Buckinghamshire & Milton Keynes Fire Authority

MEETING	Overview and Audit Committee
DATE OF MEETING	7 March 2018
OFFICER	Graham Britten, Director of Legal and Governance
LEAD MEMBER	Councillor Netta Glover
SUBJECT OF THE REPORT	**General Data Protection Regulation (GDPR) Progress**
EXECUTIVE SUMMARY	The purpose of this report is to advise Members of the progress being made to ensure that the requirements of the GDPR will be met. It gives an update of departmental progress from interviews with the Authority's GDPR lead officers (**Appendix A**) and the findings of an online self-assessment from the Information Commissioner's Office (ICO) (**Appendix B**) including the ICO's feedback and proposals for next steps and an explanation of the self-assessment marking for each question.
ACTION	Noting.
RECOMMENDATIONS	That the report be noted.
RISK MANAGEMENT	The Corporate Risk Register includes an information security "red" risk of failure to: a) comply with statutory or regulatory requirements; b) manage technology; c) manage organisational resources. This is a high-level risk that contains a number of discrete records management issues that may impact on GDPR compliance. The twelve steps that the Information Commissioner's Office (ICO) recommends that organisations take (set out for ease of reference at **Appendix A**) have been included in the Information Governance Risk Register. These also contain numerous discrete risks which are being actioned or recorded for future action. Where an individual risk or its risk treatments are thought to have privacy implications an Integrated Impact Assessment (IIA) will be completed and any equality and diversity, place, health or environmental issues will be investigated as part of this process.

FINANCIAL IMPLICATIONS	There are no financial implications directly associated with this report. However, a number of risk treatments will have associated costs – such as training. A contingency budget and reserves are held in the event of a serious information disclosure breach incident occurring.
LEGAL IMPLICATIONS	None arising from the recommendations. Failure to comply with the GDPR and the Data Protection Act 2018 (when they come into effect) may result in reputational and financial risk for the Authority.
CONSISTENCY WITH THE PRINCIPLES OF THE DUTY TO COLLABORATE	The potential to share GDPR implementation plans with other FRS and agencies has been considered but, to meet business needs, organisations are prioritising the necessary actions in differing priority order. However, Data Protection Officers (DPOs), including the National Forum for Information Governance in the Fire and Rescue Service, have set up discussion groups aiming to clarify the meaning and impact of changes the regulation brings and to share their understanding and initiatives in introducing these changes.
HEALTH AND SAFETY	No issues of legal compliance to health and safety policy have been identified.
EQUALITY AND DIVERSITY	See "Risk Management".
USE OF RESOURCES	***Communication with stakeholders*** Good records management enables the Authority to demonstrate transparency in the management of public information and security in the protection of personal information. A number of discussions have taken place with managers about the changes in legislation, what they will need to do, and the support they and their teams will need. This includes appropriate training. The Authority intranet has been used to publish an article to explain what the changes in data protection legislation will mean to employees. Procedures to support the regulatory changes and codes of practice are being written and consulted on and further articles are planned to explain how these may affect the way we work. ***The system of internal control*** Departments have been developing a list of all the

	types of records / information they hold, whether these include personal and / or special category[1] information, where it is stored and how long for, and who is responsible for managing it. – This is recorded in the "Records Retention and Disposal / Information Asset Register" on the intranet and is being further developed to ensure that access to personal and special category information is only granted by a person in a role responsible for these records to people who have a lawful basis for accessing (i.e. processing) this information. Departments and teams have to undertake specific activities to ensure GDPR compliance by the 25 May 2018, when the regulation comes into effect in the UK. Progress of these activities will be advised to the Data Protection Officer (the Information Governance and Compliance Manager) who will report through the internal meeting structure to provide assurance to the Senior Information Risk Owner (the Director of Legal and Governance) that regulatory requirements are being met and continue to do so over time.
PROVENANCE SECTION & BACKGROUND PAPERS	**Background** The GDPR is a Regulation intended to strengthen and unify data protection for individuals within the European Union (EU). It is an evolution of the EU's data rules, the Data Protection Directive (DPD) and aims to address many of the shortcomings in the DPD which were seen as: • outdated, in terms of technology and regulatory approach; • having unclear objectives and insufficient focus on detriment, risk and practical enforcement; • bureaucratic, burdensome and too prescriptive; • unclear about how much choice and control individuals should have; • having become a rigid control mechanism with effort being devoted to the artificial justification of otherwise unobjectionable processing; • becoming increasingly unclear in terms of scope; • having unrealistic international transfer rules against a backdrop of high-volume, globalised data flows; and • insufficient for 21st century themes for regulating the privacy and integrity of personal information which must involve greater emphasis on trust, confidence, transparency, governance and

[1] Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

	accountability: privacy and safeguarding information have become major reputational issues for businesses and governments*. * Extract of the review of the EU Data Protection Directive: (May 2009). Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now (Information Commissioner's Office) General Data Protection Regulation – European Commission Guide to the General Data Protection Regulation (GDPR) – Information Commissioner's Office Data Protection Bill
APPENDICES	Appendix A - GDPR Progress Report March 2018 Appendix B - ICO GDPR Checklist for Data Controllers February 2018 (as at 15 February 2018)
TIME REQUIRED	10 minutes.
REPORT ORIGINATOR AND CONTACT	Gerry Barry gbarry@bucksfire.gov.uk 01296 744442

Appendix A: GDPR Progress Report

1. Purpose

The purpose of this report is to advise Members of the progress being made to ensure that the requirements of the GDPR are being met. The Information Commissioner's Office (ICO) provides guidance to Data Protection Officers (DPOs) and others with day-to-day responsibility for data protection, to support the development of processes and procedures in readiness for the 25 May 2018 when the GDPR comes into effect in the UK. Core to this guidance is the ICO's: **Preparing for the GDPR: 12 steps to take now**

1 Awareness
Make sure that decision makers and key people in the 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
Document what personal data we hold, where it came from and who we share it with.

3 Communicating privacy information
Review privacy notices and plan for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
Check procedures to ensure they cover all the rights individuals have, including how we would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests
Update procedures and plan how we will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data
Identify the lawful basis for our processing activity, document it and update our privacy notice to explain

7 Consent
Review how we seek, record and manage consent and whether we need to make any changes. Refresh existing consents if they don't meet the GDPR standard.

8 Children
Do we need to put systems in place to verify individuals' ages and obtain parental or guardian consent for any data processing activity?

9 Data breaches
Make sure we have procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
Familiarise ourselves with the ICO's code of practice on Privacy Impact Assessments, guidance from the Article 29 Working Party, and how and when to implement them.

11 Data Protection Officers
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 our organisation operates in more than one EU member state we should determine our lead data protection supervisory authority.

2. What is the difference between the Data Protection Bill and the GDPR

The GDPR has direct effect across all EU member states and UK organisations will have to comply with this regulation when it comes into force on 25 May. However, GDPR member states have limited opportunities to make provisions for how it applies in their country and, in the UK, the Data Protection Bill is one element of this and needs to be read in conjunction with the GDPR. Parts of the Bill cover the ICO's duties, functions, powers and enforcement provision.

3. Accountability and Governance

The GDPR promotes accountability and governance. Whilst these are currently implicit requirements of data protection law, good practice tools - such as privacy impact assessments and privacy by design – under the "accountability principle[2]" these will, in certain circumstances, be a legal requirement. To demonstrate compliance we must implement appropriate technical and organisational measures. These may include privacy procedures, employee training, internal audits of processing activities, and the use of tools that meet the principles of data protection by design and by default, for example:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- the ongoing creation and improvement of security.

4. Training

GDPR is the most significant change to Data Protection in the last twenty years and it is important that all employees have a general understanding of the regulation and a more detailed understanding of how it impacts their working processes.

Some individuals with a day-to-day role in processing personal information have received GDPR training and are helping to cascade this learning to their teams. An external training organisation has also been engaged to provide on-site training to four large groups to enable faster organisational learning and reduce the risk of a breach of information security. The Data Protection Officer will continue to produce articles on the intranet to raise awareness and encourage employees to ask questions about what the changes will mean to their role so that role specific training can be delivered.

5. Procurement

Under the Data Protection Act we are required to have a written contract in place between the Authority (the Controller) and Processor,[3] outlining the security measures in place to protect personal information. The GDPR requires much more - it specifies the detailed terms the contract must contain with the aim of setting high standards and protecting the interests of data subjects. Both controllers and processors may now be liable to pay damages or be subject to significant fines or penalties.

Our procurement team have been working with colleagues across the Thames Valley (both Fire and Rescue Service and the Thames Valley Police) to develop standard

[2] Article 5(2) It is our responsibility to demonstrate that you comply with these accountancy principles.
[3] A controller is a natural or legal person or organisation which determines the purposes and means of processing personal data; and a processor is a natural or legal person or organisation which processes personal data on behalf of a controller.

contract terms and conditions for all contracts that will be put in place, or continue, from 25 May 2018. A letter will be sent to all our suppliers explaining the reasons for the changes and their new obligations.

6. Data-sharing and the lawful basis for processing

As the GDPR brings in new accountability and transparency requirements, we must clearly document the lawful basis for processing people's personal information. For contracts with suppliers providing data processing services on behalf of the Authority, this is part of the procurement team's review, but departments also share data with other organisations and are currently reviewing the agreements they have with them to ensure that we understand and record the lawful basis for sharing (processing) this personal information, inform people of this, and include it in our privacy notices.

7. Policies and Procedures

All departments are reviewing the policies and procedures that deal with personal information. Some of the changes necessary may not be clear until the Data Protection Bill becomes law, at which time the changes will be implemented and employees consulted to ensure they understand what these changes mean to them.

Appendix B: GDPR Checklist for Data Controllers

The ICO has produced an online self-assessment tool for data controllers to verify their progress against the requirements of the GDPR. This has been completed by the DPO and submitted online. An automated response, from the ICO advising actions that should (where the assessment is RED i.e. not yet implemented or planned) be taken or (where the assessment is AMBER i.e. partially implemented or planned) offering a number of options to choose from, is then received. – Where the options are already covered or being covered they have not been included.

ICO guidance and suggested actions are shown in black text with questions in black italics. Self-assessments and comments are shown in colour (see "overall rating" below).

Overall rating: As at 15 February our overall rating was amber

3	**Not yet implemented or planned**	**+ DPO comments**
17	**Partially implemented or planned**	**+ DPO comments**
7	**Successfully implemented**	**+ DPO comments**
2	**Not applicable**	**+ DPO comments**

Step 1 of 4: Lawfulness, fairness and transparency

1.1 Information you hold

You should organise an information audit across your business or within particular business areas. This will identify the data that you process and how it flows into, and out of your business. An information flow can include a transfer of information from one location to another. (For example, site to site).

1.1a Your business has conducted an information audit to map data flows.

AMBER: Partially implemented or planned

An initial audit has been undertaken by each department which has been documented. The DPO has assessed as partially implemented as not all data has been identified.

You should: Ensure this is conducted by someone with in-depth knowledge of your working practices; and identify and document any risks you have found, for example in a risk register.

1.2b Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.

AMBER: Partially implemented or planned

The origin of data is being identified. The arrangements in place for sharing this data and what it is used for are also being identified.

You should:

- maintain records of processing activities detailing what personal data you hold, where it came from, who you share it with and what you do with it. This will vary depending on the size of your business;

- ensure you have procedures to guide staff on how to manage information you hold.

1.2 Lawful bases for processing personal data

You need to identify lawful bases before you can process personal data and special categories of data. Your lawful bases for processing have an effect on individual's rights. For example, if you rely on someone's consent to process their data, they will have a stronger right to have their data deleted. It is important that you let individuals know how you intend to process their personal data and what your lawful bases are for doing so, for example in your privacy notice(s).

1.2a Your business has identified your lawful bases for processing and documented them.

AMBER: Partially implemented or planned

A number of Fire and Rescue Services (FRS) are working together to try to agree lawful bases for processing information for all the services we provide.

1.3 Consent

The GDPR sets a high standard for consent. Consent is not always needed and you should also assess whether another lawful bases is more appropriate. Consent means offering people genuine choice and control over how you use their data. You can build trust and enhance your business by using consent properly.

Your obligations don't end when you first get consent. You should continue to review consent as part of your ongoing relationship with individuals, not a one-off compliance box to tick and file away. Keep consent under review, and refresh it if anything changes. You should have a system or process to capture these reviews and record any changes.

If your current consent doesn't meet the GDPR's high standards or is poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

1.3b Your business has systems to record and manage ongoing consent.

AMBER: Partially implemented or planned

While systems are in place these may not be adequate under GDPR and are being reviewed.

You should:

- Keep a record of when and how you got consent from the individual.
- Keep a record of exactly what they are told at the time.
- Regularly review consent to check that the relationship, processing and the purposes have not changed.
- Have processes to refresh consent at appropriate intervals, including any parental consent.
- Make it easy for individuals to withdraw their consent at any time and publicise how to do so.
- Act on withdrawals of consent as soon as you can.
- Don't penalise individuals who wish to withdraw consent.

1.3a Your business has reviewed how you ask for and record consent.

AMBER: Partially implemented or planned

Process of consent is currently being reviewed.

You should:

- Check that consent is the most appropriate lawful bases for processing.
- Give granular options to allow individuals to consent separately to different types of processing wherever appropriate.
- Name your business and any specific third party organisations who will rely on this consent.
- Tell individuals they can withdraw consent at any time and how to do this.
- Ensure that individuals can refuse to consent without detriment.
- Don't make consent a precondition of service.

1.4 Consent to process children's personal data for online services

If you offer online services to children and you rely upon consent, only a child aged 13 or over will be able to provide their own consent.

1.4a If your business relies on consent to offer online services directly to children, you have systems in place to manage it.

Not applicable

The Authority does not offer online services for children.

1.5 Registration

1.5a Your business is currently registered with the Information Commissioner's Office.

GREEN: Successfully implemented

Until May 2018, you are still required to register with the ICO (unless an exemption applies).After May 2018 you need to pay the ICO a data protection fee.

Step 2 of 4: Individuals' rights

2.1 Right to be informed including privacy notices

Individuals need to know that their data is collected, why it is processed and who it is shared with. You should publish this information in your privacy notice on your website and within any forms or letters you send to individuals.

2.1a Your business has provided privacy notices to individuals.

Your business has made privacy notices readily available to individuals.

AMBER: Partially implemented or planned

Privacy notices have to be amended to ensure the basis for processing is clearly understood. There may be a need for additional notices.

You should:

Your privacy notice should:

- let individuals know who you are, why you are processing their data and who you share it with;
- be written in clear and plain language, particularly if addressed to a child;
- free of charge.

2.2 Communicate the processing of children's personal data

You must provide children with the same fair processing information as you give adults. It will be good practice to also explain the risks involved in the processing and the safeguards you have put in place.

2.2a If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.

Not applicable

The Authority does not offer online services for children. However, as part of the review of privacy notices the use of simple language will be considered.

2.3 Right of access

Individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.

You should provide a copy of the information free of charge. However, you can charge a 'reasonable fee' under certain circumstances.

2.3a Your business has a process to recognise and respond to individuals' requests to access their personal data.

GREEN: Successfully implemented.

However, all written procedures are under review and the Data Protection procedure will include the circumstances for charging.

2.4 Right to rectification and data quality

2.4a Your business has processes to ensure that the personal data you hold remains accurate and up to date.

AMBER: Partially implemented or planned

All written procedures are under review and the Data Protection procedure will include the circumstances for charging.

You should:

- implement procedures to allow individuals to challenge the accuracy of the information you hold about them and have it corrected if necessary;
- have procedures to inform any data processors (third parties) you have disclosed the information about the rectification where possible;
- conduct regular data quality reviews of systems and manual records you hold to ensure the information continues to be adequate for the purposes of processing; regularly review information to identify when you need to correct inaccurate records, remove irrelevant ones and update out-of-date ones; and

- promote and feedback any data quality trends to staff through ongoing awareness campaigns and internal training.

2.5 Right to erasure including retention and disposal

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary in relation to the purpose for which it was originally collected/processed;
- the individual withdraws consent;
- the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- it was unlawfully processed (ie otherwise in breach of the GDPR);
- it has to be erased in order to comply with a legal obligation; or
- it is processed in relation to the offer of information society services to a child.

However, the request does not give them an automatic right to have their data erased.

2.5a Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.

AMBER: Partially implemented or planned

The Authority has a written retention schedule in place that is under further development. See 1.1 and 1.2 above.

You should:

- have procedures in place which allow individuals to request the deletion or erasure of their information your business holds about them where there is no compelling reason for its continued processing;
- have procedures to inform any data processors (third parties) you have shared the information with about the request for erasure;
- have procedures to delete information from any back-up systems;

2.6 Right to restrict processing

Individuals have a right to block or restrict the processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future.

2.6a Your business has procedures to respond to an individual's request to restrict the processing of their personal data.

RED: Not yet implemented or planned

A process will be put in place to restrict the processing of personal data as permitted under the GDPR and under the new Data Protection Act (once these come into effect).

You should:

- review your procedures to determine where you may be required to restrict the processing of personal data;
- implement a process that will enable individuals to submit a request to you;

- have a process to act on an individual's request to block or restrict the processing of their personal data;
- have procedures to inform any data processors (third parties) you have shared the information with, if possible; and
- inform individuals when you decide to lift a restriction on processing.

2.7 Right of data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. They can receive personal data or move, copy or transfer that data from one business to another in a safe and secure way, without hindrance.

2.7a Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

RED: Not yet implemented or planned

A process will be put in place to facilitate the movement, copying of transfer of personal data, when requested by the individual.

You should:

- provide the personal data in a structured, commonly used and machine readable format;
- ensure that the medium in which the data is provided has appropriate technical measures in place to protect the data it contains; and
- ensure that the medium in which the data is provided allows individuals to move, copy or transfer that data easily from one organisation to another without hindrance.

2.8 Right to object

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); and processing for purposes of scientific/historical research and statistics. Individuals must have an objection on "grounds relating to his or her particular situation".

2.8a Your business has procedures to handle an individual's objection to the processing of their personal data.

RED: Not yet implemented or planned

A process will be put in place to stop or prevent the processing of personal data as permitted under the GDPR and under the new Data Protection Act (once these come into effect).

You should:

- review your processes and privacy notice(s) to ensure they inform individuals of their right to object "at the point of first communication". This information should be displayed or given clearly and separately from any other information;
- have processes in place to investigate an individual's objection to the processing of their personal data within the legitimate grounds outlined within the GDPR; and
- provide training or raise awareness amongst your staff to ensure they are able to recognise and respond (or know where to refer the request to) to an objection raised by an individual.

2.9 Rights related to automated decision making including profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

2.9a Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.

AMBER: Partially implemented or planned

The Authority's procurement contracts are currently being reviewed and as part of this the use of automated processing by any processor will be identified and documented. (See 3.2)

You should:

- identify whether any of your processing operations constitute automated decision making;
- ensure that within any automated processing or decision making you undertake individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it;
- implement appropriate safeguards when processing personal data for profiling purposes.

Step 3 of 4: Accountability and governance

3.1 Accountability

Documenting policies alone is often not enough to provide assurances that staff are adhering to the processes they cover. You should ensure that you have a process to monitor compliance to data protection and security policies. Measures that are detailed within the policies should be regularly tested and the results reported to senior management to provide assurances as to their continued effectiveness.

3.1a Your business has an appropriate data protection policy.

AMBER: Partially implemented or planned

The Data Protection procedure will be reviewed to reflect additional requirements of the GDPR and the revised Data Protection Act (once this comes into effect).

3.1b Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.

AMBER: Partially implemented or planned

Compliance process will be reviewed to reflect additional requirements of the GDPR and the revised Data Protection Act (once this comes into effect).

You should:

- establish a process to monitor compliance to the policies;
- regularly test the measures to provide assurances that they continue to be effective;
- ensure that responsibility for monitoring compliance with the policies is independent of the persons implementing the policy, to allow the monitoring to be unbiased; and
- report any results to senior management.

3.1c Your business provides data protection awareness training for all staff.

You should brief all staff handling personal data on their data protection responsibilities. It is good practice to provide awareness training on or shortly after appointment with updates at regular intervals or when required. Specialist training for staff with specific duties, such as, information security and database management and marketing, should also be considered.

The regular communication of key messages is equally important to help reinforce training and maintain awareness (for example intranet articles, circulars, team briefings and posters).

GREEN: Successfully implemented

Training is delivered to all employees as part of induction and is refreshed at least every two years. One to one and 'one to many' training for employees with specific roles in managing personal information is also given. A programme of GDPR training has been identified and will be implemented by the time GDPR comes into effect on 25 May.

3.2 Data processor contracts

Whenever you use a processor you need to have a written contract in place so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract. You are liable for your processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

3.2a Your business has a written contract with any data processors you use.

AMBER: Partially implemented or planned

The Authority's procurement contracts are currently being reviewed to ensure that the contract terms meet the additional requirements of the GDPR.

3.3 Information risks

You should set out how you (and any of your data processors) manage information risk. You need to have a senior staff member with responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets. Where you have identified information risks, you should have appropriate action plans in place to mitigate any risks that are not tolerated or terminated.

3.3a Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.

GREEN: Successfully implemented

In addition to the Corporate Risk Register there is an Information Management Risk Register managed by the DPO, detailing all identified information risks.

3.4 Data Protection by Design

Under the GDPR, you have a general obligation to implement appropriate technical and organisational measures to show that you have considered and integrated data protection into your processing activities. This is referred to as data protection by design and by default. You should adopt internal policies and implement measures which help

your organisation comply with the data protection principles – this could include data minimisation, pseudonymisation and transparency measures.

3.4a Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.

AMBER: Partially implemented or planned

All written procedures are under review and additional procedures may be required to reflect processes used to protect information.

You should:

- look to continually minimise the amount and type of data you collect, process and store, such as by undertaking regular information and internal process audits across appropriate areas of the business;
- create, review and improve your data security features and controls on an ongoing basis.

3.5 Data Protection Impact Assessments (DPIA)

DPIAs help you to identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.

3.5a Your business understands when you must conduct a DPIA and has processes in place to action this.

GREEN: Successfully implemented

Privacy Impact Assessments have been in place for some time and the process is under constant review to ensure that they are conducted early when a new process or project is being initiated. The process will be revised to change the name to DPIA as part of the Integrated Impact Assessment process.

3.5b Your business has a DPIA framework which links to your existing risk management and project management processes.

GREEN: Successfully implemented

Privacy Impact Assessments have been in place for some time and the process is under constant review to ensure that they are conducted early when a new process or project is being initiated. The process will be revised to change the name to DPIA as part of the Integrated Impact Assessment process.

3.6 Data Protection Officers

It is important to make sure that someone in your business, or an external data protection advisor, takes responsibility for data protection compliance. The DPO should work independently, report to the highest management level and have adequate resources to enable your organisation meet its GDPR obligations. The DPO's minimum tasks are to:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.6a Your business has nominated a data protection lead or (DPO).

GREEN: Successfully implemented

The Authority has had a DPO under the Data Protection Act 1998. The Information Governance and Compliance Manager is the DPO and is managing the process of GDPR implementation.

3.7 Management Responsibility

You should make sure that decision makers and key people in your business are aware of the requirements under the GDPR. Decision makers and key people should lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within your business, for data protection. They should help to drive awareness amongst all staff regarding the importance of exercising good data protection practices, take the lead when assessing any impacts to your business and encourage a privacy by design approach.

3.7a Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.

AMBER: Partially implemented or planned

This has been assessed as partial as, although decision makers and key people are largely aware of the requirements under the GDPR, to facilitate them in their supporting roles, additional training will be made available.

You should:

- ensure you have a policy framework and information governance strategy in place to support a positive data protection and security culture which has been endorsed by management;
- run regular general awareness campaigns across your business to educate staff on their data protection and security responsibilities and promote data protection and security awareness and compliance.

Step 4 of 4: Data security, international transfers and breaches

4.1 Security policy

You should process personal data in a manner that ensures appropriate security. You will need to assess the risks to the personal data you hold and choose security measures that are appropriate to your needs. Keeping your IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise. If you are processing personal data within your IT system(s) you need to recognise the risks involved and take appropriate technical measures to secure the data.

4.1a Your business has an information security policy supported by appropriate security measures.

AMBER: Partially implemented or planned

Information security is covered in a number of procedures but these will be reviewed to reflect additional requirements of the GDPR and the revised Data Protection Act (once these come into effect).

You should:

- ensure the policy covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management;
- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with your security policy
- implement periodic checks for compliance with policy, to give assurances that security controls are operational and effective; and
- deliver regular staff training on all areas within the information security policy.

4.2 International transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

4.2a Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.

AMBER: Partially implemented or planned

The Authority's procurement contracts are currently being reviewed and any appropriate arrangements for the processing of information will include overseas transfers.

4.3 Breach notification

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In all cases you must maintain records of personal data breaches.

You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

4.3a Your business has effective processes to identify, report, manage and resolve any personal data breaches.

AMBER: Partially implemented or planned

An internal breach reporting procedure will be developed which will have robust breach detection, investigation and internal reporting procedures in place which will facilitate decision-making as to the need to notify the relevant supervisory authority or the public.

You should:

- train staff how to recognise and report breaches;
- have a process to report breaches to the appropriate individuals as soon as staff become aware of them, and to investigate and implement recovery plans;
- put mechanisms in place to assess the likely risk to individuals and then, if necessary, notify individuals affected and report the breach to the ICO; and
- monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.