Buckinghamshire & Milton Keynes Fire Authority

MEETING	Overview & Audit Committee
DATE OF MEETING	13 March 2019
OFFICER	Graham Britten, Director of Legal and Governance
LEAD MEMBER	Councillor Netta Glover
SUBJECT OF THE REPORT	**Implementation Progress of General Data Protection Regulation (GDPR)/Data Protection Act 2018 (DPA 2018)**
EXECUTIVE SUMMARY	The purpose of this paper is to advise Members of the progress made in implementing measures to facilitate compliance with GDPR. It also considers the possible impact that Brexit would have on the UK's GDRP arrangements in as much as they would affect the Authority's management of personal information. *The top level plan for monitoring GDPR compliance* within the Authority is to identify and create a Records Retention and Disposal / Information Assets Register (IAR). The IAR is a multi-purpose register identifying not only all the information assets i.e. anything that has value to the Authority that it owns and manages but also the sensitivity of these and any restrictions on processing. It identifies record types that hold Personally Identifiable Information (PII) and associated Records Of Processing Activities (ROPA)[1] which explain how, and with who, PII is shared. Where information has been identified as an asset, it is protectively marked to indicate that adequate technical and organisational measures[2] must be taken to protect it from unauthorised access and accidental or unlawful destruction. – The detailed information risks on the Information Management Risk Register will inform this process. None of the Authority's implementation plans would be negated through Brexit but additional measures may be required. *Further actions necessary to assist compliance* The IAR must be reviewed and maintained at a frequency relevant to the level of change it is subject to.

[1] Article 30 GDPR Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.
[2] Article. 32 GDPR "Security of processing".

	All areas of the Authority will hold "Clean-up" events to identify files and folders that have yet to be classified. Other plans and processes are being developed to increase the identification and security of information and support compliance to GDPR.
ACTION	Noting
RECOMMENDATIONS	1. That the GDPR implementation progress, the impact of Brexit, and associated risks be noted. 2. That periodic progress reports on implementation progress be received.
RISK MANAGEMENT	The Information Management Risk Register is a detailed listing of all information risks that have been identified and their treatments. It is frequently reviewed and includes all known risks associated with privacy legislation, best practice, and security. All new and amended processes, projects and other activities involving PII are subject to screening to identify the need for a full Data Protection Impact Assessment (DPIA) which considers the legality and risks associated with the activity. Information Asset Owners (IAOs) and Information Stewards are responsible for maintaining their schedules to ensure all types of information) that they hold, are recorded in the IAR and managed.
FINANCIAL IMPLICATIONS	There are no financial implications associated with this paper. Improvements in compliance may be triggered by changes in software, training and audit but these will be subject to cost / benefit evaluation and submitted for consideration through normal channels.
LEGAL IMPLICATIONS	The purpose of this paper is to consider the status of Authority compliance with GDPR and the impact of Brexit.
CONSISTENCY WITH THE PRINCIPLES OF THE DUTY TO COLLABORATE	All organisations will have to tailor compliance plans to fit their current state. However, complex issues are consulted on in forums for Data Protection Officers (DPOs) such as "The National Forum for Information Governance in the Fire and Rescue Service" and "Knowledge Hub." The Authority's DPO is a member of these forums and works collaboratively with other members to identify optimum solutions. The Authority is working collaboratively with the South East Regional Organised Crime Unit (SEROCU)[3] to develop and strengthen knowledge and awareness of cyber security risks. This supports article 32 GDPR

[3] SEROCU is part of the National ROCU network - partners of the National Cyber Security Centre (NCSC) – and they deliver holistic advice and training on cyber security.

	"Security of processing".
HEALTH AND SAFETY	The IAR supports compliance with health and safety through providing reassurance as to protective measures for people's personal information.
EQUALITY AND DIVERSITY	Implementation of processes to ensure compliance to privacy legislation and best practice are subject to a DPIA screening which reviews risks to all affected individuals. All processes that affect people are also subject to further impact assessment to consider equality, diversity or inclusion issues.
USE OF RESOURCES	**Communication with stakeholders** Everyone with a role in the management of Authority records has had the opportunity to assist in the development of processes to assist compliance to GDPR. New and revised procedures are communicated to all employees and published on the Authority intranet. Privacy statements are published on the Authority internet foe the general public to understand the use of their personal information. **The system of internal control** As the Authority is a data controller it must ensure that the DPO is involved properly and in a timely manner, in all issues which relate to the protection of personal information and must provide her with the necessary resources to perform her tasks. Therefore any weakness in compliance to GDPR will be reported to appropriate officer and member committees.
PROVENANCE SECTION & BACKGROUND PAPERS	**Background** Data Protection Act 1998 (DPA98) Data Protection Act 2018 (DPA18) General Data Protection Regulation (GDPR) Section 46 Freedom of Information Act 2000 2018 reform of EU data protection rules GDPR Facts Information Commissioner's Office (ICO) GPDR progress report to O & A (7 March 2018) Data Protection and Brexit (ICO)
APPENDICES	None
TIME REQUIRED	5 minutes
REPORT ORIGINATOR AND CONTACT	Gerry Barry gbarry@bucksfire.gov.uk

	01296 744442

1. Background

The GDPR, is a binding legislative act to harmonise data privacy laws across Europe, protect the personal information of individuals and make organisations more accountable. The GDPR came into effect on 25 May 2018 and must be applied in its entirety across the EU, replacing the Data Protection Directive 95/46/EU.

The DPA18 also came into effect on 25 May 2018. It sits alongside GDPR to update data protection laws in the UK whilst extending domestic data protection laws to areas not covered by the GDPR. – Such as National Security.

Along with these changes in privacy law the Information Commissioner (IC) has been given additional powers of regulation and enforcement and is able to levy higher fines on data controllers and processors for serious breaches. A maximum of £17m (€20m) or 4% of global turnover that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process information or violating the core of Privacy by Design concepts.

Fines come under two tiers and for lesser infringements, such as not having organisational records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting a DPIA, organisations can be fined up to £8.5m (€10 million), or 2% annual global turnover – whichever is higher.

The IC can bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

2. Implementation

To quote the IC, Elizabeth Denham:

"The creation of the Data Protection Act 2018 is not an end point, it's just the beginning, ….Organisations must continue to identify and address emerging privacy and security risks in the weeks, months and years beyond 2018".

However, whilst having achieved initial compliance to assist in addressing privacy issues is not an end point it is a requirement of the GDPR that should have been met by 25 May. There is evidence of non-compliance within some of the activities we undertake and the Authority must take urgent action to address this. Demonstrating strong information rights management is important to both customers and employees who need to understand why the information is collected and how it is handled.

2.1 Self-assessment

Prior to the GDPR coming into effect the Authority followed the ICO's 12 step programme and self-assessment tool to assess readiness. As limited guidance was available at that time, the Authority took a cautionary approach and assessed itself as having very few 'greens' (i.e. everything in place to support GDPR compliance). The ICO has since developed a number of self-assessment tools to indicate an organisation's implementation progress, and the Authority has recently undertaken a data controller compliance assessment and an information security assessment.

As a data controller we have assessed ourselves overall as 'amber' (additional actions necessary for full compliance). We have no red indicators, as everything has been actioned, even if not fully. Whilst we have made significant progress in auditing the information we hold, we have also assumed that we have not identified all of this information or that we have created sufficient information necessary to demonstrate compliance.

This includes records such as information Sharing Agreements (ISAs) and DPIAs. We are aware that where we have information sharing arrangements with partner agencies these agencies may not have reviewed and revised these arrangements to ensure that there is a legal basis for the processing of personal information, or undertaken a DPIA to determine if the risk involved in the sharing is acceptable.

For the information security assessment we have assessed ourselves as 'green' for our systems and processes albeit people issues do continue to be considered 'amber' as security behaviours will need to be fully embedded across all areas of the Authority and consistently rolled out to new starters/ new in post.

2.2 Training

We have rolled out training to employees, including more specialised training for those with significant roles in managing personal information. This is an ongoing process so that departments understand how GDPR directly applies to the records management processes they use.

With the growth in machine learning and "big data," privacy and security are converging, security training will be delivered by a Police Cyber Security Advisor from the South East Regional Organised Crime Unit (SEROCU).[4] The Authority is working collaboratively with SEROCU to develop and strengthen knowledge and awareness of cyber security risks. This supports article 32 GDPR "Security of processing".

2.3 Risk

The process of implementation of the GDPR principles demands a thorough approach to risk assessment. Under-estimating risk can result in significant monetary penalties and reputational damage to an organisation.

The Information Management Risk Register is a detailed list of risks to information held by the Authority. Many of these risks can be treated or mitigated concurrently rather than sequentially. Therefore the top level plan for monitoring GDPR compliance is to identify and create a register- Records Retention and Disposal / Information Assets Register (IAR) of all the types of records of information held by the Authority[5] and which of these are information assets (anything with a value to the Authority including all personal information).

Where information has been identified as an asset, it is protectively marked[6] to indicate that adequate technical and organisational measures[7] must be taken to protect it from unauthorised access and accidental or unlawful destruction. – The detailed information risks will inform this process.

This top-level register is the IAR and is sub-divided into departmental schedules which will identify all information held by the Authority and how this is managed in terms of:

- what information/ type of is collected?
- what are the sources of the information gathering?
- What is it used for?

[4] SEROCU is part of the National ROCU network - partners of the National Cyber Security Centre (NCSC) – and they deliver holistic advice and training on cyber security.
[5] Records retention and disposal – this will be used to identify all of the data held by the Authority / in authority systems
[6] Protective Marking – used to identify any sensitive information (whether personal or business sensitive) to ensure that adequate measures are taken to protect it.
[7] Article 32 GDPR

- how long we keep records for?
- what format are these recorded in (hardcopy, electronic – file format etc)
- where are they held?
- who is the IAO and Steward?
- who can access these records?
- What, if any, protective marking do they have?

Additionally, for personal information:

- is there a DPIA and is it being maintained?
- What is the basis for processing?
- who will we share this with?
- Is there a privacy statement in place?

This IAR collects information required to meet the article 30 requirement for keeping Records Of Processing Activity (ROPA) When complete, this register will provide visibility to the Authority of all its information holding, its information assets and the justification for holding this information (the basis for processing) together with the measures in place to protect this information.

2.4 Further actions necessary to assist compliance

The IAR must be reviewed and maintained at a frequency relevant to the level of change it is subject to as an audit of all the information held across the Authority.

To assist the development of the IAR all areas of the Authority need to review information held in personal and network drives, email files and in any other format that they hold information in – this may be other electronic systems and tools or hardcopy. It is thought that a number of files and folders have been created that have yet to be classified. Therefore, as part of the implementation plan "clean-up[8]" events are needed to remove unwanted information and reduce the likelihood of information assets being "hidden" within files and not identified resulting in information being held unlawfully.

"Clean-up" events will be scheduled for different area of the Authority to classify information and delete unwanted files and folders.

For electronic records, once this exercise is completed, any unclaimed records sitting in shared areas of network drives will be reviewed and, if they have no obvious value, deleted. For physical records (paper-based, CD-ROMS, photographs etc) it is the responsibility of the department to classify or destroy these.

To prevent additional electronic records being created on shared network files an exercise has been running for several months to prevent the creation or changes in access to files and folders all requests to ICT must reflect entries in the IAR or these requests will be refused. Additional processes will be developed for hardcopy and information stored on local drives.

[8] "Clean-up" events - these are used to reduce the amount of data held and may involve clearing down files that have been inactive for a prolonged period, are not described on the retention schedules and are therefore unlikely to be information assets (having a value to the Authority).

Hardcopy information that is held as "archived" for eventual destruction is held in an off-site professional archiving facility that protects the integrity of the information from damage and destruction and automatically deletes files at the appointed destruction date.

Other plans and processes are being developed to increase the identification and security of information.

3. Information rights and Brexit

(This section covers the issues that will or may affect the Authority if the UK exits the EU on or after the 29 March 2019. The basis on which the UK will leave the EU has still to be decided).

3.1 What will the UK data protection law be if we leave without a deal?

The GDPR is an EU Regulation and will no longer apply to the UK if we leave the EU without a withdrawal agreement i.e. a deal. The government intends to incorporate the GDPR into UK data protection law with the necessary changes to tailor its provisions for the UK (the "UK GDPR") and sit alongside the DPA18. As a consequence there will be little change to the core data protection principles, rights and obligations found in the GDPR.

The UK government intends that the UK GDPR will also apply to controllers and processors based outside the UK, where their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

The DPA18 supplements and tailors the GDPR within the UK, and will continue to apply. The ICO expects the government to use new legislation to make technical amendments to the GDPR so that it works in a UK-only context.

Although the GDPR will be absorbed into UK law at the point of exit, organisations that rely on the transfers of personal information between the UK and the European Economic Area (EEA) will be affected if the UK leaves the EU without a deal that provides for the continued flow of personal information. Whilst the Government has made clear its intention to permit information to flow from the UK to EEA countries, transfers of personal information from the EEA to the UK will be affected. However it is unlikely to affect Authority information transfers/ information sharing of personal information as it is thought that all of these occur in the UK. A review of current contracts that include the processing of personal information, is being undertaken and, if applicable, "Standard Contractual Clauses" with organisations outside the UK, will be considered.

Transfers on the basis of a European Commission adequacy[9] decision

The Government has stated its intention to seek adequacy decisions for the UK. An adequacy agreement would recognise the UK's data protection regime as equivalent to those in the EU, allow information flows from the EEA and avoid the need for organisations to adopt any specific measures.

[9] A decision adopted by the European Commission on the basis of Directive 95/46/EC, which establishes that a non-EU country ensures an adequate level of protection of personal data by reason of its domestic law or the international commitments it has entered into.

3.2 ICO and the European Data Protection Board (EDPB)

This section outlines the roles of the national supervisory authorities of EU and EEA states and the EDPB, the independent body established by the EU GDPR to ensure consistency within the EU as regards interpreting the law and taking regulatory action. It looks at the relationship of the national supervisory authorities among themselves and with the EDPB, both before and after exit date.

3.3 What is the role of the ICO and the EDPB?

The EU GDPR says each EU and EEA state must have an independent public authority responsible for monitoring the application of the EU GDPR. In the UK this is the ICO.

The EU GDPR also provides for the establishment of an independent body of the EU, the EDPB. The EDPB is made up of representatives from the supervisory authorities of each EU member state and each EEA state (without voting rights), and the European Data Protection Supervisor. The European Commission is able to participate in the activities of the EDPB but has no voting rights.

The EDPB's role is to ensure the consistent application of the EU GDPR across the EU. It does this by issuing guidelines and providing opinions, and (if there is a dispute between supervisory authorities) making decisions on the application of the EU GDPR, which are binding on those supervisory authorities.

On exit, the ICO will not be the regulator for any European-specific activities caught by the EU version of the GDPR and so will not be an EDPB member.

The ICO will continue to be the independent supervisory body regarding the UK's data protection legislation and the UK government will continue to work towards maintaining the close working relationships between the ICO and the EU supervisory authorities if the UK has left the EU.

3.4 Making plans for leaving the EU

The government plans to incorporate the GDPR into UK law if we leave[10]. Therefore, the best preparation for the future UK regime is to ensure that we are effectively complying with the GDPR now. The Authority will:

- continue to apply GDPR standards and follow current ICO guidance;
- review privacy information and internal documentation to identify any details that will need updating if the UK leaves the EU;
- keep up to date with the latest information and guidance;
- plan to implement adequate safeguards. - There may not be an adequacy decision in place by the 29 March 2019.

[10] Amendments to UK data protection law in the event the UK leaves the EU without a deal on 29 March 2019