Information Governance Alliance

THE GENERAL DATA PROTECTION REGULATION: GUIDANCE ON ACCOUNTABILITY AND ORGANISATIONAL PRIORITIES

Information Governance Alliance IGA

Contents

1 Introduction 2

2 Accountability and demonstrating compliance 3

3 Outline action plan and resources 5

1 Introduction

The EU General Data Protection Regulation (GDPR) was approved in 2016 and will become directly applicable as law in the UK from 25th May 2018. The current Data Protection Bill, which will become the Data Protection Act 2018 (DPA18), fills in the gaps in the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit but the DPA18 will ensure continuity by putting in place the same data protection regime in UK law pre- and post-Brexit, equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

The Bill does not replicate all the provisions of the GDPR but cross-refers to the relevant provisions as appropriate. When the GDPR and DPA18 come into force, it will therefore be necessary to view the DPA18 and the GDPR side by side in order to see the complete picture of all the data protection legislation. This guidance note only refers to the relevant provisions of the GDPR and will therefore need to be updated to refer to the relevant provisions of all the data protection legislation, once the DPA18 comes into force. The guidance will also be kept up to date in light of any relevant guidance issued from Government and the Information Commissioner's Office (ICO).

A key provision of the GDPR is the principle of 'accountability'. Organisations (controllers) must be able to demonstrate compliance with the GDPR principles and in particular that they have appropriate technical and organisational measures in place.

The purpose of this guidance is to facilitate dialogue between Data Protection Officers (DPOs) and individuals who are accountable for organisational compliance in relation to information governance, i.e. the Board or equivalent. Note that the appointment of a DPO is a requirement for public authorities and/or organisations processing data concerning health on a large scale under the GDPR.

This document presents an overview of organisational priorities for achieving accountability in a public authority delivering health or social care. The outline action plan should be used in conjunction with **The IGA GDPR: Implementation Checklist** and other resources highlighted.

In this guidance

The word **must** is used in this document to indicate a legal requirement.

The word **should** is used to indicate that, in particular circumstances, there may exist valid reasons not to follow the guidance, but the full implications must be understood and carefully considered before choosing a different course.

The word **may** is used to indicate a discretionary activity for data controllers. This includes decisions where a permissive legal power is available. Under UK law, data controllers which are public authorities are additionally required to act in accordance with public law principles and to exercise their discretion reasonably and fairly, subject to judicial review, so again such organisations will need to understand the full implications and be able to justify their actions and decisions.

2 Accountability and demonstrating compliance

The GDPR includes a set of principles in Article 5(1) that are substantively the same or similar to the data protection principles in Schedule 1 to the Data Protection Act 1998 (DPA98). A significant addition [Article 5(2)] is the principle of 'accountability'. In addition to complying with the data protection principles in Article 5(1), organisations must also be able to demonstrate compliance. This accountability principle is reinforced by the specific responsibilities of 'the controller' under Article 24, to implement appropriate technical and organisational measures, including policies where proportionate in relation to processing activities.

The focus is on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties available for non-compliance. The key obligations supporting accountability that organisations must meet are:

- the appointment of a suitably experienced and appropriately resourced DPO – for public authorities
- the recording of all data processing activities with their legal bases and data retention periods
- ensuring that the DPO is involved at an early stage in all data protection matters, assesses the need for data protection impact assessment and monitors their effectiveness
- in particular conducting a data protection impact assessment where processing health data on a large scale
- implementing measures such as data minimisation, pseudonymisation etc. – to meet the principle of Data Protection by Design and Default (see the Information Commissioner's Office (ICO) Overview to the GDPR, section on accountability and governance)
- ensuring demonstrable compliance with enhanced requirements for transparency and fair processing, including notification of rights
- ensuring that data subjects' rights are respected;
  - provision of copies of personal data with accompanying supporting information free of charge
  - right to rectification
  - right to erasure (where engaged)
  - right to restrict processing
  - portability (where lawful basis for automated processing is consent)
  - right to object
  - right to object to automated decision making
- notification of personal data breaches to the Information Commissioner – unless the breach is unlikely to result in a risk to the rights and freedoms of the individual(s) in question

- communication of a personal data breach to the data subject where it is likely to result in a high risk to their rights and freedoms
- having technical and organisational measures in place that ensure and demonstrate that you comply, and in particular:
  - organisational policies and procedures in particular to address the points above
  - provision and monitoring of training.

Some of these requirements already accord with established good practice and organisations that are performing well in their information governance toolkit scores should have a good baseline from which to work.

3 Outline action plan and resources

GDPR REQUIREMENT	ACTION POINT	RESOURCES
1) Accountability – demonstrating compliance	**Establish a programme for GDPR compliance** • Appoint an appropriately skilled programme manager or lead. • Ensure appropriate resources are available to undertake the compliance plan. • Conduct a gap analysis: - DPA98 compliance against GDPR and Data Protection Act 2018. - focus on NHS Digital 12 point action plan - reference Information Governance Toolkit compliance evidence - operational impact on your organisation operation. • Record major gaps in your risk register and where possible, set out initial resourcing requirements. • Develop compliance plan based on gap analysis and review resource requirements. • Where appropriate commission independent review of compliance plan – to determine any missing areas relevant to your organisation. • Identify resources required after 25 May 2018, in particular to support the Data Protection Officer (DPO) role.	IGA – Changes to Data Protection legislation: why this matters to you (CEO briefing on GDPR and Accountability for Data Protection) NHS Digital – General Data Protection Regulation Implementation Checklist ICO – Overview of the GDPR IGA – What's new

GDPR REQUIREMENT	ACTION POINT	RESOURCES
2) Accountability – Management awareness	**Raise awareness with the highest level of management** • Highlight the benefits of getting compliance right - building trust with service users - safeguarding data privacy and security - avoiding fines - unlocking the benefits of information sharing. • Report on gap analysis compliance plan and resource requirements • Ensure the compliance plan has ownership, accountability and oversight at a senior level – to ensure that there is a mandate for organisational 'buy in' Many actions on the plan will be reliant upon members of staff from the organisation wider than the compliance team, e.g. • Changes to the information asset register • Updates to fair processing information • Policy development • Internal communications • Awareness and training	IGA – Changes to Data Protection legislation: why this matters to you (CEO briefing on GDPR and Accountability for Data Protection) ICO – Overview of the GDPR ICO – Accountability and governance ICO – Key areas to consider
3) Accountability – policy framework	**Revise information governance framework and policies** • Make a statement on organisational accountability addressing Article 5(2)	IGA – Changes to Data Protection legislation: why this matters to you (CEO briefing on GDPR and Accountability for Data Protection)

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Establish the DPO role • Establish arrangements for the DPO to provide regular reports to the highest management level • Your data protection impact assessment (DPIA) process should feed directly into your asset register to ensure that all new processing is accounted for and compliance demonstrated Art. 5 – Principles ((2) - 'accountability') Art. 24 – Responsibilities of the controller (2) – data protection policies	IGA – The General Data Protection Regulation – Guidance on the role of the Data Protection Officer ICO – Accountability and governance ICO – Key areas to consider
4) Information held	**Revise or establish information asset register** • Establish or update asset register to record the information required by Article. Use your information asset register as to record your processing activities • This will also inform your organisation of relevant information needed for action points: - 7 Lawful basis for processing personal data - 8 Consent - 10 Communicating privacy information - 11 Individuals' rights Although not specifically required by Article 30, the record should include the Article 6 and 9	ICO – Accountability and governance

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	conditions that apply as these are required by Articles 13/14 to be included in privacy notices and determine whether some of the rights are engaged. It would be beneficial to standardise purpose descriptions to enable a summary list to be included in privacy notices. Art. 30 – Records of processing activities Art. 6 – Lawfulness of processing Art. 9 – Processing of special categories of personal data	
5) Data Protection by Design and Data Protection Impact Assessments	**Revise policy and procedures on the introduction of new processes** • The DPO must be consulted as a matter of routine on the need for data protection impact assessment and other data protection matters. • Assurance of compliance must be addressed by default in the design and implementation of processing activities. • The requirement for DPIA is mandated within business change, programme management and procurement processes. • The need for DPIA is assessed prior to the introduction of all new processes – not just IT projects.	ICO – Privacy by Design ICO – Conducting privacy impact assessments code of practice ICO – Anonymisation: managing data protection risk code of practice

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Using your information asset inventory for reference, conduct an audit of current information systems to ensure that the principles are respected, in particular data minimisation, and measures such as pseudonymisation are implemented wherever possible. • Review access levels and access management procedures. Art. 25 – Data protection by design and default Art. 35 – Data protection impact assessment Art. 36 – Prior consultation	
6) Appoint a Data Protection Officer	**Appoint a DPO whose job description is compliant with GDPR requirements** • This should be one of the first steps you or your organisation undertakes. • This step is not reliant on drawing up an overarching compliance plan and can be done immediately. • Smaller organisations may wish to appoint an external or DPO that is a shared by several organisations. Arts. 37-39 – The data protection officer	IGA – The General Data Protection Regulation – Guidance on the role of the Data Protection Officer

GDPR REQUIREMENT	ACTION POINT	RESOURCES
7) Lawful basis for processing personal data including Consent	**Review processing activities and identify the legal bases** • Article 6 – for all processing • Article 9 – for special categories (previously 'sensitive personal data') • Using your information asset register, conduct a review of the legal bases for your processing of personal data and record the relevant lawful condition. This will involve: - All personal data: checking in relation to the DPA98 Schedule 2 condition currently relied upon that an equivalent or alternative condition in Article 6 GDPR can be relied upon, and - Sensitive personal data: checking in relation to the DPA98 schedule 3 condition currently relied upon that an equivalent or alternative condition in Article 9(2) GDPR can be relied upon In particular: • Where the current basis for processing is based on consent (i.e. paragraph 1 of Schedule 2), you should assess whether it meets the conditions for consent in Article 7 or otherwise consider alternatives – please refer to IGA Guidance on consent and lawful processing. N.B. consent for GDPR purposes is not the same	IGA – The General Data Protection Regulation – Guidance on lawful processing IGA – The General Data Protection Regulation – Guidance on consent **Notes:** • Art. 6(1)(e) '…public interest…or in the exercise of official authority…' is likely to be available to public authorities as an alternative to legitimate interests or consent. • Arts. 9(2)(h) '…health or social care…' is available as an alternative to consent for the processing of special categories data. Other conditions are available – please refer to the guidance highlighted above.

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	as consent for the purposes of common law duty of confidence, where implied consent will continue to suffice. • Identify processing for which 'legitimate interests are used as a basis for processing under DPA98 Schedule 2 (para 6) and, where this is not available under Article 6(f) because the processing is being carried out by a public authority in performance of its tasks, identify another condition from Article 6. Art. 6 – Lawfulness of processing Art. 9 – Processing of special categories of personal data	
8) Children	**Review and revise fair processing information provided to children** • Ensure that it is presented in appropriate language. **Identify any online services provided to children** • Ensure that the basis for lawful processing is 6(1)(e) '...public interest...or in the exercise of official authority...' • It is very unlikely that any health or social care organisations will offer any online services to children that fall into the scope of GDPR requirements • If such services do exist in your organisation you should check the fair processing	IGA – The General Data Protection Regulation – Guidance on consent ICO – Draft consent guidance **Notes:** Publicly funded health and social care online services such as Patient Online are not captured by Article 8 because: 1) they are not provided for remuneration as the definition requires; 2) Article 8 only applies where the condition for lawful processing under Article 6 is consent.

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	elements of the system, the verification elements of the system and have legal advice on whether the system is appropriate around issues of capacity.	
9) Communicating privacy information	**Review and revise transparency information** • Include the information required by Articles 13/14 and to meet the accessibility requirements of Article 12. • Where personal data are collected from the data subject your organisation must make sure that the information required by Article 13 is available at least by offering summary information and a web link to more detail. • Where personal data are not obtained from the subject, ensure that the information required by Article 14 is provided - within a reasonable period – no later than one calendar month, or - at the time of communication with the subject, or - at the latest when data are first disclosed to another recipient Unless the provision of the required information proves impossible or would involve a disproportionate effort, in which case you must make the information publicly available. Art. 12 – Transparency and modalities	ICO - Privacy notices, transparency and control: a code of practice on communicating privacy information to individuals

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	Art. 13 – Information to be provided where personal data are collected from the data subject Art. 14 – Information to be provided where personal data have not been obtained from the data subject	
10) Individuals' rights	**Establish policy and procedures to respect subjects' rights:** • Art. 16 – Right to rectification • Art. 17 – Right to erasure ('right to be forgotten') • Art. 18 – Right to restriction of processing • Art. 20 – Right to data portability • Art. 21 – Right to object • Art. 22 – Automated individual decision, making including profiling • Consider establishing consolidated procedure for responding to subjects' rights requests, including subject access: - These will need to take account of the circumstances when respective rights are available – i.e. where they are dependent on the legal bases that are being relied on. - The legal basis recorded in your information asset register will help with this • Identify any processing that involves automated processing including profiling (e.g. risk stratification):	IGA – The General Data Protection Regulation – Guidance on lawful processing IGA – The General Data Protection Regulation – Guidance on consent ICO – Draft consent guidance WP29 – Guidelines on the right to data portability **Notes:** • The right to data portability is **only available** where the basis for processing under Arts. 6 or 9 is consent/ explicit consent and the processing is automated. • The right to erasure is **not available** where the basis for processing under Art. 9 is 9(2)(h) '…health or social care…'

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- review procedures to ensure that no decision is taken with legal or significant effect, without the subject having an opportunity to object to such a decision. - ensure that the processing this right is publicised in fair processing materials. Arts. 15-22 – subjects' rights	
11) Subject access	**Revise subject access procedure** • Allow for charging only when manifestly unreasonable or repetitive. • Reflect timescale of one calendar month • Require provision of required supplementary information specified. • See action point 11 regarding consolidated subjects' rights procedures.	ICO – The right of access
12) Data Breaches		ICO – Breach notification