COUNTY SUPPORT GUIDE

Data Protection 2013

CONTENTS

OBJECTIVES

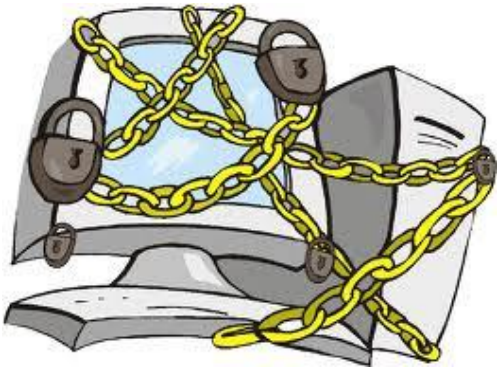
This support guide will help you to:

- Explain why the Data Protection Act (DPA) was introduced and its purpose
- Identify the eight DPA principles and rules governing the use of personal data
- Understand your legal responsibilities under the Data Protection Act
- Build a culture of security and awareness within your county/club

A2.25

Some paragraphs of particular complexity will be annotated with a bubble similar to this one next to it. The number contained in these bubbles relates to the relevant section in the 'Guide to Data Protection' which can be downloaded from the www.ico.gov.uk web site

The guide has been developed to disseminate and collate the main points of the legislation. Clubs and Counties are required to interpret the DPA and apply it to the various aspects of their own environment; therefore, sometimes there are no hard and fast rules. In these circumstances advice and clarification can be sought by calling the ICO help line found at www.ico.gov.uk



!

Note: Please make reference to the glossary on page 18

INTRODUCTION TO THE DATA PROTECTION ACT

The Data Protection Act (DPA) has a significant impact on our organisation. Everyday members trust us with personal and financial information, which could be very valuable in the wrong hands. We therefore have a duty of care, as well as a legal obligation to ensure this data is obtained and processed fairly and accurately.

As a member of NFYFC, you will be dealing with all sorts of facts and figures relating to our members. A good understanding of the DPA and how we comply with the DPA is vital to us all.

The Data Protection Act 1998

Background

The Data Protection Act 1998 (DPA) was introduced following public concern about personal privacy in the face of the rapidly developing and growing use of computer technology. The Data Protection Act 1984 was the first piece of legislation introduced and regulated the use of automatically processing information, which in the main is information processed on a computer. As a result of an EU Data Protection Directive, a new act, the Data Protection Act 1998, has now replaced the original Act, extending the law to include certain manual files.

About The DPA

Today in our modern world, computers and technology are used everywhere to store data. Much of this data is about individuals. This is known as personal data. The DPA exists to protect the privacy of living identifiable individuals by ensuring personal data is obtained and processed fairly. Under the DPA individuals have the right to:

- ask for copies of all data held about them
- insist on the modification of personal data if it is incorrect, inaccurate or outdated
- claim compensation for any damage suffered due to any loss, inaccuracy or unauthorised disclosure of data
- limit the issues to which their data may be put; and
- have their details held and processed fairly.

Some Important Jargon

There is a glossary at the back of this Support Guide but three phrases you need to be very familiar with are:

Data Subject

This means an individual who is subject of personal data

Data Controller

This means a person (either alone or jointly or in common with other persons) who determines the purposes for which and the manner in which any personal data are, or are to be, processed. So this means anyone who decides how and why personal data is processed.

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.

The Principles

The DPA is based on eight principles designed to protect an individual's privacy by ensuring data is used properly. The Principles state that the data must be:

- Obtained and processed fairly and lawfully
- Obtained only for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Held only as long as necessary for the purpose
- Only processed in accordance with the rights of the Data Subject
- Kept Secure
- Only transferred outside of the European Economic Area where adequate Data Protection safeguards exist.

Note: There is more information on the 8 principles on page 11

THE INFORMATION COMMISSIONER

The Information Commissioner is an independent officer appointed by the Queen, who reports directly to parliament. The Commissioner is responsible for overseeing the DPA and duties include:

- maintaining a register of data users
- publishing information on the DPA and how it works
- promoting compliance with the data protection principles
- encouraging the development of codes of practice to help data users to comply with the principles; and
- considering complaints about breaches of the principles of the DPA.

A2.25

Organisations are required to notify the type of data held and also the purposes for which the data is to be used with the Information Commissioner's Office. Using the data in any way, which is contrary to the notification, is an offence. An organisation must register every year at a cost of £35.

!

Note: Some organisations can be excluded from notification i.e. not for profit organisations but there are tight restrictions with this. 1) the type of personal information you can hold 2) the people that it relates to 3) the disclosures you can make **An exemption does not exclude you from complying with the DPA Act.**

In terms of membership data you do not need to take any action as the National Office owns and regulates the Membership Database and is therefore the Data Controller. However, if at County/Club level you collect and process data over and above the membership application forms, or use it for anything other than the reasons stated on the form you will be a Data Controller in your own right and you will need to decide whether you want to take advantage of this exemption or not. Examples of additional information collected may be: qualifications, employment status, car user, type of farming undertaken, hobbies etc.

!

Note: We advise you refer to the 'Exemption from Notification for Not-for-Profit Organisations' and the 'Brief Guide to Notification' to be found on www.ico.gov.uk

WORKING WITH DATA

As we saw in the last section, there are principles and rules, which must be adhered to when working with data. In this section we will look at what this means to us as processors of data and our procedures.

When working with data there are general rules we must follow, some examples are shown on the following table.

DO	DON'T
Ensure safe destruction of obsolete data.	Mislead or deceive the individual as to why the data is needed.
Ensure data relates to the business you are dealing with.	Release information to unauthorised personnel or individuals.
Clearly state and ensure the individual understands the reason for the personal data being held	Allow unauthorised access to personal data.
Keep data up to-date.	Leave personal data unattended by leaving your screen unlocked.
Record information accurately.	Include account/security details in unsecured e-mails to members.
Store data securely.	Leave personal data on a memory stick that isn't password protected
Keep your password protected and secret.	Leave consent forms or member details in cars, including laptopsthat are not encrypted

There are some frequently asked questions that you can refer to at the back of this guide.

DATA PROCESSING

The definition of data processing covers a very wide range of activities including: obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, aligning, blocking, erasing and destroying.

Under the DPA the person the data relates to is known as the Data Subject and processing of data is only permitted where the Data Subject has consented for this to happen. The consent for NFYFC to collect data for the membership database is within the privacy notice contained on the application form.

A3.12

Special rules apply to the processing of sensitive data. This is defined as information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life, criminal record, or court proceedings.

RELEASING PERSONAL DATA

Personal data can only be released to:

- the individual to whom the data relates
- a nominee such as a spouse, solicitor, power of Attorney or financial advisor but only if you have written consent from the Data Subject
- a member of staff or member of NFYFC ***within the remit of their duties or***
- 'A duly authorised person acting under the power of law'. This covers the fact that a court order is not always required e.g. the CSA (Child Support Agency) can request information under certain Acts but do not need a court order.

If you are releasing data in writing, always write directly to the individual unless you have written confirmation from them that a third party is acting on their behalf.

Note: Take care to ensure the communication is addressed correctly. When working with members' confidential documents (i.e. passports, bank statements, ID) please take extra care to ensure these are returned to the correct address.

If a caller claims to have authority to receive the personal data, ask for a telephone number and let them know that you will call back (this must be done by finding out the telephone number independently). Never assume they are entitled to have this information.

Note: At all times, only give out the data the individual is asking for and entitled to receive. Do not be tempted to give additional personal data.

Deleting Personal Data

The SILO database is maintained by NFYFC and therefore counties must not delete any data. However, if a county is a Data Controller within its own right because it collects additional data (see page 6) it must have a system in place which enables the prompt deletion of any additional data kept once it has served the purpose for which it was gathered, and we no longer have a legitimate reason to keep the data. If we need the data for analysis, we must remove all personal identifiers from it (i.e. names, addresses and account numbers).

DATA ADMINISTRATOR ROLE

The role of data administrator within the counties is an important one. The role includes:

- Ensuring that individuals have passwords for their computers
- Overseeing the smooth operation of those computers and
- Making sure data is backed up.

The data administrator should have a deputy who can sort immediate issues out when the data administrator is not available. All data administrators and deputies should read the Support Guide and sign the Data Control Policy document. Both the data administrator and the deputy should have access to change users passwords in cases of emergency.

It is very important that every individual who uses a county office computer or shares a computer has their own password. The practice of logging in under someone else's password should be discouraged for two reasons:

- They may then have access to personal data that they should not see.

- Anything that they do and the accompanying audit trail is only attributable to the password owner and in the case of legal proceedings that person will be deemed to be the perpetrator.

As a further security measure it is advisable to keep any personal data in separate folders protected by a password within your documents on the computer.

Note: Please refer to the FAQs at the end of this Support Guide for further examples

THE EIGHT PRINCIPLES

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the 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.

1) Processing personal data fairly & lawfully

This is the first data protection principle. It means that you must:

- Have legitimate grounds for collecting and using the personal data.
- Not use the data in ways that have unjustified adverse effects on the individuals concerned.
- Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data.
- Handle people's personal data only in ways they would reasonably expect
- Make sure you do not do anything unlawful with the data

2) Processing personal data for specified purposes

The DPA states that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose/s

3) Information standards (inc 4 & 5)

The 3rd, 4th and 5th principles are grouped together under the heading of 'information standards' and state that personal data should be:

- Adequate, relevant and not excessive
- Accurate and, where necessary, kept up to date
- Kept for no longer than necessary

Note: There are clear links between the third, fourth and fifth data protection principles and you need to be aware of how they connect. For example, if you don't update information when circumstances change, information that was originally adequate becomes inadequate. If information is kept for longer than necessary, it may be irrelevant and excessive

6) The rights of individuals

Individuals' rights are:

- A right of access to a copy of the information in their personal data.
- A right to object to processing that is likely to cause or is causing damage or distress.
- A right to prevent processing for direct marketing.
- A right to object to decisions being taken by automated means i.e. a loan is applied for online and criteria is used to give an immediate yes or no.
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed i.e. when an incorrect black mark has been placed on the credit reference agency when the debt has actually been repaid.
- A right to claim compensation for damages caused by a breach of the DPA

7) Information security

This principle means you must have the appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. It can be used for fake credit card transactions, mortgage fraud, child grooming and exposing the addresses of people at risk of assault or abuse amongst many other things. You must make sure that:

- Only authorised people can access, alter, disclose or destroy personal details.
- Those people only act within the scope of their authority.
- If personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals involved.

The DPA also requires 'physical' security i.e. quality of doors and locks, supervision of visitors, disposal of paper waste. Above all else you should be seen to be building a culture of security and awareness within your organisation

8) Sending personal data outside the European Economic Area (EEA)

B8

The eighth principle will only apply if the information moves to a country, rather than simply passing through it on route to its destination. There are no restrictions on the transfer *(please see glossary)* of personal data to EEA countries. These are currently:

Austria	Belgium	Bulgaria	Cyprus	Czech Republic	Denmark
Estonia	Finland	France	Germany	Greece	Hungary
Iceland	Ireland	Italy	Latvia	Liechtenstein	Lithuania
Luxembourg	Malta	Netherlands	Norway	Poland	Portugal
Romania	Slovakia	Slovenia	Spain	Sweden	

OUR LEGAL RESPONSIBILITIES

The DPA imposes legal responsibilities on both you and the organisation. By understanding the DPA and its principles and following the guidelines outlined you will meet your legal responsibilities.

The Key Things to Remember

- All data you collect must relate to the business you are dealing with, which means not collecting additional information just because it may come in handy.
- Ensure you gain **consent** to hold the data and ensure the individual understands the reasons we are requesting it.
- Don't mislead or deceive the individual as to why you need this data.
- Follow the eight DPA principles.
- When returning non-secure e-mails ensure that all personal and account details have been removed as e-mail is not always secure.
- Do not include details of account or credit card numbers, or any other personal data in any e-mail.

Consequences of Breaching the DPA

The consequences of breaching the DPA can be extremely costly both to you as an individual and the organisation.

You personally could face disciplinary action, **and criminal prosecution** for which you may be fined.

The organisation could face criminal action because of what employees/members do or fail to do. In addition the organisation faces a civil action which may mean:

- Revising our procedures.
- A claim for compensation by individuals.

This could lead to us having to de-register or wiping the data, both of which would result in us being unable to function.

FAQ's

Please refer to the guide (pdf, 286KB) the ICO publication 'Practical Guide to IT Security' for extra information

1. Can county officers download a copy of the database on their laptops or USB/memory stick?

Yes, however, the officer should ensure that the information is password secured or encrypted and the information is required within the remit of their role during their term of office i.e. for planning events within the YFC programme. The information should only include the required fields , should only be used for YFC purposes and not shared without justification. Officers should be vigilant when carrying this information and laptops/memory sticks should not be left unattended and ensure that data is deleted as soon as it has been finished with.

For support with password protecting files or USB/memory sticks please contact NFYFC.

2. Can the membership database be printed off and kept by an officer for the duration of their year in office?

Yes, however, as above the information must only be used for YFC purposes within the remit of duties and be locked away at all times when not in use i.e. within a locked drawer or cupboard and nobody else must have access to it, the information should not be left unattended in a car it should be kept with the person or locked away securely.
Paper copies of information from the database should only include the required fields for the event, i.e. at a competitions day when information is required for booking in teams. Where sensitive information needs to be taken note of, use a symbol on the booking in sheet next to the participant rather than the full description of the medical need. This will avoid this sensitive information being accidentally seen by others booking in. The full information on the participants needs can then be found on the consent form.

Where possible use a mini export form including name, DOB, club name and membership number and manual item number when creating spreadsheets

3. Who should have overall administrator rights on the computers that counties own?

To comply with the eight principles of the DPA a person must be able to access personal data only if it is within the remit of their role therefore the same rule applies to an administrator. If ordinarily they would not have access to personal data they should not have administrator rights. County federations operate under many different management structures; they should ensure that those with access to the membership database are justified to do so within their role.

4. What are the restrictions on the use of data stored on the membership database?

The personal data collected on the membership database can only be used within the confines of the YFC network and should not be displayed in the public domain i.e. county magazines or web sites unless the consent box has been ticked on the membership form and the member has agreed for this information to be shared. This is especially important for children under a protective order. Data administrators and county federations need to ensure that they have permission to disseminate all the information they share in order to protect our member's identity and information.
On a practical level, where parents have requested that the image of their child is not shared, a picture of the child should be held on file and this file checked before pictures are uploaded onto websites/social media or are sent to the press for publication.

5. What are the recommendations regarding using photos and contact details on the internet and in written publications?

The privacy notice on the membership forms gives permission to disclose this information within the public domain. When including members details in publications like the county handbook or on county websites, ensure that the member has consented to their information being shared in this manner and they are happy to be contacted on a personal number or email regarding YFC business.
We also recommend that you avoid putting individual member photographs against contact details as this allows people easier routes to access information for potentially fraudulent or abusive behaviours especially when they have access to addresses of individuals.

Care should be taken when including the contact details of members under the age of 18 in county handbooks or websites. We suggest that you seek permission to include the child's contact details and ensure that younger members in club roles are aware of how to deal with YFC enquiries and what to do if they are subject to inappropriate contact. Alternatively details of parents or other officers contact details can be put against their name or or you may wish to write 'please contact the club chairman' instead.

6. Can more than one person have access to the computer and database passwords in case people are ill or unable to attend work?

They can if it is within the remit of their duties i.e. they need to access certain information in order to complete their job role (volunteer or paid staff). Ensure that they have read the County Policy for Data Controls document. We recommend that the county has job role specifications that include statements regarding this as stated in the County Policy for Data Controls.
Each year a document containing who has access to member information held by the county federation should be updated to reflect the changes in roles. Information held by previous office holders should be reclaimed and destroyed.

See appendix for example document County Policy for Data Controls.

7. Who should have access to safe recruitment information within the county?

Only those involved in safeguarding decisions within the county federation should have access to CRB certificates during the recruitment of a staff member/volunteer which should be filed away securely under the same guidelines as other data. CRB regulations state that the actual CRB certificate should be destroyed after 6 months and only the certificate number, the date the check was processed and any other relevant information such as cautions or convictions can be recorded as part of the recruitment decision process.

8. How long should safe recruitment information be kept?

As stated above, CRB forms need to be destroyed (shredded) after a recruitment decision has been made, within 6 months of receiving the document. Relevant information used in the recruitment decision should be recorded and kept on the staff/volunteers file.

References for staff and volunteers should be kept for the duration of the person's involvement with the organisation and following this should be archived for 6 months after their involvement as a volunteer within the organisation has ceased.

We realise this presents a challenge with the storage of documents and have been advised that information can be scanned into an electronic version and saved in computer files should an enquiry emerge about a previous staff member/volunteer and this information could support an investigation.

9. How long should parental consent forms be kept?

We have been advised by NFU Mutual there is no insurance requirement for parental consent to be retained for any set period of time. It would be good practice to be able to demonstrate care has been taken in these areas but the desirability of doing this should be balanced against the practicalities of storing large volumes of paper.

However, for booking in lists with members details, attendance signatures and proof that parental consent was obtained should be retained ideally for 7 years in the event of an enquiry about the event, for insurance purposes, data collection and evaluation.

For an example Booking-In List please contact James Eckley

10. Is our county/club a data controller?

No, NFYFC is the data controller, you only become the data controller if you are collecting personal data over and above the information collected on the membership forms, adding additional fields to the database OR using it for purposes other than those stated in the privacy notice.

Information on what is a data controller can be found on page 5

11. What measures do I need to take if other people use our computers?

All computers containing personal data must have appropriate anti-virus and firewall software installed. All personal data should be separated into specified folders and files which should be password protected at all times. At no time should members personal details be accessible to third parties who may 'hot desk' or share computers. A separate log-in should be created for those using the county computers that should not have access to the membership database.
We would recommend members should be using a log-in with no access to files stored in other accounts.

12. What happens if personal data is lost or stolen?

If, despite the security measures you take to protect the personal data you hold, a breach of security occurs, it is important that you deal with the security breach effectively. The breach may arise from a theft, a deliberate attack on your systems, from the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately. You should assess any risks associated with the breach. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

You should, for example, consider notifying the individuals concerned; the ICO; other third parties such as the police and the banks. The National Office must also be notified. It is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

More information can be found in the ICO publication Guidance on information security breach management

13. Are we able to advise members on what contact details are given out when promoting club activities?

When promoting club activities a member may be given the job of coordinating bookings or being the lead contact point for an event such as a harvest supper. If the event is advertised to the general public in the form of posters, advertisements in magazines or on the internet including social media platforms we should be cautious about the information we share. Individuals should avoid giving out to many personal details, avoid having a home address on promotional material to have correspondence sent to, this should be sent to a common address like the county office.

A mobile phone number or email address for contact is appropriate but members should report any strange calls or messages they may receive regarding the event to the county office. This is especially important if an under 18 year old member is the lead for a specific event. In this case communication may be better directed via an adult officer in the club or the child's parents. Where this is not possible it is important to inform the parents of the members that they will be taking calls and emails regarding this event and their mobile number and email address will be shared. The member should also be informed that if they have enquiries that they don't know how to deal with they should ask a club officer or parent for support. Many clubs have a generic email address and club mobile phone that they use for all communication regarding club events, if the club can facilitate this can be useful as it avoids the need to share individual members personal contact details.

14. How do we practically advise our Club Secretaries and Chairpersons to keep personal information secure when out in 'the field'

Please also refer to FAQ 2

As clarification, when a member of the National Office is out supporting events they always have paper copies of consent forms and other records. These are kept in a file and with a member of staff at all times. They are then moved to different locations i.e. hotels or different venues in a rucksack or bag and therefore still within the person's possession.

Paper copies of information from the database should only include the required fields for the event, i.e. at a competitions day when information is required for booking in teams.

15. How long should electronic membership data be kept?

If the YFC member has ticked the box on the membership form asking for data not to be kept the whole record must be deleted by the National Office. However, keeping data for long periods of time i.e. after the member has left the organisation, is allowed if it is required for marketing purposes including (but not exhaustive) invitations to future events or to enlist their services as judges or stewards. However, to comply with the law all sensitive data must be removed from the record. This can be done at county level.

For more information on 'sensitive data' please see the Data Protection Support Guide 2013 page 9

16. Should the Club Secretary or Club Chairperson have the consent forms with them at every meeting?

Please also refer to FAQ 2.

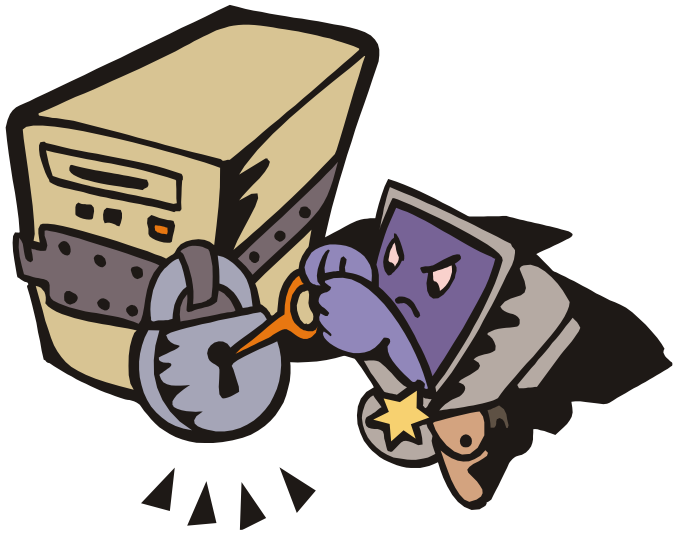
Yes – these should be available at every meeting as they contain the emergency contact details and medical information on the members in your care.

17. If an 'Under 18' is in charge of an event can they put their contact details on facebook or other marketing channels?

Please also refer to FAQ 6 and FAQ 2

Yes they can, however, we still have a duty of care so we recommend that you still contact the parent to get verbal consent for this to happen and record the conversation in note format.

We also highly recommend the purchase of a cheap 'pay as you go' mobile phone that can be used for club activities and then be passed between members when they are organising different events. This then eliminates any personal contact details having to be divulged.



GLOSSARY

Within the Act the following words must be interpreted with the following meanings

Word	Meaning
DATA	Information which is: a) Being processed by means of equipment operating automatically in response to instructions given for that purpose b) Recorded with the intention that it should be processed by means of such equipment c) Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system
DATA SUBJECT	An individual who is the subject of personal data
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
DATA PROCESSOR	Any person (other than an employees of the data controller) who processes the data on behalf of the data controller
THIRD PARTY	Any person other than a) The data subject b) The data controller c) Any data processor
PERSONAL DATA	Means data which relates 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 This 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

Word	Meaning
PROCESSING	Obtaining, recording or holding the information or data or carrying out any operation on the information or data, including: a) Organisation, adaption 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 transformation, dissemination or otherwise making available d) Alignment, combination, blocking, erasure or destruction of the information or data
RELEVANT FILING SYSTEM	Any set of information relating to individuals to the extent that, although the information is structured, either by reference to individuals or by reference to criteria relating to those individuals, in such a way that specific information is readily accessible.
RECIPIENT	Any person to whom the data are disclosed, including any person to whom they are disclosed in the course of processing i.e. an employee or agent of the data controller
TRANSFER	A transfer involves sending personal data to someone in another country. *Example: A travel agent sends a customer's details to a hotel in Australia where they will be staying while on a visit.* A transfer is not the same as the transit of information through a country.