



Appendix 1

## DECISION PAPER

DECISION: 2017/35	20TH. DATE: NOVEMBER 2017
TITLE: GENERAL DATA PROTECTION REGULATION	
REPORT BY: ANGELA HARRISON (DIRECTOR)	

### Executive Summary

The Data Protection Act 1998 regulates how the Commissioner uses and stores the personal data of its customers and staff. An EU Directive, the General Data Protection Regulation (GDPR) will replace the Data Protection Act. The GDPR sets out how organisations can collect and use personal data. The GDPR comes into force on 25 May 2018. Before then, the UK will pass a new law so that the GDPR applies in the UK. The GDPR applies to organisations that provide goods or services to individuals in the EU. This includes organisations outside the EU that want to provide goods or services within the EU. The GDPR (and the new law) will continue to apply in the UK after the UK leaves the EU.

### Recommendation

The Commissioner is requested to note the report.

Signature

Police and Crime Commissioner

Date 20th November 2017

## **PART II**

### **1. Background**

- 1.1. The current Data Protection legislation is enshrined in the European Data Protection Directive 95/46 EC. European member states implemented in this legislation by introducing domestic legislation. In the UK this was the Data Protection Act 1998 (DPA)
- 1.2. The DPA placed obligations on organisations processing (handling) personal information to comply with eight principles and to fulfil certain responsibilities as Data Controllers of personal information and it gave individuals certain rights. It also introduced corrective powers and administrative fines for noncompliance with the Act.
- 1.3. The General Data Protection Regulation (GDPR) became European law on 24th May 2016. On 25th May 2018 the GDPR will take effect in UK law following a two year transitional period. It will remain in force until the UK leaves the European Union and amends or repeals the legislation. It is highly likely that post Brexit UK privacy legislation will retain significant elements of the GDPR.
- 1.4. Recent unprecedented and rapid advances in technology have brought about fundamental changes to the way people use and share information. A series of high profile security breaches, phone hacking scandals and globally reported whistle-blowing revelations have all served to increase public awareness of the impact of technological advances on their personal privacy
- 1.5. The GDPR responds to these challenges and opportunities by introducing changes to strengthen individual's rights and build trust. Those processing personal data will face increased accountability and compliance obligations.
- 1.6. The overall themes of the GDPR are to:
  - Harmonise data protection law across member states
  - Increase the importance of data protection within organisations
  - Widen the scope of what constitutes personal data and to introduce special categories of data eg., Biometric data.
  - Introduce legislation that applies to data processors as well as data controllers
  - Provide individuals with greater rights and powers over their personal information
  - Simplify the current DPA principles

- Introduce greater sanctions such as higher fines.
- 1.7. The current eight principles that organisations must comply with are being replaced by six, as follows:
- Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limited
  - Integrity and confidentiality
- 1.8. The principles in some cases place similar obligations on organisations but there are some differences, such as the obligation to be transparent and greater emphasis on only processing personal information for the specified purpose and only collecting the minimum amount of data. Appendix 1 provides further detail on the differences.
- 1.9. In summary, the GDPR retains the fundamental principles of current data protection law. Any organisation which can demonstrate good compliance with the DPA and the NHS IG Toolkit (or any successor framework) will be well-positioned for compliance with the new regulation.
- 1.10. The ICO will remain the UK regulator. Existing data protection CSE law and subsequent rulings under the new regulation prior to the UK's departure from the EU, will continue as a binding part of UK law. The Human Rights Act and European Convention on Human Rights will remain an important element of privacy and information law in the UK, in particular the right to a private and family life.
- 1.11. The ICO have issued initial guidance for preparing the introduction of the GDPR, 'GDPR – 12 Steps to Compliance' which can be seen in Appendix 2. This has been followed by their Overview of the GDPR in January 2017, which will be regularly reviewed and updated. In addition, the ICO is providing updates on its website on the DP Reform page and is providing updates in the monthly newsletter.
- 1.12. The ICO have stated that compliance with the current Data Protection Act is seen as a good starting point for compliance with the GDPR.
- 1.13. The next steps for the Commissioner's Office are to:
- i. Produce an Implementation Action Plan based on the GDPR 12 Steps to Compliance document.
  - ii. Ensure awareness of the GDPR is raised and maintained with decision makers and key people, through regular reports and briefings;
  - iii. Identify all Commissioner information assets to ensure processing of personal information is documented and in accordance with the GDPR. This will link to the Information Asset Owner register and role and inform the development of Privacy Notices; and

- iv. Ensure existing and future contracts are reviewed and amended as appropriate to comply with GDPR requirements.

## 2. Financial Implications

- 2.1. Non-compliance with the GDPR could have a serious financial implication for the Commissioner.
- 2.2. Organisations that breach the current Data Protection Act are liable to a fine, capped at £500,000. Under GDPR, organisations are liable to a fine up to 20million Euros or 4% of turnover, whichever is higher. If a breach involves personal data of an individual, they can also claim damages.
- 2.3. The appointment of our Data Protection Officer will through the Constabulary necessitate payment for half the salary.
- 2.4. Additional support to assist us in meeting the tight deadline will be provided through independent consultancy, for which financial provision has already been made.

## 3. Legal Implications

- 3.1. The GDPR is a large document of regulations, over 80 pages. The GDPR reinforces the established legal principle that we can only collect and use personal data if it has a legitimate reason and before collecting or processing personal data, we must make sure it has a proper reason.
- 3.2. The GDPR sets out when the Commissioner can collect or process personal data. The main reasons are:
  - We have the consent of the data subject (the person that the data we are collecting is about) Processing is necessary to carry out a contract with the data subject or to take steps to enter into a contract
  - Processing is necessary for compliance with a legal obligation (something we must do by law)
  - Processing is necessary so we can do something in particular that is in the public interest or because we are legally allowed to in order to do something that we are responsible for
  - Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (this reason is not applicable to public authorities)
- 3.3. The GDPR requires that any consent must be freely given, informed and give a clear indication of an individual's wishes. There are also special requirements for consent from children, which will affect some of our services.
- 3.4. The individual's rights under the GDPR include:
  - 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 be subject to automated decision making and profiling

#### **4. Human Resource Implications**

- 4.1. The GDPR requires organisations to demonstrate compliance with the regulation; this includes training, internal audits, data protection by design and the appointment of a Data Protection Officer (DPO).
- 4.2. In response to the GDPR, the Commissioner's office will appoint a DPO at Lancashire Constabulary.
- 4.3. The DPO is not responsible for compliance with GDPR. It is the responsibility of the Office. The DPO will monitor how the Office implements GDPR and will provide advice.
- 4.4. There will be briefings and training in the coming months for all staff.

#### **5. Conclusion**

- 5.1. The GDPR marks a major change in the way we must use and store personal data from 25 May 2018. We must approach the new directive very seriously and ensure that the Commissioner's Office treats individual data relating to customers and staff with the utmost respect and ensure that we are not subject to the financial penalties that will occur if we do not.
- 5.2. The Commissioner is requested to note the report and receive and update on progress in February 2018.

#### **6. Background Papers**


Regulation (EU) 2016/679 of the European Parliament and of the Commissioner 27 April 2016 (GDPR)

<http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

#### **7. Appendices**

Appendix 1 – Main changes introduced by GDPR.

Appendix 2 - 12 steps for the implementation of the GDPR.

Officer declaration	Date
As above <b>LEGAL IMPLICATIONS</b>	
As above <b>FINANCIAL IMPLICATIONS</b>	
As above <b>EQUALITIES IMPLICATIONS</b>	
As above <b>CONSULTATION</b>	
<p><b>Chief Executive Officer (Monitoring Officer)</b></p> <p>I have been informed about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. I am satisfied that this is an appropriate request to be submitted to the Police and Crime Commissioner for Lancashire.</p> <p>Signature...  ...Date..... 20.11.2017</p>	

## **Appendix 1**

### **MAIN CHANGES INTRODUCED BY THE GDPR**

Many of the changes from the GDPR will already be familiar to organisations in the UK, such as mandatory privacy impact assessments for high risk processing, the concept of pseudonymisation (data de-identification) and financial penalties.

#### **Individuals will notice:**

Wider rights of subject access and information about processing  
Greater transparency about processing, and  
Stricter conditions for consent and the right to object

#### **For organisations there will be a focus on accountability and pro-active, evidenced-based compliance:**

Thorough risk assessments, and the principles of 'privacy by design' and 'data protection by default'

Requirement to maintain accurate records of all data processing activities

Increased regulatory enforcement powers and penalties and

Stricter breach notification requirements to both regulators and to the individuals affected.

**A summary of the main changes and the requirements of the GDPR can be found below, and will be further explained when guidance has been issued by the ICO:**

- a. A wider and more detailed definition of what constitutes personal data
- b. A greater obligation on Data Controllers to demonstrate compliance with the GDPR, through:
  - i. The maintaining of specified documents detailing the processing of personal information including clearly identifying the Data Controller and Processor if applicable
  - ii. A legal requirement to conducting impact assessments for 'higher risk' processing;
  - iii. Implementing data protection by design and by default, ie., data minimisation and de-identification to maintain and support privacy and confidentiality;
  - iv. Appointing a designated Data Protection Officer with professional knowledge and experience who reports to the highest level of the organisation; and
  - v. Contracts will need to be more explicit with Data Processors and sub-contractors.
- c. New obligations on Data Processors acting on behalf of a Data Controller in relation to the processing of data.
- d. Enhanced conditions to be met when data processing is on the basis of consent and where possible processing will be underpinned by legislation or statutory duty
- e. Privacy Notices will need to be more comprehensive and set out the rights of the data subject

- f. New rights for the data subject including the right to be forgotten and data portability, which allows them to receive their data in a structured and commonly used format so it can be easily transferred to another data controller.
- g. The timescales for dealing with a subject access request will be reduced to a calendar month and we will no longer be able to charge a fee (currently £10), unless the request is 'manifestly unfounded or excessive'.
- h. A requirement to notify the ICO of breaches within specified timescales, and to notify data subjects if there is a 'high risk' to their rights and freedoms, and
- i. Increased financial penalties can be imposed of the ICO for breaches



## Appendix 2

### GDPR – ICO 12 STEPS TO COMPLIANCE

Following is the Information Commissioner's Office (ICO) 12 GDPR 12 Steps to Compliance that will be used as a template for the Commissioner's Office GDPR Action Plan as more guidance becomes available.

<b>Step 01</b>	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.
<b>Step 02</b>	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.
<b>Step 03</b>	You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
<b>Step 04</b>	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
<b>Step 05</b>	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.
<b>Step 06</b>	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.
<b>Step 07</b>	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
<b>Step 08</b>	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.
<b>Step 09</b>	You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
<b>Step 10</b>	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.
<b>Step 11</b>	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.
<b>Step 12</b>	If your organisation operates in more than one EU member state (ie 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.

