Committee(s)	Dated:
IT Sub Committee – For Information	14 July 2017
Subject: GDPR Briefing	**Public**
Report of: The Chamberlain	**For Information**
Report authors: Sean Green & Gary Brailsford-Hart	

Summary

- The purpose of this report is to brief Members on the General Data Protection Regulations (GDPR) that will replace the Data Protection Action 1998, coming into force in May 2018.
- This report provides a brief overview of GDPR and additional or changed responsibilities from the current required DPA compliance responsibilities.
- The report also outlines next steps to ensure both the Corporation and City of London Police are compliant with GDPR.

Recommendation(s)

Members are asked to:

- *Note the report.*

Main Report

Updates

General Data Protection Regulations

1. GDPR is the new EU regulation that comes fully into force on 25th May 2018. The regulations introduce uniform rules for data protection across Europe. The regulations are intended to make data regulation fit for the digital world we now live in. From the 25th May 2018, the regulations will replace the Data Protection Act (DPA) (1998).

2. The core principles of current Data Protection legislation remain unchanged. However the GDPR adds new obligations to provide a higher level of protection of personal data and these new obligations could require additional effort in order to comply with and meet these requirements. The Corporation has an Information Management Board chaired by Michael Cougher the Senior Information Responsible Officer (SIRO) for the Corporation and the City of London Police also has an Information Management Board chaired by their SIRO, the Commissioner.

3. The purpose of GDPR is to protect the privacy of individuals; ensure that data is not processed without the knowledge and consent of individuals; to grant data subjects various additional rights (including greater scope their rights to access their data).

4. The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

5. Current DPA states the following eight principles:

    - Data shall be processed lawfully
    - Data shall be processed for a specified purpose
    - Data shall be adequate, relevant and not excessive
    - Data shall be accurate and up to date
    - Data shall not be kept longer than necessary
    - Data shall be processed in accordance with the rights of data subjects
    - Data shall be kept secure
    - Data shall not be transferred outside of the European Economic Area (EEA) with adequate controls

6. In summary compared to the DPA, GDPR will result in:

    - More data being in scope;
    - Corporation Suppliers and processors of data in scope;
    - Tougher sanctions for breaches;
    - Compulsory notifications to the Information Commissioner of data breaches;
    - More rights for individuals;
    - Explicit recording and management of consent;
    - A new statutory senior role for the Data Protection Officer;
    - Greater accountability and governance.
      (Note: Appendix A provides a more detailed breakdown of the changes)

7. Within the Queens Speech of 21st June the Data Protection Bill was confirmed. The Government has stated that the new UK bill would ensure the country met its obligations while a member of the EU, and would help the UK maintain its "ability to share data with other EU member states

and internationally after we leave the EU". The new bill will replace the Data Protection Act 1998. The government has stated its key priorities as follows:

- ensuring data protection rules were "suitable for the digital age";
- "empowering individuals to have more control over their personal data";
- giving people the "right to be forgotten" when they no longer wanted a company to process their data - providing there were no legitimate grounds for a company retaining the data;
- modernising data processing procedures for law enforcement agencies;
- allowing police and the authorities to "continue to exchange information quickly and easily with international partners" to fight terrorism and other serious crimes.

8. An audit is being commissioned with internal audit to help the Corporation identify gaps in compliance and then produce an action plan (possibly requiring a project) to address these gaps. The GDPR audit includes:

    - readiness assessments, detailed risk-based compliance assessments across all GDPR clauses and themed compliance reviews e.g. cross-border transfer analysis, implementation of our compliance program and on-going monitoring;
    - Privacy Impact Assessments (PIA);
    - breach response reviews;
    - third-party privacy reviews;
    - design and implementation of privacy and operating models;
    - data protection internal audits;
    - training and awareness programmes;
    - audit compliance, implementation and change management related to GDPR; and
    - cyber security and information security.

9. It should be anticipated that the new GDPR regulations will require new or updated policies, procedures and possible changes to employee roles and guidance as well as additional technical enablers to manage the tracking of assets and consent. This will need to be backed up by new training materials, communication and awareness.

10. Based on the findings from the audit and the 12 steps preparation guidelines issued by the Information Commissioner's Office (ICO) see Appendix B, Director of Information will finalise the action plan across the Corporation and the City of London Police.

11. A further update on GDPR will be brought back to the IT Sub-Committee in November 2018.

Sean Green
IT Director
T: 020 7332 3430
E: sean.green@cityoflondon.gov.uk

Gary Brailsford-Hart
Director of Information
T: 020 7601 2352
E: Gary.Brailsford@cityoflondon.pnn.police.uk

Appendix A – DPA Obligations comparison with GDPR

Theme	DPA	GDPR
Rights of Data Subjects	• Access to personal data • Prevent processing likely to cause damage or distress • Prevent processing for direct marketing • Object to automated decision making • Have inaccurate personal data removed • Claim compensation for damages caused by a DPA breach	• Data portability • To be forgotten • Object to processing
Subject Access Requests	• Where an individual requests access to their own information • Required ID and a written request • 40 day deadline to respond • £10 fee required	• Deadline to respond 1 month • No fee required
Data Breaches	• Report to Senior Responsible Information Officer (SIRO) • No need to report to the Information Commissioner's Office (ICO) • Maximum fine £500,000	• Must be reported to ICO within 72 hours • Fines up to 2% of turnover or €10m for poor record keeping, contracting etc • Fines of up to 4% of turnover or €20m for breaches of rights or principles • New definition 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed
Privacy Notices and Consent	• A privacy notice should contain: The identity of the data controller; the purpose for which you intend to process the information; any extra information you need to give individuals the context to enable you to process the information fairly • Soft opt in to data protection and use of information for specified reasons is permitted (e.g. tick this box if you don't want us to use your information)	• Show the legal basis for processing information • Data must be trackable • No more 'soft opt ins' • Controller must prove consent
Privacy Impact Assessments	• Not Mandatory • Recommended when processing large amounts of data	• Mandatory for all business cases • Privacy by design
Other Considerations		• DPA Officers mandatory role in an organisation processing data • Consent for use of Children's Data • Child likely to be defined as anyone under 13 years of age

Appendix B – Information Commissioners Office: 12 steps preparation guidelines

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now

1 Awareness You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

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.

5 Subject access requests You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

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.

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.

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.

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

10 Data Protection by Design and Data Protection Impact Assessments You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

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.

12 International If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's Overview of the General Data Protection Regulation. The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, 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. You should document this. 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.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

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 those 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.

The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

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;
- 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 the 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 the 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 Subject access requests

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 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.

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 the 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 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 the GDPR, and use our 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, pre-ticked 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, 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'.

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 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 (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.

10 Data Protection by Design and Data Protection Impact Assessments

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; or
- where there is processing on a large scale 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.

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

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 lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states. If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

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