Information Governance Alliance

THE GENERAL DATA PROTECTION REGULATION: IMPLEMENTATION CHECKLIST

Information Governance Alliance IGA

Contents

1 Introduction

Purpose of document

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 of the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit – it is expected that the DPA18 will ensure continuity by putting in place the same data protection regime in be UK law pre- and post-Brexit, to create a data protection regime in the UK 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).

This document is based on 'Preparing for the General Data Protection Regulation 12 steps to take now' published by the Information Commissioner's Office.

This document is guidance that aims to support organisations to identify the work required for compliance with the GDPR by May 2018. **It does not constitute legal or other professional advice. Specific legal advice should be taken in regards to an organisation's own data protection law obligations.**

Objectives

The document complements IG Toolkit version 14.1 released 5 July 2017 by mapping existing IG Toolkit requirements to the GDPR and highlighting new obligations. The objective is to provide guidance on the steps organisations should consider taking to build on the work they will already have completed when undertaking annual IG Toolkit assessments. The checklist provides guidance on:

- The new legal obligations;
- Reviewing your existing data protection framework to identify gaps;
- Implementing measures that are necessary to comply with GDPR.

Target audience

This document is aimed at those working on the information governance agenda in organisations that are required to demonstrate IG assurance using the IG Toolkit.

The future

The redesigned IG Toolkit is scheduled to go live in April 2018. The current intention is for the new Tool to include GDPR and DPA18 requirements.

2 Implementation Checklist

GDPR REQUIREMENT	ACTION POINT	RESOURCES
1) Accountability Establish an implementation programme or a plan (depending on organisation size)	**a) Accountability – demonstrating compliance** **Establish a programme or plan for GDPR compliance** Establish a programme or plan for GDPR compliance The GDPR requires that organisations comply with the updated data protection principles, and additionally requires that they can demonstrate their compliance. A programme or structured plan for implementation (dependent on organisation size) can help your organisation prepare for GDPR. As part of the programme or plan, you should consider: • Appointing an appropriately skilled person to act as programme manager / lead (or equivalent implementation role). • Ensuring appropriate resources are available to support implementation. • Conducting a gap analysis: - DPA98 compliance against GDPR and DPA18. - Reviewing and revising the evidence used for your annual Information Governance Toolkit. - Considering the impact of GDPR and DPA18 on the way your organisation operates. • Recording major gaps in your risk register and where possible,	Senior roles - 101/114/120/130/140/144 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 IGA – What's new

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	setting out initial resourcing requirements. • Developing a compliance plan based on your gap analysis that covers: - Demonstrating compliance with the GDPR. - Keeping records of data processing activities **- see item 2**. - Addressing data protection in all data processing activities **- see item 3**. - Carrying out Data Protection Impact Assessments for high risk processing **- see item 3**. - Identifying resources required after 25 May 2018, in particular to support the Data Protection Officer (DPO) role, mandatory for all public authorities **- see item 4**. - Ensuring an appropriate legal basis for each type of processing **- see item 5**. - Identifying and reviewing processing for which consent was the lawful basis - see item 6. - Complying with more stringent transparency requirements **- see item 7**. - Where paid-for online services are offered to children ensuring their rights are appropriately managed **- see item 8**. - Supporting individuals to exercise their data protection rights **- see item 9**. - Discontinuing charging individuals for most subject access requests **- see item 10**.	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- Reporting specified security breaches to the ICO within 72 hours - **see item 11**. • Where appropriate commissioning an independent review of your compliance plan - to determine any missing areas relevant to your organisation.	
Compile a report for the Board/senior team to ensure there is corporate buy-in.	**b) Accountability – Management awareness** **Raise awareness with the highest level of management** As with any successful change process, implementation of GDPR will require organisational leaders to buy into and support the changes to organisational processes. To gain this support and any necessary resources, you could provide the highest level of management in your organisation (Board or equivalent team/ personnel) with a briefing that: • Highlights the benefits of getting compliance right, e.g. building trust with service users, protecting confidentiality and security, avoiding fines and unlocking the benefits of appropriate sharing. • Describes the necessary ownership, accountability and oversight at a senior level – to ensure that there is a mandate for organisational 'buy in'. • Includes the findings of your gap analysis and the necessary resource requirements.	Senior roles - 101/114/120/130/140/144 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

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Contains a summary of the actions (e.g. from your compliance plan) necessary for the organisation to comply with the changes GDPR brings.	
Start to raise awareness amongst staff and contractors	**c) Accountability – Staff and contractor awareness** **Inform your staff and contractors** Similarly, successful organisational compliance with GDPR will not be achievable unless your staff know what to do, and many actions on the plan will be reliant upon members of staff from the organisation wider than the compliance team/staff member, for example: • Making changes to the information asset register(s) - **item 2**. • Updating transparency information - **item 7**. • New policy development. • Creating and disseminating internal communications. • Revising awareness and training materials. You might want to consider: • Communicating significant changes to all staff, e.g. timely breach reporting, shorter timescales for meeting subject access requests (SARs). • Providing more detailed information to key staff, e.g.	Staff training and awareness- 112/117/123/134/143/148

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	information asset owners, those responsible for SARs, contracts staff, those likely to design and implement new ways of using data, communications staff. GDPR also imposes new obligations on your relationships with third party contractors / data processors, therefore it would be advisable to: • Inform all third party contractors about the implications of the GDPR for them; in particular of any new requirements they must meet, e.g. liabilities in respect of a breach by the data processor including liability for a breach by a sub-contractor. • Advise them that contracts are being reviewed/updated to ensure new requirements are included - see **item 3**.	Third party contracts - 110/116/122/132/142/146
Ensure your IG framework and IG policies are GDPR-compliant	**d) Accountability – Policy framework** **Revise information governance framework and policies** • Make a statement on organisational accountability setting out how the organisation is responsible for, and is able to demonstrate compliance with the data protection principles (Article 5). • Where required (mandatory for public authorities) establish the Data Protection Officer (DPO) role - see **item 4**.	IG Management Framework and policies - 101/105/114/115/120/121/ 130/131/140/141/144/145 IGA – Changes to Data Protection legislation: why this matters to you (CEO briefing on GDPR and Accountability for Data Protection) IGA – The General Data Protection Regulation – Guidance on the role of the Data Protection Officer ICO – Accountability and governance

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Establish arrangements for the DPO to provide regular reports to the highest management level. Make changes so that your data protection impact assessment (DPIA) process (item 3) feeds directly into your information asset register(s) (item 2) to ensure that all new processing is accounted for and compliance is demonstrated.	ICO – Key areas to consider
2) Keep records of data processing activities Ensure there is a comprehensive understanding of the information held and how it is used	**Revise or establish information asset register(s)** It is likely that you will have a head start on the GDPR requirement to keep records of data processing activities because compilation of information asset registers and data flow mapping are an intrinsic part of IG Toolkit compliance. It is therefore advised that you: • Ensure there is a comprehensive understanding of the personal information held by the organisation: - For example, if not already in place you could implement a process to regularly **review** existing information asset registers and update where necessary, e.g. does the asset still exist, has the information asset owner (IAO) changed, etc. • Ensure there is a comprehensive understanding of where/how personal information is received or sent and of the protection in place for transfers and receipt:	Protection of assets - 323/ 351/382 Secure transfer - 211/223/241/308/322/ 350/375 ICO – Accountability and governance

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- Similarly, if not already in place consider implementing a process to regularly **review** existing information flow mapping and updating it where necessary, e.g. has the recipient or transfer method changed. • Carry out an information audit to identify and document any information assets and flows not previously captured. • Ensure all assets are linked to an IAO. • Add your findings to a register or registers. **Note**: It is recommended that the Article 6 and 9 conditions (lawful basis) for each processing activity are added to the register(s) as each lawful basis for processing must be included in transparency information. • Lawful basis for processing personal data **- item 5**. • Consent **- item 6**. • Transparency requirements **- item 7**. • Individuals' rights **- item 9**.	
3) Data protection by design and default and DPIAs Use your findings from the information audit and flow mapping to ensure all current processing activities	**Revise policy and procedures on the introduction of new processes** Clear organisational direction and guidance for staff are key components for compliance, and you may already have policy documents in use that direct staff to privacy impact guidance. If so, you should:	Policies and controls - 105/115/121/131/141/145 Impact assessments - 210/215/237/256 ICO – Privacy by Design ICO – Conducting privacy impact assessments code of practice

GDPR REQUIREMENT	ACTION POINT	RESOURCES
have data protection compliant technical and organisational controls in place. Carry out DPIAs to ensure proposed processing activities are also protected.	• Update organisational policies including guidance for staff regarding data protection by design and default. • Ensure Data Protection Impact Assessments (DPIAs) are carried out where processing is likely to result in high risk to the rights and freedoms of individuals, in particular: - Automated processing. - Large scale processing of special categories data - which includes health and genetic data. - Systematic monitoring of a public area on a large scale. It is recommended that you review your privacy impact assessment documentation and update it to set out when it is necessary for staff to carry out a DPIA. Noting that the GDPR requires: • Seeking the advice of the organisation's DPO (**see item 4**) when carrying out a DPIA; and • Consulting the Information Commissioner's Office (ICO) where a DPIA indicates high risk to the rights and freedoms of individuals that cannot be sufficiently mitigated. It is also important that you communicate the requirement for a DPIA to those staff that are most likely to be responsible for managing new projects, introducing new systems and processes or devising new ways of working that require the use of personal information.	ICO – Anonymisation: managing data protection risk code of practice

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	For current and proposed processing, ensure that information is sent / to be sent by secure means and assets are protected by: • Reviewing existing data processing - see **item 2** above regarding information audit and mapping. • Ensuring that the current technical and organisational measures for data at rest and during transfer comply with DP principles. • Documenting your findings to demonstrate that you've considered how to integrate data protection compliance principles into your processing activities. • Addressing any gaps to ensure that data protection compliance is considered in both the design and operational phases of data processing, including when procuring or designing new IT systems.	Secure transfer - 211/223/241/308/322/350/375/ Protection of assets - 323/351/382
	Many of the contractual obligations necessary to comply with GDPR were already required under the DPA98 and/or NHS Standard Contracts - key components are set out in the guidance to the relevant IG Toolkit requirements. • However, GDPR introduces some key changes that must be incorporated within third party contracts to reflect the new obligations placed on data processors by Article 28. For example: - The data processor's liabilities in respect of a breach of GDPR.	Contracts with 3rd parties - 110/116/122/132/142/146

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- The data processor's liability for a breach by one of their sub-contractors. • You should consider how you will: - Review third party contracts. - Update contracts to reflect new responsibilities. - Address non-compliance by your third party contractors.	
	Article 4 states that pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. However, where personal data have undergone pseudonymisation, but can still be attributed to a natural person by the use of additional information held by the same organisation this should still be considered to be information on an identifiable natural person; and hence is still identifiable personal data under GDPR. • A pseudonymisation policy will help to ensure compliance with data minimisation obligations. • Consider other technical and organisational controls to support data minimisation - for example:	Pseudonymisation - 324/334/352/383 Technical and organisation controls - 300 series

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- Technical controls that prevent information from being inappropriately copied or downloaded. - Physical controls that prevent unauthorised access to locations. **Note:** Privacy by design and data minimisation has always been an implicit requirement of the data protection principles.	
4) Appoint a Data Protection Officer Review the responsibilities of the DPO and ensure an appropriately qualified person is assigned the role.	**Appoint a DPO whose job description is compliant with GDPR requirements** A Data Protection Officer (DPO) is mandatory if your organisation: • Is a public authority, or • Carries out regular and systematic monitoring of data subjects on a large scale; or • Carries out processing on a large scale of special categories or personal data relating to criminal convictions and offences. Where you are required to appoint a DPO it should be one of the first steps you or your organisation undertakes, it is not reliant on drawing up an overarching compliance plan and can be done immediately. A single DPO can be appointed by a group of data controllers provided that the DPO is easily accessible from each organisation. Public authorities may appoint the same DPO, taking into account their	Senior roles - 101/114/130/140/144 IGA – The General Data Protection Regulation – Guidance on the role of the Data Protection Officer Article 29 Working Group - Guidelines on Data Protection Officers

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	organisational structure and size. Smaller organisations may wish to appoint an external DPO or a DPO that is shared by several organisations. The DPO must be someone: • Of the right level of seniority - who has the requisite professional qualities and expert knowledge of data protection compliance. • That reports directly to the highest level of management. • Who is knowledgeable about the way the organisation works. • Who is involved in all material matters regarding data protection (including, following a security breach), and can operate independently of instruction and is not dismissed or penalised for performing their task. The DPO must be provided with sufficient resources so that they can meet their primary objective of ensuring organisational compliance; and undertake their responsibilities which include: • Advising their colleagues on compliance. • Training and awareness raising. • Monitoring compliance, and carrying out audits. • Providing advice regarding DPIAs. • Taking a risk based approach to compliance. • Being the main contact point with the ICO. • Maintaining their own expert knowledge of data protection.	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
5) Identify the lawful basis for processing Document a legal basis for each processing activity identified through audit and flow mapping	**Review processing activities and identify the legal bases** The new 'accountability principle' in the GDPR means that organisations need to be able to demonstrate compliance with the data protection principles. This will include being able to identify a legal basis for each use of personal data. GDPR Articles 6 and 9 contain the conditions for lawful processing, which can be compared with/ derived from the Schedule 2 and 3 conditions in the DPA98, and see the note below for additional requirements stemming from common law and administrative law. To comply, your organisation could build on the information audit and flow mapping findings, for example by: • **Using** your information asset register(s) (**item 2** above) to conduct a review of the legal bases for your processing of personal data. • Where the current basis for processing is based on consent you should consider whether the GDPR conditions in Article 7 are met or otherwise consider alternatives – please refer to IGA Guidance on consent and Guidance on lawful processing. • **Identifying** processing for which 'legitimate interests'; is used as a basis for processing under DPA98 Schedule 2 - and identifying a	Legal basis - 202/212/220/232/242/253 IGA – The General Data Protection Regulation – Guidance on lawful processing IGA – The General Data Protection Regulation – Guidance on consent

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	different legal basis within GDPR as public authorities will no longer be able to rely on legitimate interests as a basis for processing in the performance of their tasks - see **note e** below. • **Adding** your findings to the register / registers compiled for **item 2** above. • **Explaining** the legal basis for processing in your transparency information (**item 7** below). • Ensuring your subject access procedures for staff (**item 10** below) include a requirement to inform applicants of the legal basis for processing. **Note:** a) The likely legal bases (others are available) for processing most health and social care data are: - For processing personal data - **Article 6(1)(e)** - Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. - For processing special categories of personal data - **Article 9(2)(h)** (and DP Bill 2018) - Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services, carried	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	out by or under the supervision of health professional or social work professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. b) If relying on consent-based processing (see **item 6** below), people will have a stronger right to have their data erased. But note that the right to erasure does not apply to an individual's health or care record, or for public health or scientific research purposes. c) If the personal data are held in confidence an additional requirement is imposed over and above the GDPR conditions for processing i.e. there must be consent, statutory authority or a public interest justification that enables the common law duty of confidence (confidentiality) to be satisfied. N.B. Consent for these purposes may include implied consent, and is not to be assessed against the higher standard in GDPR, in particular Article 7. d) Bodies created in statute must additionally identify which of their statutory functions give them the authority to carry out the activity in question. e) Legitimate interests is no longer available to public authorities as a basis for processing in the	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	performance of their tasks, although it may be possible as a basis for processing carried out not in the performance of their official tasks – for example, the management of a car park permit database.	
6) Demonstrate compliance with consent requirements Update your communication materials and internal processes to support the obtaining of verifiable consent that is freely given, specific, informed and unambiguous	**Identify processing for which consent/explicit consent is used as a basis for processing under DPA98 Schedules 2/3** When consent is mentioned there are different interpretations of what that means depending on the context. For the purposes of implementing the GDPR, it is important to know that there are specific and clear instructions for consent if you need to rely on that for your legal basis for processing (although there are alternative legal bases offered by the GDPR - see item 5 above). However, consent is interpreted differently in the context of the common law. Here the requirements of satisfying consent differ from the GDPR requirement so for this reason both forms of consent are discussed below. **Common law confidentiality requirements are unaffected** The fact that consent may be obtained for confidentiality purposes does not mean that consent must be the lawful basis applied for the purposes of processing data in compliance	Consent - 202/212/220/232/242/253 IGA – The General Data Protection Regulation – Guidance on consent

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	with the GDPR. Well established national guidance on confidentiality remains applicable. GDPR requirements do not affect the common law duty of confidence (confidentiality). Health and social care professionals do not need to change their consent practices in order to comply with the GDPR, unless their organisation chooses to rely on consent as the basis for lawful processing under Article 6, or on explicit consent as the basis for processing special categories data under Article 9. Although the practice of relying on implied consent for processing data for direct care purposes will not comply with the higher GDPR standard of consent, this does not mean that implied consent ceases to be valid for confidentiality purposes. However, where an organisation does implement the higher GDPR-compliant consent, this will definitely meet confidentiality requirements. **Consent under the GDPR** In the limited circumstances that consent is the only/most appropriate condition to use as the lawful basis for processing – i.e. none of the other conditions in Articles 6 and 9 apply – organisations will need to consider the practical implications, such as ensuring the consent is valid for GDPR purposes.	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Firstly, consider whether you actually need to rely on consent - is another legal basis for processing more appropriate - see **item 5**. If you must rely on consent it must also be **verifiable** - Consider: • How will you request consent: - Are communication materials clear about what you are requesting consent for; - Do they provide separate consent options for each type of processing; - Do your staff have access to guidance so they can discuss with individuals in a clear and unambiguous way what you want to do with their personal information and the individual's consent options and rights - see **items 7-10** below. • How will you record consent choices, for example: - Is there is a common method to record consent; - Do your staff understand and adhere to the method - consider carrying out monitoring and random checks. • How often will you review consent, for example you could: - Set timescales (consider using electronic flags if feasible); - Identify who will carry out the review. • How can people withdraw their consent:	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	- Is there a process for withdrawal of consent; - Is it as easy as the way in which individuals gave their consent; - How will you ensure individuals are aware of the process.	
7) Comply with more stringent transparency requirements Update your communication materials to support people being properly informed.	**Revise and review fair processing information** GDPR contains stringent transparency requirements in Articles 13 and 14 to support people being properly informed of the use of their personal information and of their rights, before or at the time their information is collected. To aid compliance, it is recommended that you review and update your existing privacy/fair processing notices/communication materials to ensure they provide the following transparency information in a clear and concise manner: **1)** In the case of personal data collected from the data subject: • Identity and contact details of the data controller or their representative. • Contact details of the Data Protection Officer - see **item 4** above. • Why you want the information and what you will do with it. • The legal basis for each use of personal information - see **item 5**. • If relying on 'legitimate interests'	Informing individuals - 203/213/243/250/253 ICO - Privacy notices, transparency and control: a code of practice on communicating privacy information to individuals IGA – The General Data Protection Regulation – Guidance on lawful processing

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	for processing, what these legitimate interests are - see **note** below • Whether you will share the information and who with. • If information is to be shared with overseas recipients, the adequacy of their data protection regime and the safeguards in place to protect the information. • How long you will retain the information, or how you will decide the retention period. • The rights of access, rectification or erasure of personal data or restriction of processing and to object to processing as well as the right to data portability - see items **9-10** below. • The right to withdraw consent where this was the legal basis for the processing - see **item 6** above. • The right to complain to the ICO. • Whether individuals are obliged by statute or contract to provide the information. • Whether there are consequences for failure to provide the information. • Rights in relation to automated decision-making - the logic behind it, its significance and any consequences for the individual - see **item 9** regarding rights in relation to **decisions** made solely by automated processing. You may be able to meet this requirement by offering summary	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	information and a web link to more detail. **2)** Where the information is obtained from someone other than the subject of the data, transparency information must still be provided to the data subject, although what is required does slightly **differ** as below. • Identity and contact details of the data controller or their representative. • Contact details of the Data Protection Officer - see **item 4** above. • Why you want the information and what you will do with it. • The legal basis for each use of personal information - see **item 5**. • **The categories of personal information.** • If relying on 'legitimate interests' for processing, what these legitimate interests are - see **note** below. • Whether you will share the information and who with. • If information is to be shared with overseas recipients, the adequacy of their data protection regime and the safeguards in place to protect the information. • How long you will retain the information, or how you will decide the retention period. • The rights of access, rectification or erasure of personal data or restriction of processing and to object to processing as well as the right to data portability - see **items 9-10** below.	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• The right to withdraw consent where this was the legal basis for the processing - see **item 6** above. • The right to complain to the ICO. • **The source of the personal information.** • Rights in relation to automated decision-making - the logic behind it, its significance and any consequences for the individual - see **item 9** regarding rights in relation to **decisions** made solely by automated processing. As it may not be possible to provide transparency information to the data subject at the time the information is collected from someone else, GDPR makes provision for the notice to be provided at different times as follows: • Within a reasonable period after obtaining the information, but at the latest within one month; • If the information is to be used for communication with the data subject, at the latest at the time the first communication takes place; or If there is to be a disclosure to another recipient, at the latest when the information is first disclosed.Where it is impossible or disproportionate to provide the above notice within those timescales, then you must make the information publicly available. **Note:** Legitimate interests is no longer available to public authorities as a basis for processing in the	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	performance of their tasks, although it may be possible as a basis for processing carried out not in the performance of their official tasks – for example, the management of a car park permit database.	
8) Manage children's rights If you offer any paid-for online services directly to children, provide age-appropriate communication materials; and implement processes to enable you to demonstrate that you verified the child's age, and that consent was freely given, specific, informed and unambiguous.	**Identify any online services provided to children** If you offer any paid for online services to a child under 13 you will need a parent or guardian's consent in order to process their personal data lawfully; if the child is 13 or over, and the legal basis for the processing is consent, you will need to comply with the GDPR verifiable consent requirement (see **item 6** above). Whilst it is very unlikely that any health or social care organisations will offer any online services to children that fall within scope, you should identify whether any such services do exist in your organisation. If they do, you will need to: • Check the fair processing elements of the system. • Check the verification elements of the system and where necessary develop a process to verify the child's age. • Obtain legal advice on whether the system is appropriate around issues of capacity. • Ensure any materials aimed at children are presented in an	Informing individuals - 203/213/243/250/253 IGA – The General Data Protection Regulation – Guidance on consent ICO – Draft consent guidance Directive (EU) 2015/1535

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	appropriate language and written with children in mind. **Note:** a) Information society services are defined in Article 1 of Directive (EU) 2015/1535 - any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. b) This does **not** apply to providing children with preventative or counselling services, and publically funded health and social online services such as Patient Online are not within scope as they are not provided for remuneration. c) In addition, Gillick competence still applies for services provided to/ for children that are not part of 'information society services' e.g. preventative or counselling services.	
9) Support individuals' rights Update your communication materials and internal processes to support individuals' rights of rectification, erasure (the right to be forgotten), restriction, data portability and, objection to processing.	**Establish policy and procedures to respect subjects' rights** Individual rights must be respected and therefore your internal processes should support individuals to exercise those rights. You can assist individuals by ensuring your transparency materials (see **item 7** above) inform individuals in a clear manner that the following rights exist: • Rectification of inaccurate information.	Informing individuals - 203/213/243/250/253 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

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes. • Restriction of some processing. • Object to processing undertaken on some legal bases - see **note a** below. • Not to be subject to a decision made solely by automated processing in some circumstances - see **note b** below. • The right to data portability when processing is automated and based on consent - see **note c** below. • Subject access - see **item 10** below. Consider establishing a consolidated procedure for responding to all enquiries about rights which takes into account the circumstances when different rights are available, i.e. when they are dependent on the legal basis being relied on for the processing - see notes below. When developing a process for managing enquiries, consider: • Who will assess the application; • Who will inform the applicant about the outcome of their application; • Who will make agreed changes and how will changes be made; • What processes are in place if the applicant wishes to appeal a decision etc;	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• The timescales, e.g. rectification - reply within one month. **Note**: a) The right to **object** to processing applies only where processing is: - **For direct marketing** - here there is an absolute right to object, meaning that if the individual objects, the processing must stop. - **Based on legitimate interests or to performance of a task in the public interest/exercise of official authority** - this is a qualified right, processing must stop unless the organisation can demonstrate compelling legitimate grounds which outweigh the interests of the individual; or where the processing is for the establishment, exercise or defence of legal claims. - **For scientific/historical research/statistical purposes** - also a qualified right, the individual must demonstrate grounds relating to his/her particular situation, if they do so the processing must stop unless it is demonstrated that the processing is necessary for the performance of a task carried out for reasons of public interest. Individuals must be told about their right to object, clearly and separately, at the point you first	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	communicate with them. Further guidance on the right to object, and the interplay with the new national policy opt out, will be issued once the DPA18 is in force and the policy has been issued. b) Individuals have the right not to be subject to a **decision** based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her. You should identify any processing that involves automated processing including profiling (e.g. risk stratification): - 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 this right is publicised in transparency materials. c) The right to **portability** applies where processing is based on consent and is by automated means - individuals have the right to receive the data in a 'commonly used and machine readable format', you should consider: - Whether your systems can enable this - do you need to discuss with suppliers? - Developing a process for management of requests - who will manage requests; timescales, etc.	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
10) Manage subject access requests Update your internal processes to provide individuals with access to their personal information normally within one month and at no charge.	**Revise your subject access procedure** GDPR removes the requirement to pay a fee for most subject access requests although a reasonable fee for administrative costs may be charged if a request is manifestly unfounded or excessive, for example if it is repetitive. The time to comply with requests has been reduced from 40 days to 1 month. To aid compliance consider: • Consolidating your procedures for responding to all requests from individuals about their rights - see **item 9** above. • Making process changes so that you can meet the new 1 month timescale and remove the requirement to pay a fee for most requests. • Reviewing your records retention policy/policies to ensure you are retaining information appropriately and in accordance with good practice guidance such as the Records Management Code of Practice for Health and Social Care 2016. • Whether online access is an option if you receive a large amount of requests. • Updating your subject access procedures so that staff are directed to provide individuals with the information in **note a** below or a copy of your transparency information - see **item 7** above.	Subject access requests - 205/213/234/243 Confidentiality audits (informing individuals of who has accessed their records) - 206/216/221/235 ICO – The right of access IGA – Records Management Code of Practice for Health and Social Care 2016

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	• Providing advice for staff on manifestly unfounded or excessive requests and how they will be measured and handled. **Note:** a) Individuals making subject access requests are required to be provided with the information below, therefore it may make sense to provide them with your transparency information which should also contain this information (and more): - Why you have their information and what is being done with it. - The categories of personal information. - Whether you have or will share the information and who with. - If information has been shared or is to be shared with overseas recipients, including the safeguards in place to protect the information. - How long you will retain the information, or how you will decide the retention period. - The rights of rectification or erasure of personal data or restriction of processing and to object to processing - see **item 9** above. - The right to complain to the ICO. - The source of the personal information if not obtained from the data subject. - The existence of any automated decision-making	

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	or profiling - the logic behind it, its significance and any consequences for the individual . b) The exemptions under Data Protection Act modification orders have been incorporated within the Data Protection Bill 2018.	
11) Detect, report and investigate personal data breaches Update your internal processes to comply with the requirement to report specific breaches to the ICO within 72 hours of becoming aware of such a breach.	**Review breach notification policy and procedure** Incident management and reporting procedures are already required as part of the annual IG Toolkit assessment. GDPR places some specific breach reporting requirements on both data controllers and data processors. To comply, it is advised that you review existing incident management and reporting procedures, and consider: • How you will meet the requirement to notify personal data breaches to the ICO within 72 hours of becoming aware of the breach. • How you will communicate breaches to individuals affected where necessary. • What breach reporting structure is in place for your data processors - see **item 3**. **Note:** a) Health and care organisations are already required to assess the severity of personal data breaches relating to **NHS patient data** via the IG Incident Reporting Tool	Incident management - 302/320/333/349/365/373 Confidentiality audits (identifying unauthorised access or attempts) - 206/216/221/235 ICO – Breach notification

GDPR REQUIREMENT	ACTION POINT	RESOURCES
	within 24 hours of the breach becoming apparent. Breaches assessed using the Tool as severity level 2 or higher are automatically notified to the ICO. GDPR requires organisations to report specific breaches relating to all personal data (e.g. users of social care services, staff members), not just those relating to NHS patient data. b) The criteria and mechanism for reporting is currently being defined with the ICO. c) The Duty of Candour already requires that individuals are informed of breaches of their NHS patient data. d) Failure to report to the ICO when required could result in a fine, as well as a fine for the breach itself.	