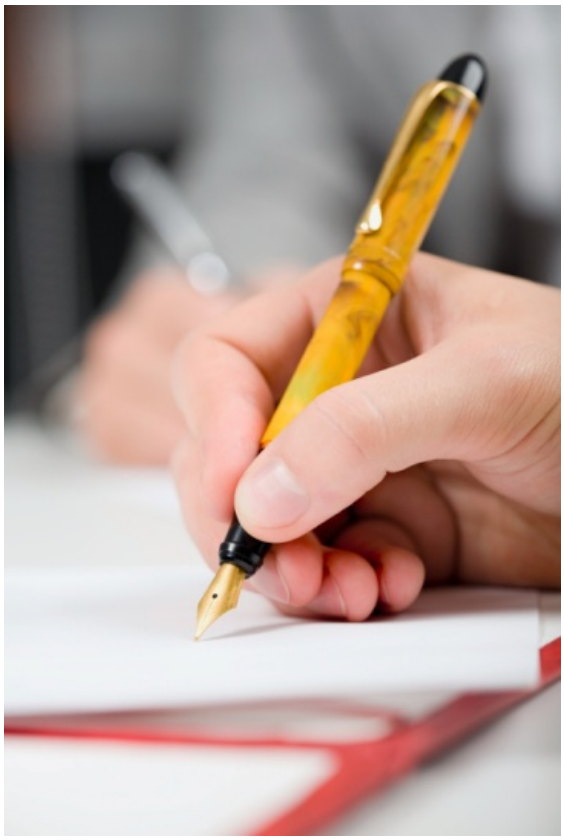
DATA PROTECTION ACT

A guidance note for advocacy providers



action for advocacy

irwinmitchell solicitors

ISP IMCA Support Project

Contents

Introduction

The area of data protection is relevant across the advocacy sector, not just IMCA but the premise of this guidance came from the IMCA sector and questions they were often faced with from external agencies. Unlike other types of advocacy, the IMCA service is the only one that is required by law to submit their findings to an external body, their findings being the advocacy work they have carried out. This raised many issues with respect to responsibilities within data protection. However other advocacy schemes not providing IMCA but seeking clarity on data protection issues led us to consider that this was an area of need for the sector in terms of a resource that provided information specific to advocacy. We have worked with Irwin Mitchell law firm to devise a fact sheet, which gives information and guidance about advocacy providers' responsibilities under the Data Protection Act.

The issues are particularly relevant to the IMCA report as family members become aware of the IMCA role, requests for a copy of the IMCA report are becoming more frequent and consequently IMCAs need to be aware of their responsibilities and the rights of other people under this Act. The guidance makes it clear that IMCAs are considered data controllers and therefore have responsibilities in relation to the disclosure of data, including the report.

The guidance also provides clarity on issues of security, transfer of contracts, requests from the person or their representative for information that advocacy providers hold on them as well as information for advocacy providers who work within organisations that have many services, not just advocacy.

We've included a checklist to go with the factsheet, which will guide advocates through the process should a request for disclosure of data be received from either the client or their representative. We hope this will be a useful tool for advocacy providers to use and thank you to Irwin Mitchell for devising the guidance based on the questions which are regularly posed to A4A.

Jakki Cowley & Sue Lee

IMCA Support Project Managers

July 2011

Background

In the United Kingdom, the way in which **personal data** is used is governed by the **Data Protection Act 1998 (DPA)** which is based on European legislation. The **DPA** is enforced by the **Information Commissioner's Office**. All organisations using or storing **personal data** need to be aware of their obligations under the **DPA**.

What is Personal Data?

The **DPA** regulates the processing of **personal data.** This is information about an identifiable living individual (the **data subject**), and includes expressions of opinion about that individual as well as more "obvious" personal data, such as information about the individual's name, address, date of birth and so on. Essentially, if information is "obviously about" a living individual, or impacts on their privacy in some way then it is likely to be caught by the **DPA**.

One caveat to this is that, outside the public sector, **personal data** only includes information which is recorded electronically or in structured filing systems. If the only records maintained are paper files, which are in date order, they may not be caught by the requirements of the **DPA** (although if you are holding such files on behalf of a public authority they may be caught – and in any event, compliance with the **DPA** can be seen as a matter of good practice and can help you comply with confidentiality obligations whether or not it is strictly required).

There are two types of **personal data –** "normal" **personal data** and **sensitive personal data**. **Sensitive personal data** is **personal data** which consists of information as to:

- The racial or ethnic origin of the data subject
- His political opinions
- His religious beliefs or other beliefs of a similar nature
- Whether he is a member of a trade union
- His physical or mental health or condition
- His sexual life
- The commission or alleged commission by him of any offence
- Any proceedings for any offence committed or alleged to have been committed by him, including any sentence in such proceedings

Given the nature of the work carried out by advocates, it is highly likely that **sensitive personal data** will be collected and used. **Sensitive personal data** attracts a higher level of protection under the **DPA**.

Who is responsible for compliance with the DPA?

The **DPA** distinguishes between **data controllers** and **data processors**. The **data controller** is legally responsible for compliance with the **DPA**, but may engage **data processors** to process **personal data** for it.

The **data controller** is the organisation which determines the purposes for which the **personal data** is processed. A **data processor** processes **personal data** on the instructions of the **data controller** but does not do anything with the **personal data** on its own account. It is possible for two organisations to be **joint data controllers** if they both have a say in how the **personal data** is used.

It is important to note that the **data controller** is the organisation rather than a specific individual within the organisation. Whilst you may have an individual who is responsible for overseeing data protection compliance (who may be referred to as the data controller, but is more correctly called a data protection officer), it is the company as a whole rather than that individual who is legally responsible for the data.

Example: X is employed by Y Ltd. Although X needs to comply with data protection rules in the course of his/her duties, any enforcement action would be taken against Y Ltd. Y Ltd is the data controller.

It is likely that advocacy organisations will be **data controllers** in respect of almost all of the **personal data** which they process, although in some situations, if they are carrying out work dictated by a third party and do not use the **personal data** for their own purposes they may also be **data processors** for the third party. However, this is only likely to be the case in very limited circumstances where the activities of the advocate are entirely dictated by the third party and due to the independence of the advocate it is unlikely to happen.

This guidance note focuses on data protection compliance in relation to client files and IMCA Reports, but it is important to remember that the advocacy organisation will also

be a **data controller** in relation to information about its employees, and this must also be processed in accordance with the **DPA**.

What are the requirements of the DPA?

The **DPA** sets out eight **data protection principles** which **data controllers** must comply with at all times when processing **personal data**.

1. **Personal data** must be fairly and lawfully processed
2. **Personal data** must be processed for limited purposes
3. **Personal data** must be adequate, relevant and not excessive
4. **Personal data** must be accurate and up to date
5. **Personal data** must not be kept for longer than is necessary
6. **Personal data** must be processed in line with the data subjects' rights
7. **Personal data** must be secure
8. **Personal data** must not be transferred outside the EEA without adequate protection

These **data protection principles** will be considered in more detail later in this guidance note.

In addition, the **DPA** imposes a requirement on **data controllers** to register with the **Information Commissioner's Office** unless they only process **personal data** for a limited number of "core business purposes" such as staff administration and accounts and records.

Fair and Lawful Processing

The **first data protection principle** requires all **personal data** to be fairly and lawfully processed. This includes the following requirements:

- Data must be obtained fairly and lawfully – you should not deceive or mislead anyone about the purposes for which you will use data.
- You must give the **data subject** information about who you are and how you will use their **personal data** – this information is often known as a privacy statement or privacy policy. Advocates should provide this information as part

of explaining their role – an oral explanation could be backed up with a written document made available on request.

- You may find it useful to update **data subjects** on an ongoing basis about what information you hold as part of the service you provide – for example sharing correspondence.
- You must have a "condition for processing". The conditions which can be used differ depending on whether you are processing **sensitive personal data** or normal **personal data**.

Conditions for Processing

It is often thought that the consent of the **data subject** is required in order for **personal data** to be processed. Whilst this is one of the conditions for processing set out in the **DPA** it is not the only one, and due to the nature of work carried out by advocacy organisations it is likely that an alternative condition for processing will be required if the **data subject** is not capable of giving informed consent and there is no-one who is able to give consent on the **data subject's** behalf. Where consent can be given it is preferable to get it, but advocacy organisations will need to be aware of the other potential conditions for processing.

For statutory advocacy schemes, processing will be permitted because processing in accordance with a statutory obligation or scheme fulfils a condition for processing. However, this only applies to the extent that the data is used in relation to the statutory scheme – any other use of the data would need an alternative condition for processing.

Where consent cannot be obtained, and there is no statutory basis for the advocacy, the following conditions for processing may be relevant:

- Where the **personal data** is NOT **sensitive personal data**, the following may apply:
  - The processing is necessary in order to protect the vital interests of the **data subject**;
  - The processing is necessary for the purposes of legitimate interests pursued by the **data controller** or any third party, and there is no unwarranted prejudice to the rights, freedoms or legitimate interests of the **data subject.**

- Where the **personal data** is **sensitive personal data**, the following may apply:
    - The processing is necessary in order to protect the vital interests of the **data subject** or another person in a case where consent cannot be given by or on behalf of the **data subject** or the **data controller** cannot reasonably be expected to obtain consent. For example, if the **data subject** needs urgent medical treatment and you know about an existing medical condition, you would not breach the **DPA** by letting the doctors know, even if it is outside the scope of your normal role as an advocate.

What are the rights of data subjects?

The **sixth data protection principle** requires you to process information in accordance with the data subjects' rights. These rights are set out elsewhere in the **DPA** and include the following rights:

- The right to access **personal data** – this is commonly known as a data subject access request. A **data subject** (or their representative) is entitled to be told what data is processed about them, the purposes for that processing, and the identities of any third parties to whom the data is disclosed. The data subject is also entitled to a copy of the data in permanent form.

It is important to note that there is no specific form of this request, so any request by an individual for information about themselves may fall within the **DPA** provisions.

There is a 40 day time limit for the provision of information, and it is possible to make a charge of up to £10.

There are a number of situations in which data does not need to be disclosed, for example if it contains information about other individuals.

It is recommended that organisations have a subject access policy and nominate an individual to be the main point of contact for these requests.

- The right to prevent processing likely to cause damage or distress. Where an individual feels that the use of **personal data** may cause unwarranted and substantial damage or distress to himself or a third party he may request that processing is stopped. Again, there are a number of exceptions. If the request is not complied with, and none of the exceptions applies, the individual may apply to court.
- The right to prevent processing for the purposes of direct marketing.

- Rights in relation to automated decision taking – essentially where a decision is taken by automated means, the individual can require the **data controller** to reconsider the decision without using the automated processes.
- The right to require inaccurate personal data to be rectified, blocked, erased or destroyed. The **data subject** may apply to court to exercise this right. This means that if a **data subject** (or their representative) disagrees with information you hold on them they may ask you to delete it – or include a statement setting out their view.

What are the consequences of a breach of the DPA?

There are three main consequences of a DPA breach:

- The most important is that you could be the subject of an investigation by the **Information Commissioner's Office**. If you are found to be in breach of the **DPA** you can be asked to sign undertakings which set out a commitment to revise practices and take specific steps to ensure that breaches do not happen in the future. For more serious breaches, particularly those relating to large amounts of **personal data** or which relate to **sensitive personal data**, the **Information Commissioner's Office** can also impose financial penalties of up to £500,000. In the past fines have been issued even where lost data has not been entirely the **data controller's** fault – for example organisations have been fined where unencrypted laptops have been stolen, because even though they could not have prevented the theft they could have encrypted the laptop to ensure that the data on it was not accessed.
- It is also possible for **data subjects** to claim compensation where they have suffered loss or damage as a result of the breach. It is not sufficient for them to merely have suffered distress, which means that in practice claims for compensation are relatively rare, but not impossible. For example, if you disclose **personal data** when you should not and this means that a **data subject** suffers loss – which could include things like losses arising from identity theft, or being put to additional expense, they may be able to ask you to compensate them for that loss.
- Finally, any action taken by the **Information Commissioner's Office** is a matter of public record and data breaches are often reported in the media which can affect the reputation of the **data controller**.

Specific Data Protection issues and questions

How long should information about clients be kept for?

There is no fixed timescale in the **DPA** although the **fifth data protection principle** says that **personal data** must not be kept for longer than is necessary. What is necessary will depend on the circumstances, including the following:

- How long the information is required in order to provide the services requested
- Any contractual obligations to retain data
- Any statutory or regulatory obligations to retain data – for example agreements with a funder
- Any period after the provision of services where you may be subject to complaints or legal action in respect of the services carried out
- Any requirement to retain data for accounting or tax purposes

Best practice is to have a policy in place taking account of the organisation's need to retain data. You should review the information you keep on a regular basis and delete information which is no longer required.

What security measures do we need to take?

The **seventh data protection principle** requires organisations to take appropriate technical and organisational security measures to protect the data. What is appropriate will depend on the nature of the data and the harm which could be caused if it is lost or stolen. **Sensitive personal data** will usually require a higher level of security.

Although the **DPA** itself does not set out specific security measures, the **Information Commissioner's Office** has taken enforcement action against organisations who have lost data, and these decisions indicate that the following security measures should be considered:

- Password protection is important to control access either to the system as a whole or to individual client files or databases;
- Encryption of laptops and portable storage media. Password protection alone is **not** considered to be sufficient for portable computer equipment;

- Where **sensitive personal data** is to be transmitted (for example by email or fax) there should be adequate security measures which could include sign off by a senior member of staff, phoning to confirm receipt, and verification of fax numbers/email addresses.
- It is preferable to store all **personal data** on a central server rather than on local drives – access should preferably be by way of a VPN. Where **personal data** does need to be stored locally (for example an employee needs to work on it in a location with no internet access), only the data required should be saved onto the local drive, and it should be deleted once no longer required.
- Records which are no longer needed should be deleted.
- It is sensible to have a written plan which sets out your security measures and also what steps you would take in the event of an emergency – for example back ups.

Can client records be kept at home?

It is not recommended that client records are routinely stored at home. However, if they are needed and appropriate security measures are taken this can be done. For example, only the files which are needed should be removed from the office, and it may only be necessary to take part of the file. Care should be taken of the files – for example it may be appropriate to keep them with you rather than leaving them unattended in cars, and care should be taken to ensure that they are not lost.

Can we use cloud computing?

It is becoming increasingly common to use internet services which allow you to store data "in the cloud" and access it from any device from any location. From a data protection point of view, this causes problems and is not recommended particularly where you are dealing with **sensitive personal data**.

If you do want to use cloud storage, you should consider the following points:

- The cloud provider will be your **data processor** and you will need to ensure that there is a contract in place which contains adequate security provisions in order to comply with the **seventh data protection principle**.
- You should check that the cloud provider does not use servers outside the EEA for the storage of your data, as this may cause problems under the

eighth data protection principle unless there is an adequate level of protection for personal data in place.

- You should consider whether the service is sufficiently secure against hacking to be suitable for the storage of personal data. As the **data controller** you will remain legally responsible for the data if it is accessed by third parties.
- If you use cloud storage for temporary access to documents while on the move, you should ensure that it is not used for long term storage.

Can we use case records elsewhere in our organisation?

For example, if we have a housing service or another advocacy service? Even if the data is being used within the same organisation and not being transferred to a third party, if it will be used for a different purpose there are still restrictions under the **DPA**. The **second data protection principle** states that **personal data** should only be used for the purposes for which it is collected. In addition, the **first data protection principle** requires you to tell **data subjects** about how their information will be used and obtain consent or ensure there is another condition for processing.

If you have told the **data subject** that you will use their **personal data** for this purpose and they are happy with this, you are likely to be able to share it with other services within the organisation. However, it may not be appropriate to share all the information you hold – it may be possible to make a referral with more limited information than you hold for the purposes of advocacy.

If you do not have consent, you will need to be satisfied that another **condition for processing** applies. If the referral does not contain **sensitive personal data** and is in the **data subject's legitimate interests** it may be permitted, but care needs to be taken and you should always be open about who the data will be shared with.

What if we lose a contract and it is awarded to another service?

For example, what happens to case file? Generally speaking, if a "business" is transferred from one organisation to another and the information will be used for the same purposes before the transfer as afterwards, there is unlikely to be a breach of the **DPA** in transferring the personal data used by the business. Some safeguards need to be complied with, for example informing **data subjects** that the transfer has taken place and ensuring that any conditions for processing remain. However, where the only change is the identity of the **data controller** rather than the way in which the

personal data is used, the transfer is likely to be permitted. There is no requirement to obtain consent, although if an individual is not happy with the transfer their views should be taken into account.

However, this does not mean that there is necessarily an obligation to transfer files. If you have concerns you would be entitled to retain them until you are comfortable with how they will be used after the transfer.

How does the DPA apply to rough notes and paper files?

Strictly speaking the **DPA** only applies to information held on a computer and would not apply to rough notes. However, due to the cross over with confidentiality, and the fact that files will usually contain hard copies of information which is also stored on a computer, the safest approach is to treat them with the same degree of care as you treat electronic information, particularly when looking at security requirements and who information can be disclosed to.

However, if you receive a data subject access request it is permissible to remove hand written notes before disclosing case files as these are not covered by the rights of access to information.

Who owns the data we hold?

Talking about ownership of data can be misleading as there are a number of rights in data which may have different considerations.

For example, it is possible for two organisations to have copies of exactly the same data, but to use it for different purposes. In this situation each organisation will be a **data controller** in respect of the data and responsible for compliance with the **DPA**.

Example: multiple organisations are likely to have the name and address of a data subject. Although the information held is identical, the information will be used for different purposes by each organisation, and each is responsible for its own use of the data. The same principle applies for more complex personal data – more than one organisation may have a case file on the same data subject, and some information may be held on both files. Each organisation is independently responsible for its own file.

In addition, any **personal data** is held subject to the rights of the **data subject**. The **DPA** is drafted on the basis that a **data subject** can ask for his or her **personal data** not to be used in certain ways, and the **data controller** may need to ask for the **data subject**'s consent. Therefore, the **data controller** does not have a free rein to use the **personal data** for any purpose it wants.

How should we deal with requests for personal data?

Where the request is made by or on behalf of the **data subject** you will almost always need to disclose the **data subject's personal data** under **s7 DPA** (a data subject access request).

- A **data subject** (or their representative) is entitled to be told what data is processed about them, the purposes for that processing, and the identities of any third parties to whom the data is disclosed.
- Where a request is made by a representative you need to be comfortable that they have authority to act on behalf of the **data subject** – either because the **data subject** has given them authority (either through a 'form of authority' if they have capacity or through a lasting power of attorney) or because the court has done so (through appointing a deputy). Relatives will not automatically be able to act on behalf of the **data subject** unless they have the appropriate authority.
- The data subject is also entitled to a copy of the data in permanent form**.**
- The request does not need to be in any specific form of writing but does need to be made in writing e.g. letter or email.
- You are entitled to charge up to £10 (although you do not have to do so).
- There is a 40 day time limit for the provision of information which runs from the day of receipt of the information required to confirm the individual's identity and information sought (if required) and the fee (if requested). You should not delay asking for further information or a fee.
- You should not disclose information about third parties unless you have consent, or it is reasonable to disclose the information without consent. If this is not possible, you may need to edit the information before disclosing it to the **data subject**. This may be the case if the information you hold about the **data subject** also contains information about third parties they come into contact with. It is likely to be reasonable to disclose the names of individuals such as social workers, but it may not be reasonable if you hold information which the third parties would not want to be disclosed to the **data subject**.

- The right is to access **personal data** rather than the documents it is contained in. It may therefore be possible to edit documents to remove non-personal data. However, unless there is a good reason for doing so (such as to protect third parties or in relation to medical information not known to the data subject) it is usually preferable to disclose full copies.
- Some medical information is subject to specific rules. Where disclosure involves medical information which is not already known to the data subject you should consult with an appropriate medical professional as to whether it is appropriate to disclose. If the medical professional decides that it is not, for example because it would be detrimental to the **data subject's** physical or mental health you may not be required to provide the information. You may need to take specific advice on this. In addition, if the request is made on behalf of the **data subject** (for example by someone appointed by the court to act on their behalf), you should not disclose medical information which was provided in the expectation that it would not be disclosed, or which the **data subject** has asked not to be disclosed. Again, specific advice may be required.
- Advocacy organisations should have procedures to deal with subject access requests, including knowing who is responsible for compliance and procedures to ensure that they are dealt with within the statutory timescale.

Where a request is made by a third party there is no obligation to disclose the **personal data** under the **DPA** (although other statutory obligations may impose a requirement – if so, disclosure will be permitted).

However, there are a number of situations in which a disclosure will not breach the **DPA**. You do not have to disclose, but if you choose to you will be protected. For example:

- Requests for data to be used in legal proceedings will often quote **s35 DPA**. In order for disclosure to be permitted you must be comfortable that the disclosure is necessary for that purpose.
- **s35 DPA** also allows you to disclose information which is required by law – for example if there is a court order or statutory obligation requiring you to disclose it.
- Requests from the police or other law enforcement authorities will usually be on a **s29 Form** or quote **s29 DPA**. If they do not, you should clarify whether

the request is made under **s29** which permits disclosures which are necessary for the prevention and investigation of crime and the apprehension of offenders.

Disclosure of IMCA Reports

IMCA Reports will inevitably contain personal data and will be shared with third parties.

Where the report is created as part of a statutory advocacy role, the advocacy organisation will be required to submit its findings to the local authority or NHS body. Because this disclosure is required by law, it is permitted under the **DPA**.

It is important to remember that the advocacy organisation is a **data controller** for IMCA Reports. Where a copy of a report is submitted to the local authority or NHS, that body will hold a copy of the report. To the extent that it uses it for its own purposes in making decisions about the **data subject**, it will then also become a **data controller** for IMCA Reports but its ability to use the report for purposes other than making the relevant decision will be limited. Therefore the report can only be shared within the responsible body (to colleagues) OR with those not working within the responsible body but who have decision making responsibilities for this specific decision (for example a learning disability partnership will be made up of NHS and Local Authority staff but they are all working on the decision at hand). However, because the report has been obtained under a statutory scheme, it should not be used for any other purposes and must be used in accordance with statutory restrictions.

It is possible that the responsible body will receive requests for data it holds. The responsible body is under a legal obligation to respond to the request where **s7 DPA** applies.

If any other person or organisation requests a copy of the report, from the IMCA provider, the advocacy organisation will need to ensure that any disclosure is in accordance with the **DPA**.

For example:

- Disclosure to the **data subject** will be permitted (subject access request).
- Disclosure to the **data subject's** authorised representative will be permitted (subject access request).
- Disclosures made with the **data subject's** consent are permitted.
- Disclosure for use in legal proceedings will be permitted if the disclosure is necessary for those proceedings.
- Disclosure to the police will be necessary if the disclosure is necessary for the investigation of crime and/or the apprehension of offenders.
- Disclosure is likely to be permitted if it is necessary in order to protect the **data subject**'s vital interests.
- Disclosure of non-sensitive **personal data** is likely to be permitted if it is in the legitimate interests of the advocacy organisation, the **data subject** or any third party and does not unduly prejudice the **data subject**. This would not permit disclosure of **sensitive personal data**.
- Any disclosure should also be in accordance with the MCA Code of Practice. For example, if information is requested in relation to a specific decision, information provided should be limited to that which is needed to make the decision.

This is not an exhaustive list and each disclosure will need to be considered individually. However, the following situations may arise:

If family or friends of the person request a copy of the report

If they have appropriate authority this may be a subject access request. In other situations the IMCA provider would need to determine if the sharing of this information is in the person's best interests as per the Mental Capacity Act 2005 (Chapter 16 of the Mental Capacity Act Code of Practice offers further guidance about disclosure of information) and in line with the Data Protection Act considerations set out above

If any other organisation, requests a copy of the report

For example, an external agency, such as a care home? The external agency is unlikely to have authority to make a subject access request, so it should be

treated as a third party request in the same way as requests from family and friends.

If another advocacy organisation requests a copy of the report

You will need to determine whether it is in the person's best interests including how this information will be used specifically to support the advocate in their role as the person's representative.

If a solicitor requests a copy of the report

You are under no obligation to provide the report, but you are unlikely to breach the **DPA** where the disclosure is required for the purpose of legal proceedings or legal advice. You should also consider whether disclosure is in the best interests of the client.

If a request is made from another person within the responsible body

For example, someone that isn't the decision maker e.g. a doctor, in another part of the hospital. If the request is for the purposes of making the relevant decision, the information can be shared. This is likely to be in the best interests of the client.

Data Protection Checklist

Actions once a **request for personal data by a third party who presents themselves as a representative of the client** (data subject) has been received by the advocacy organisation. Good practice is that organisations have data protection policies and procedures to guide staff.

The checklist should be used in conjunction with the a4a data protection guidance for advocacy providers

It does not give detailed information about the law.

If it is not already in writing, ask the representative to put the request for personal data in writing and ask them to state what information they are seeking and why.	
Ensure that every action/decision taken by the advocacy organisation and the reason for the action/decision is recorded. Keep a record of information sent, information withheld, any redactions and any exemption in the Data Protection Act you applied.	
Confirm receipt of the request for data by writing to the representative. Give information about any charge being made (max £10) and that the request will be acted on promptly and within the statutory 40 calendar days. Request any further information you need.	
Consider if the request is covered by section 7 of the Data Protection Act 1988 (data subject access request).	
Ascertain if the representative has the authority to act on behalf of the data subject. Consider if proof of identify is required / copy of LPA	

certificate/evidence that the representative has been appointed by the Court. Some people may have a letter from the person nominating them as their representative. If the representative has the right to make a s7 request on someone's behalf, you would need to have a valid reason to refuse to comply with the request. Valid reasons would include, for example, if the client has capacity to make the decision about disclosure and refuses consent, the data is outside of the requestor's authority, or if you have concerns that the data is being requested for the requestor's own purposes rather than the disclosure being on behalf of and in the best interests of the client.	
Ascertain if the client (data subject) has the capacity to consent or refuse to their personal information being disclosed. Be specific about what the information requested is about and who is requesting it when discussing it with them. To have capacity they would need to understand that someone has made a request to see their personal information, retain it for long enough to make a decision, weigh up the pros and cons of the person seeing the information and communicate whether or not they agree to the disclosure. If they have capacity it is their decision as to whether or not the information is disclosed.	
If the client lacks capacity, consider if you are satisfied that the person requesting information is acting on behalf of and in the best interests of the person and that they need the information to act properly. If an attorney or deputy asks for information the request must be within the scope of the requestor's authority. If the requestor asks for data for their own purposes related to the data subject this may not be within the scope of their authority and it may be more appropriate to treat it as a third party request.	
If the request for personal data relates to a case which is to be considered by the Court, liaise with the official solicitor to check if the request should be dealt with by the Court, particularly if the request is received from an interested party.	

When considering what information can be disclosed, it should be borne in mind that another person's privacy must be protected if that person is mentioned in the document (s). You may want to consider obtaining their consent to disclose information about them.	
Check whether a professional who has contributed to the information being considered for disclosure has any objections to their name and business addressed being disclosed.	
You may want to edit parts of the document as appropriate. Make sure you record your decisions in your own records about any information you are withholding.	
If the information contains opinions from other professionals you should check with them which information could be disclosed and which information they consider should not be disclosed. Explain you will consider their views but the final decision rests with you as the data controller.	
Consider any information which may cause serious harm to the physical or mental health or condition of the data subject or any other person which should not be disclosed without obtaining the view of the relevant medical practitioner. This applies to health and social work records.	
Once all of the above has been considered, and any document(s) edited where appropriate, the representative should be sent a hard copy of the information.	

This factsheet has been prepared with the assistance of Irwin Mitchell LLP. It refers to the law of England and Wales as of July 2011 and is intended for general information only and not as legal advice and should not be relied on as such. It should not be used in isolation as the basis for making decisions or for taking or not taking any steps in relation to any legal matters as it does not take account of your particular circumstances. Detailed specific advice on your particular circumstances should always be obtained from a suitably qualified lawyer before taking, or not taking, any action.

irwinmitchell IM

Action for Advocacy

Registered as a company in England and Wales No 4942158 Charity Number 1103575
Registered Office:

The Oasis Centre
75 Westminster Bridge Road
London
SE1 7HS

Tel: 0207 9214395
Fax: 0207 9214201
www.actionforadvocacy.org.uk

The IMCA Support Project is funded by The Department of Health