The General Data Protection Regulation (GDPR)
LACVS - Briefing Paper, March 2018

GDPR INTRODUCTION

On 25th May 2018 the Data Protection Act (DPA) will be replaced by the European General Data Protection Regulation (GDPR) and be incorporated into UK law. GDPR is intended to intend strengthen data protection and the digital rights of individuals.

GDPR governs the processing and control of personal data, including the storage, use and transfer of information relating to living individuals who can be identified. Whilst GDPR is broadly similar to its predecessor the DPA, there are some new/ different requirements that organisations need to get to grips with.

Key features of GDPR include:

- stricter rules on obtaining consent to collect personal data, which must be freely given, specific, informed and unambiguous;
- organisations will need to review their privacy notices and tell individuals the legal basis for processing their information.

Organisations will have to demonstrate compliance with GDPR and must report data protection breaches. They will face significant fines for not reporting a breach of data protection. The maximum fine will increase from £500,000 to £17 million in case of a breach.

The Information Commissioner's Office (ICO) recognises that not all organisations will be fully GDPR-compliant by May 2018 but expects to see strong evidence that any organisation that comes to its attention is taking action to meet GDPR requirements.

This means, being able to demonstrate what work an organisation has done so far to prepare and outline what has yet to be done, when it will be done and by who.

GDPR CHECKLIST SUMMARY

1. **Identify who is responsible for data protection**
2. **Audit the information you currently hold**
3. **Update your privacy notices**
4. **Cover individuals' rights**
5. **Be equipped to deal with 'subject access requests'**
6. **Identify a lawful basis for processing personal data**
7. **Review consent**
8. **Children**
9. **Review external contracts**
10. **Data breaches**
11. **Data Protection by Design and Data Protection Impact Assessments**
12. **International**

GDPR CHECKLIST FULL

1. Identify who is responsible for data protection

You'll need to appoint someone to lead on compliance with GDPR and work out where this role will sit within your organisation's structure and governance arrangements. Implementing the GDPR could have resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute. You should also 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; or
- an organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal convictions. (The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs)

It is important that someone in your organisation, or an external data protection advisor, takes responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

2. Audit the information you currently hold

Your organisation will need to undertake an audit of all data that you currently hold on customers, members and other stakeholders. You'll need to document what you have, where it came from and who you share it with. As part of the audit process you should also review whether the personal data that you currently hold is accurate and up to date. if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy, so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. As is currently the case with the DPA, you'll also need to think about and develop ways of regularly reviewing and keeping personal data up to date in the future. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place. You'll also need to review and amend internal data storage systems such as any contact databases, communications lists and CRM systems.

3. Update your privacy notices

Under GDPR you'll have an obligation to tell customers, members and other stakeholders how you intend to use their data. You'll need to update privacy notices on your website to give additional information on how long personal data is kept for and the lawful basis for processing it. The ICO's Privacy Notices Code of Practice reflects the new requirements of the GDPR (see ICO website).

4. Cover individuals' rights

You should check that your procedures cover individuals' rights. GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- he right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion? 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; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine-readable form and provide the information free of charge.

5. Be equipped to deal with 'subject access requests'

If someone asks for their data, this is known as a subject access request. 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 a month 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.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6. Identify a lawful basis for processing personal data

You should identify the lawful basis for your processing activity, document it and update your privacy notice to explain it. Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under GDPR because 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.

7. Review 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. You should read the detailed guidance the ICO has published on consent under GDPR and use its consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, preticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

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, 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. 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'. This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9. Review external contracts

Contracts with third parties that process personal data on your behalf, such as payroll providers and IT support, may also need to be reviewed and may need to be updated or renegotiated in advance of May 2018 in order to meet GDPR requirements.

10. Data breaches

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. 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 (and possibly some other bodies) when they suffer a personal data breach. 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.

11. Data Protection by Design and Data Protection Impact Assessments

GDPR will enforce stricter rules upon organisations to ensure that they are taking all reasonable measures to guard against data theft, loss, or other breach, meaning data protection should be seen as part of our day jobs, not as an add-on. Under GDPR "privacy by design" is legally required. meaning that organisations will need to build data protection considerations into all activities, new projects and services. 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, 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. 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; or
- where there is large scale processing of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally? You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management

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. The Article 29 Working Party has produced guidance on identifying a controller or processor's lead supervisory authority.

GDPR RESOURCES

Information Commissioner's Office – Guide to GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office – Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

NAVCA - An Overview of the General Data Protection Regulation (GDPR)
https://www.navca.org.uk/resources/506-an-overview-of-the-general-data-protection-regulation-gdpr

Charity Finance Group – GDPR - A Guide for Charities
http://www.buzzacott.co.uk/getattachment/4fa8713f-a66e-41f1-ab72-1ffc27093a6c/GDPR-A-Guide-For-Charities.pdf.aspx

Information in this note was extracted from:

Information Commissioner's Office – Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

NAVCA - An Overview of the General Data Protection Regulation (GDPR)

March 2018