General Data Protection Regulations (GDPR) for NACCC Accredited Centres

Background

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

From 25th May 2018 all organisations will need to comply with this regulation

This is unlikely to change when we leave the EU as there is currently a Data Protection Bill going through parliament which will include the new GDPR and will replace the Data Protection Action 1998.

Preparing for the General Data Protection Regulation (GDPR)

In September 2017 the Information Commissioners Office (ICO) produced a document **'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'**. This document needs to be read so that you can gain a better understanding of the GDPR.

Please see information overleaf on the 12 steps and what you need to consider:

Step 1 is Awareness

This is about making sure that decision makers and key people in the organisation are aware that the law is changing to GDPR. Make a list of who are the decision makers and key people. How are you going to inform them of the law changing, confirm when this has been undertaken.

Action – Record that the decision makers are aware of the GDPR

Step 2 – Information you hold

You need to document what personal data you hold, where it comes from and who you share it with.

Personal data *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by*

reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Examples of data breaches:

- Personal data being posted to an incorrect address which results in an unintended recipient reading that information;
- Dropping or leaving documents containing personal data in a public place;
- Personal data being left unattended at a printer enabling unauthorised persons to read that information;
- Not locking away documents containing personal data (at home or work) when left unattended;
- Any action which allows an unauthorised individual access to buildings or computer systems (e.g. through losing a Smart Card, disclosing passwords or writing down passwords etc.);
- Verbally disclosing to or discussing personal data with someone not entitled to it, either by phone or in person

Are opinions that we record about people classified as personal data? If they are computerised or are intended to be computerised (e.g. scanned to a eDS) or form part of a structured filing system etc. then those opinions may well be personal data. This can include doodles and sketches.

A pro forma is available for recording the information.

This is likely to be one of the biggest tasks to be undertaken, once you know what information you hold this will help you in completing the remaining steps.

You need to also take into consideration the security of data, if you are emailing information are you sending it encrypted, is the person you are sending it to complying with the GDPR.

Action – Record what personal data you hold, where it came from and who you share it with.

Step 3 - Communicating privacy information.

You need to review your current privacy notices and then update by May 2018.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

Once you have completed step 2 this will help you see what you do with your data and then you can record it on your privacy notice. NACCC have 2 privacy notices one on our website and one on the Safe Referral System. There are no standard privacy notices available as yet for the new GDPR as information will be very specific to an organisation and as it is not enforceable until May 2018 companies are not putting out new privacy notices yet.

Refer to Step 6 also.

Action – Look at your current privacy notice, look at other organisations notices, update once you have completed step 2.

Step 4 – Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification (putting something right)
- the right to erasure
- the right to restrict processing (only allowed to store the data)
- the right to data portability (allows individuals to obtain and reuse their personal data)
- the right to object
- the right not to be subject to automated decision-making including profiling (decisions are based on human intervention rather than a computer).

NB - The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means

Action – Review your Data Protection Policy, make any necessary amendments.

Step 5 - Subject access requests http://www.opt-4.co.uk/dictionary/Consent.asp

You should update your procedures and plan how you will handle requests to take account of the new rules:

In most cases you will not be able to charge for complying with a request.

- You will have 28 days to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

Action – Ensure your policy on Subject Access requests is up to date. This may be included in your data protection policy currently.

Step 6 - Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should

document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

Action – See step 3

Step 7 – Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. The key new points are as follows:

The GDPR sets a high standard for consent.

- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh consents if they don't meet the GDPR standard.
- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and granular (finely detailed). Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent a precondition of a service.
- Public authorities and employers will find using consent difficult.
- Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

Action – Make the necessary changes to your consent form to ensure they comply.

Step 8 – Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully.

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

Action – Unless you offer online chat rooms or have apps for children that you have devised you will not need to undertake any further action.

Step 9 – Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (Information Commissioners Office) (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

You need to consider the security of your emails, are you sending them encrypted when it contains personal data, is the person you are sending it to following the correct procedures.

Action - Ensure your policy on Data Breaches is up to date. This may be included in your data protection policy currently.

Step 10 - Data Protection by Design and Data Protection Impact Assessments

Privacy impact assessments (PIAs) are tools which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals;
- whern you process data on a large scale of the special categories of data.

Action – None unless you are intending to implement the last 3 points.

Step 11 – Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale;
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

Action – Who is going to be responsible for data protection in your organisation?

Step 12 – International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

Action – None unless you do operate in more than one EU member state.

Support for Organisations

The Information Commissioners Office have set up a **dedicated advice line** offers help to small organisations preparing for the new data protection law.

The phone service is aimed at people running small businesses or charities. To access the new service dial the ICO helpline on **0303 123 1113** and select option **4** to be diverted to staff who can offer support.

As well as advice on preparing for the General Data Protection Regulation, callers can also ask questions about current data protection rules and other legislation regulated by the ICO including electronic marketing and Freedom of Information.