Discrimination Act 1995. Even if the data subject does not explicitly mention the Data Protection Act you must still treat their request as a valid claim if it is clear they are asking for their personal data.

Once a request has been made you have up to forty days to respond and fulfil the request. You need to be certain that the data subject is who they say they are and you can ask for further proof of identity. If the request has come through social media it is advisable to always verify their identity by other means. You can charge the data subject up to £10 for providing the information. A data subject can make as many requests as they wish but data controllers are not obliged to comply with similar or identical requests made by the same data subject. The information that you provide should be in an "intelligible form" and any codes that you use should be reversed so the information can be understood by the average person. If a data subject is disabled the information has to be sent in an appropriate format e.g. large print, email, audio format or Braille.

If a subject access request has come from a person on a client supplied database or list clients should be notified. By providing the data in an "intelligible form" you need to be mindful if that means sharing the questions used to collect the personal data, and therefore disclosing the intellectual property of the client, if that is the case, then the client should also be consulted.

Transferring Data

As a recruiter you will transfer data to and from clients and care has to be taken to keep this data secure. It is best practice to transfer the least amount of data so that if a data security breach occurs the minimum amount of information is at risk of being accessed or used by unauthorised persons.

Data being sent to you from clients, such as a client database, should be sent to you encrypted and any passwords sent in a separate email or another mode of communication. Any personal data or sensitive personal data should be sent encrypted.

When you are transferring personal data to a client you should use a method that has adequate security measures e.g. file transfer protocols (FTP). Well known websites such as MailBigFile or Dropbox are normally not suitable for the transfer of personal data and data transferred this way may mean that the data is transferred outside the EU/EEA.

Some companies may require you to use their own file transfer protocol system.

It is the client's responsibility to transfer personal data to venues if they have booked the venue. It is also the client's responsibility to ensure that they have an agreement with the venue to ensure that data is collected, processed and retained in accordance with the Data Protection Act and that the data will only be used for the purpose it is intended.

The transfer of personal data outside the EU or EEA has very specific requirements and it is advisable to make sure that you are allowed to transfer the personal data of EU nationals before you take on a project for a client outside these areas. This applies even if the research itself takes place in the UK.

Data recording, security, storage and destruction

This includes paper, digital, audio or visual recordings.

The Data Protection Act was written to be technology neutral and doesn't specify the use of any particular technologies as these frequently change. Principle 7 states that *"appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data"*

You should have a Data Protection Policy which lists procedures about data recording and security, your organisational security, physical security and computer security. All staff, part-time and casual workers included, must be trained on data security at induction and refresher training should be completed at least annually. Advice on how to draft a Data Protection Policy is in Module 6, The Recruiter Toolkit.

Data Security Breaches

We've all heard of big companies losing data or being subject to a cyber-attack, but it can happen to anyone. A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.

A data security breach can happen for many reasons: loss or theft of equipment on which data is stored, unauthorised use of data, equipment failure, human error, fires or floods in a building, hacking attacks or 'blagging' offences where personal data is obtained by deception.

If a data security breach has occurred, or you think it has occurred, you need to consider the following four steps:

1. Containment and recovery

Review what has happened and stop it getting any worse. Depending on the nature of the breach you may need assistance from a specialist such as an IT professional, HR or independent legal advice.

2. Assessing the risks

Once you have contained the breach you need to assess what is the likely outcome of the situation. Analyse the data that has been compromised. How useful would it be to a third party, could they use it for identity theft?

3. Notification of data security breaches

You need to consider whether any regulatory body should be notified and whether any individuals whose data has been compromised should be notified and by what method. Third parties such as police, insurers, professional bodies, bank or credit card companies might also need to be informed. If a client's list is involved you must inform your client.

4. Evaluation and response

Once you are satisfied that you have taken all the steps to contain the data security breach and notified the necessary people you will need to review your policies and procedures and organise any staff training.

Summary

Thank you for taking the time to read this module on Data Protection and we hope that you have found it informative and useful. There will soon be a short test on the module with more details coming soon.

Useful addresses

The Market Research Society (MRS) www.mrs.org.uk

The complete Data Protection Act 1998 can be found at www.gov.uk/data-protection/the-data-protection-act

The Information Commissioner's Office (ICO) www.ico.org.uk