Information Governance Alliance IGA

The General Data Protection Regulation

What's new

Contents

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 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 but 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).

The GDPR requires that organisations (controllers) that process personal data demonstrate compliance with its provisions. Part of this involves establishing and publishing a basis for lawful processing, and where relevant, a condition for processing special categories data.

Consent is one of a number of options to meet each of these requirements under the GDPR.

This guidance provides a reference tool to help understand the GDPR and its impact on health and social care organisations. It is designed to be accessible and useful both to professionals in the field of information governance and data protection, and others who may not have detailed knowledge of data protection, but need an understanding of the issues at a high level.

In particular, the purpose of the document is to support a dialogue between these two groups with a view to enabling collaboration in managing compliance. To achieve this, the document has two main sections that cover;

- similarities, changes and good practice becoming mandatory
- what's new in detail.

The similarities section not only highlights the headline changes but acts as an index to the detail section.

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 required to act in accordance with public law principles and to exercise their discretion reasonably and fairly, subject to judicial review. Hence public authorities will need to understand the full implications and be able to justify their actions and decisions.

Headline impacts

- New accountability requirement means organisations are now required, not only to comply with the new law, but to demonstrate that they comply with the new law. In particular, there is a requirement to keep records of data processing activities.
- Significantly increased penalties possible for *any* breach of the Regulation – not just data breaches.
- Legal requirement for personal data breach notification to the ICO within 72 hours where risk to data subjects.
- Removal of charges, in most cases, for providing copies of records to patients or staff who make a subject access request.
- Requirement to keep records of data processing activities.
- Appointment of data protection officer mandatory for all public authorities.
- Data protection impact assessment required for high risk processing.
- Data protection issues must be addressed in all information processes at an early stage.
- Specific requirements for transparency and the provision of information to data subjects about how their information is used.
- Tighter rules on consent where this is used as a basis for lawful processing (there are alternatives to consent).

What's similar and what's new

The table below summarises the key similarities between the Data Protection Act 1998 (DPA) and the GDPR, changes introduced, and current good practice that becomes a legal requirement under the GDPR. The provisions of the European Directive (95/46/EC) (the Directive) that underpins the DPA are also compared where this gives clarity.

Detail paragraph reference	What's similar	What's new
1. Principles relating to processing of personal data: Article 5	• The principles remain substantively the same or similar to those set out in Schedule 1 of the DPA.	• New principle of *'accountability'*. • Data controllers are responsible for and must be able to *demonstrate compliance* with the other principles.
2. Lawfulness of processing: Article 6	• The conditions available for lawful processing are again substantively the same or similar to those set out in Schedule 2 of the DPA.	• '*Legitimate interests*' is no longer available to public authorities as a basis for processing *in the performance of their tasks*. • Public authorities will be defined in the new Data Protection Act and will include statutory organisations such as NHS Trusts, and publically funded contractors such as GP Practices. • These organisations will need to use an alternative basis for their processing (most likely 6(1)(e) '*…in the public interest or the exercise of official authority…*'.)
3. Consent: Article 7 – Conditions for consent Article 4(11) – definition	• Consent is one way to comply with the GDPR, but it's not the only way, and in many health and social care contexts GDPR-compliant consent may not be possible. • To be valid under the GDPR consent must be *freely given, specific, informed and unambiguous*. (The DPA does not define consent). • *'Implied consent'* often assumed for direct care purposes for the purposes of the common law duty of confidence, meets neither the requirements of the DPA nor the GDPR, so there is no change in this respect.	• Consent must be given by a '*…statement or by a clear affirmative action…*' • Apart from this, the definition is similar to that of the Directive (the DPA has no definition). • Consent must be distinguishable from other matters in written declarations. • Controllers must be able to demonstrate that consent has been obtained *if they are using consent as their basis for lawful*. • Controllers must facilitate withdrawal of consent and it must be as easy to withdraw as to give consent.

Detail paragraph reference	What's similar	What's new
4. Conditions applicable to child's consent in relation to information society services: Article 8	• This is a new requirement. • Consent practices for common law purposes and the applicability of Gillick competence beyond the offer of *information* society services is unaffected.	• Parental consent is required for the processing of personal data where *information society services* are offered to a child under a specified age. • The default age is 16 but will be reduced to 13 in the UK by the DPA18. • Although this is a new requirement the impact on health and social care is minimal. • This provision has no applicability beyond the provision of these services, and the principle of Gillick competence is unaffected. • Publically-funded health and social care online services such as Patient Online are not affected. • Parental consent should not be necessary in the context of preventative or counselling services offered directly to a child.
5. Processing of special categories of personal data: Article 9	• Similar to Schedule 3, conditions for the processing of '*sensitive personal data*' in the DPA – includes the definition for '*special categories*'. • Health data is a special category of data. • Explicit consent is one of the conditions, but alternatives available cover health (a broad condition), public health and research.	• Genetic and biometric data are now classed as special categories of personal data. • Data relating to criminal convictions and offences are not a special category. • The condition 9(2)(h) '…*health or social care*…' differs from the equivalent condition at paragraph 8 of Schedule 3 to the DPA and the definition of 'medical purposes' in that Article 9(2)(h) expressly includes 'social care'. • There are separate conditions for public health, and archiving in the public interest, research or statistical purposes.
6. Processing of personal data relating to criminal convictions and offences: Article 10	• This is a new requirement in that the DPA does not differentiate the processing of this type of data from other sensitive personal data.	• This is not a special category of data under the GDPR. • The processing of such data by law enforcement agencies is covered by a separate Directive (2016/680) and will form part of UK law via a distinct section of the new DPA18. • As the crime directive does not cover the processing of such data by health and social care organisations, domestic legislation is required to extend the GDPR into the area of law enforcement or intelligence services activities. This will be achieved by the DPA18.

Detail paragraph reference	What's similar	What's new
7. Transparent information: Articles 12–14	• The DPA and GDPR require that specified information is provided to data subjects, currently implemented as fair processing notices or privacy notices.	• Accessibility and plain language are specifically required. • The categories of information which must be made available where the data are, or are not collected from the subject are more extensive than those in the DPA.
8. Right of access by the data subject: Article 15	• Under the DPA and GDPR subjects have the right to confirmation that their data is being processed, copies of information in an intelligible form, and further specified information in a specified timeframe. • The additional information specified is more extensive under the GDPR.	• No fee (in most cases). • New timescale (one calendar month). • More extensive information to be provided, in addition to the personal data.
9. Right to rectification: Article 16	• As with the DPA, the data controller must ensure that information is accurate. • There is a right to rectification under the DPA, but it is only enforceable by a court order. • 'Accurate' or 'inaccurate' are not defined in either the DPA or the GDPR.	• Data subjects have the right to require data controllers to rectify inaccurate personal data. • Under the DPA, this is a principle obligation, not a subject right other than by court order. • Organisations must reply to requests within one calendar month.
10. Right to erasure ('right to be forgotten'): Article 17	• Under the DPA erasure or destruction of inaccurate data can be required of a data controller, but only by a court order.	• The right is available for example where: – the basis for lawful processing is consent and the subject withdraws consent, and there is no other legal ground for processing – the subject objects and there are no overriding legitimate grounds – the personal data have been collected in relation to information society services – the personal data are no longer necessary for the purposes for which they were collected. • The right is not available in certain cases, for example where the conditions relied upon for processing are for the performance of a task carried out in the public interest or for reasons of public interest in the area of public health in accordance with Art. 9(2)(h) or(i).

Detail paragraph reference	What's similar	What's new
11. Right to restriction of processing: Article 18	• Under the DPA, blocking can be required of a data controller, but only by a court order.	• Data subjects have the right to require data controllers to restrict processing where: – accuracy is contested by the data subject – processing is unlawful and the subject opposes erasure – the data controller no longer needs the data, but the subject requires it to be kept for legal claims – the data subject has objected, pending verification of legitimate grounds.
12. Right to data portability: Article 20	• This is a new requirement.	• Data subjects have the right to receive personal data about them in a '*commonly used and machine readable format*'. • This right is only available where the processing is based on consent and the processing is automated.
13. Right to object: Article 21	• Under Section 10 of the DPA there is a right to serve a notice, requiring a data controller to cease or not to begin processing personal data on the ground that the processing is likely to cause substantial damage or distress and it is unwarranted. • In the case of direct marketing, the right to object is absolute. • The right to object does not apply where the individual has consented, the processing is necessary to comply with a legal obligation or to protect the vital interests of the individual.	• The controller must respect the objection unless they can demonstrate compelling legitimate grounds which override the individual's rights or for establishing, exercising or defending legal rights. • In the case of processing for scientific or historical research or statistical purposes pursuant to Article 89(1), the right to object need not be respected where the processing is necessary for the performance of a task carried out for reasons of public interest.

Detail paragraph reference	What's similar	What's new
14. Automated decision-making, including profiling: Article 22	• This right is available under both the DPA and GDPR, however under GDPR a written notice is no longer required. • Under both the DPA and the GDPR, the right is in relation to the decision, not the automated processing per se, which is subject to the right to object under the GDPR.	• Subjects have the right '*not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her*'. • This provision applies to the decision, not the execution of the automated processing to which the subject may object under Article 21. • Organisations involved in risk stratification or similar activities will need to make sure that subjects are given an opportunity to object before they are subject to decisions that meet the criteria.
15. Data protection by design and default: Article 25	Good Practice that becomes a legal requirement: • The Information Commissioner's Office (ICO) has published good practice guidance on privacy by design.	• The GDPR requires that organisations incorporate technical and organisational measures to minimise the risk to the rights and freedoms of subjects in both the design and operation of data processing activities. • In particular, only personal data that is necessary for each specific purpose of processing should be processed. • It also specifically mentions data minimisation and the application of, for example pseudonymisation to achieve this.
16. Article 30 – Records of processing activities	Good Practice that becomes a legal requirement: • Although a new obligation, health and social care organisations should already be maintaining information asset registers and information flow maps, as required by the information governance toolkit.	• The GDPR requires data controllers and processors to maintain records of their processing activities. • This supports an organisation's accountability and ability to demonstrate compliance, and supports information to incorporate in transparency information provided to subjects. • The information that must be included in these records is specified. • These obligations do not apply to an organisation employing less than 250 people unless other conditions are met, such as the processing carries a high risk to the rights and freedoms of a data subject, or includes special categories, for example health data.

Detail paragraph reference	What's similar	What's new
17. Data protection impact assessment: Article 35	Good Practice that becomes a legal requirement: ● The ICO has published good practice guidance on privacy by design.	● The GDPR makes it obligatory for a data protection impact assessment to be completed where the processing is likely to result in a high risk to the rights and freedoms of data subjects. ● This is required in particular for some automated processing on which decisions concerning individuals are based, processing on a large scale of special categories of data (for example health or genetic data) or systematic monitoring of a public area (for example CCTV). ● There is a list of essential elements for completion of the assessment. ● Where risks identified cannot be sufficiently addressed, the data controller must consult the ICO. ● The ICO is required to establish a list of the kind of processing activities that will require a DPIA and those which will not. Guidance is expected from the ICO on this.
18. The data protection officer: Articles 37–39	Good Practice that becomes a legal requirement: ● Most health and social care organisations will employ an individual with data protection responsibilities.	● Public authorities and organisations engaged in regular and systematic monitoring on a large scale or processing special categories data on a large scale must appoint a data protection officer (DPO). ● The designation, position and tasks of the DPO are defined. ● Key requirements are: – reporting the highest management level of the organisation – prompt involvement in all data protection issues – supported by appropriate resources – maintenance of expertise.
19. Pseudonymisation: Article 4(5)	Good Practice that becomes a legal requirement: ● The ICO has published good practice guidance on anonymisation.	● The process of pseudonymisation is explicitly defined in the Regulation. ● The fact that pseudonymised data may, depending how difficult it is to identify an individual, qualify as personal data does not mean that processing is prohibited; it means that processing needs to have an established lawful basis and otherwise comply with the GDPR.

Detail paragraph reference	What's similar	What's new
20. Administrative fines: Article 83	● The ICO continues to be able to fine, now within two distinct, strengthened and broader boundaries.	● This now applies to data processors as well as data controllers. ● Two levels of fines dependant on the type of infringement and severity of breach: – (1) fines of up to 10,000,000 Euros or 2% of total worldwide turnover – (2) fines of up to 20,000,000 Euros or 4% of total worldwide turnover.

What's new – the detail

What's new in the GDPR	Impact for health and social care organisations
1. Principles relating to processing of personal data: Article 5	
What's new ● The principle of '*accountability*' (Art. 5(2)). ● Data controllers are responsible for and must be able to demonstrate compliance with the other principles. ● Reinforced by Article 24 which requires data controllers to '*implement appropriate technical and organisational measures to ensure and to be able to demonstrate*' compliant processing. ● Technical and organisational measures apply to compliance in general not just to security. **What's similar** The principles remain substantively the same or similar as under the Directive and therefore the data protection principles set out in Schedule 1 of the DPA: (a) lawfulness, fairness and transparency (b) purpose limitation (c) data minimisation (d) accuracy (e) storage limitation (f) integrity and confidentiality.	**Impact** Organisations that are performing well in their information governance toolkit (IGT) scores should have a good baseline to work from. However, although IGT compliance evidence is a good starting point, the 2016/17 IGT requirements do not specifically or completely address GDPR requirements – the IGT is in the process of being updated. In particular, organisations will need to: ● review their IG management framework, with particular reference to the role of the Data Protection Officer (IGT 101, 105) ● enhance and update their information asset registers and information flows maps to record data processing activities with their lawful justification, data retention periods and the items listed in Article 30 (IGT 308, 323) ● review their policy on new processes routinely to conducting data protection impact assessments (AKA privacy impact assessments) where processing is likely to pose a high risk to individuals' rights and freedoms (IGT 210) ● ensure that policies and procedures are in place to incorporate data protection controls by default in the design and operation of information systems and processes (IGT 324) ● ensure demonstrable compliance with enhanced requirements for transparency and provision of information, including notification of and respect for subjects' rights (IGT 203). The points above are not exhaustive. Please refer to: ● The IGA has published good practice guidance on governance and organisational priorities. ● The IGA will publish a checklist for implementing general data protection regulations. ● ICO has published good practice guidance on accountability and governance.

What's new in the GDPR	Impact for health and social care organisations
2. Lawfulness of processing: Article 6	
What's new An important change is that '*legitimate interests*' (Art. 6 (f)) is no longer available to public authorities as a basis for processing *in the performance of their tasks*. Public authorities are to be defined under the DPA18 by reference to the definition of public authorities subject to the Freedom of Information Act 2000. These organisations will need to find another lawful basis for processing, for example: ● *6(1)(e) …necessary for the performance of a task carried out in the public interest or in the exercise of official authority.*…. Or: ● *6(1)(a) …consent…* (although see Section 3 regarding the disadvantages of using consent) An important consequence of the chosen applicable condition is that many of the subjects' rights are engaged, or not, on this basis. For more information, see subjects' right Sections 8-13 (pages 21-25). **What's similar** Organisations must be able to demonstrate that at least one of the conditions for lawful processing applies. The conditions available are largely the same as under the Directive and therefore similar to those set out in the DPA Schedule 2. Public authorities may use legitimate interests as a condition for processing data where this is not *in the performance of their tasks*.	**Impact** Organisations that are defined as public authorities in the Freedom of Information Act will be public authorities for the purposes of the GDPR. These will include, for example: ● NHS Trusts ● NHS Foundation Trusts ● Clinical Commissioning Groups ● NHS England ● Local Authorities ● NHS Digital ● National Institute for Health and Care Excellence ● Care Quality Commission ● NHS Improvement ● NHS Shared Business Services ● GP Practices ● Dentists ● Opticians ● Community Pharmacies ● Universities All of these organisations may be able to use… *6(1)(e) …necessary for the performance of a task carried out in the public interest or in the exercise of official authority.*…. …as the basis for lawful processing in the performance of their tasks. Public authorities may be able to use *6(1)(f) … legitimate interests*… as a basis for incidental processing, for example the management of a car park permit database, or system backup and recovery processes. Please refer to Section 3 (page 15) to understand the consequences of using consent as a lawful basis.

What's new in the GDPR	Impact for health and social care organisations
3. Consent: Article 7 – Conditions for consent; Article 4(11) – definition	
What's new The definition of consent has been enhanced (Art. 4(11)): ● Consent must be given by *a statement or by a clear affirmative action* ● Must be *freely given, specific, informed and unambiguous* Further requirements from Article 7 include: ● the proposed processing must be clearly distinguishable from other matters that are being consented to in written agreements ● requirement to facilitate withdrawal of consent – it must be as easy to withdraw as to give consent ● consent is not to be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment, for example if the provision of a service is conditional on consent to the processing of data ● requirement to be able to demonstrate that consent has been obtained ● where consent is used as a basis under 6(1)(a) or 9(2)(a) the following rights are available: – right to erasure (where the subject withdraws consent and there is no overriding legitimate grounds) – right to data portability. **What's similar** Under both the GDPR and the Directive, consent must be *freely given, specific, informed and signified*. Under both the Directive and the GDPR, explicit consent is a condition available for the processing of sensitive personal data / special categories. Neither the Directive nor the GDPR give a definition of explicit consent. 'Implied consent' does not meet the requirements of the DPA or the GDPR, but will continue to be available for the purposes of the common law duty of confidence, so there is no change in this respect.	**Impact** There are challenges in ensuring that consent is valid, recorded, and that withdrawal of consent is respected. Furthermore, where consent is used as a basis, there will be a requirement to implement procedures and technical solutions to respond to the subjects' requests to rights that become engaged. For these reasons organisations should consider alternatives to consent as their basis for lawful processing and special categories condition, for example: ● *6(1)(e) …public interest…exercise of official authority…* and ● *9(2)(h) …health or social care…* for special categories. It is important to ensure that where consent is used as a basis: ● all of the criteria for valid consent are met ● procedures are in place to record or otherwise evidence consent ● procedures are in place to respect the rights that become engaged. Where consent is used as a basis under 6(1)(a) or 9(2)(a) the following rights are available: ● right to erasure (Art. 17 – where the subject withdraws consent and there is no overriding legitimate grounds) ● right to data portability. It is important to highlight: ● the right to erasure does not apply where special categories (for example health information) are processed for health / social care or public health purposes (Arts. 9(2)(h) or (i)) ● the right to data portability is not available when processing is carried out in the public interest or in the exercise of official authority (Art. 20(4) referencing Art. 6(1)(e)).

What's new in the GDPR	Impact for health and social care organisations
3. Consent: Article 7 – Conditions for consent; Article 4(11) – definition (continued)	
	In relation to consent obtained for the purposes of complying with the common law duty of confidence: ● where organisations do not use consent as their basis for lawful processing for GDPR purposes, there is no need to modify consent practices that meet common law requirements to comply with the GDPR definition and conditions for consent ● organisations should continue to obtain consent that is valid for common law purposes, or ensure they have another legal basis. It is common practice for *'implied consent'* to be assumed as a basis for sharing information for direct care purposes. Strictly implied consent can only be assumed where the sharing is within the '*reasonable expectation*', of the patient, this approach is valid for confidentiality purposes (common law duty of confidence), provided the patient is appropriately informed, or the proposed activity is obvious or can be reasonably expected. However, this meets neither the requirements for consent in the DPA (as defined in Directive 95/46/EC) nor the GDPR. The validity of implied consent will depend upon the knowledge or expectation of the subject of the proposed activity. Compliance with fair processing and transparency requirements in Articles 12–14 will go a long way to supporting this knowledge and reasonable expectation. So although common law and GDPR requirements operate separately, in this context they are complementary, even though consent practices for common law purposes may not meet GDPR requirements. Please refer to IGA's guidance on consent.

What's new in the GDPR	Impact for health and social care organisations
4. Conditions applicable to child's consent in relation to information society services – Article 8	
What's new Parental consent is required for the offer of *information society services* to children aged under a specified age; the default age of 16 is to be reduced in the UK to 13 under the DPA18, the lowest age allowed by the GDPR. ● '*Information society services*' includes most internet services provided at the user's request, *normally for remuneration* – see ICO's guidance on key areas to consider. ● A further criterion is that they constitute an *economic activity*. ● The provision only applies where the basis for processing is consent (Art. 6(1)(a)). ● Parental consent should not be necessary in the context of preventative or counselling services offered directly to a child (Recital 38). **What's similar** This is a new requirement.	**Impact** Although this is a new requirement the impact on health and social care is minimal. Publically-funded health or social care online services are out of scope. ● Consent practices for common law purposes and the applicability of Gillick competence beyond the offer of information society services are unaffected. ● As the definition of *information society services* includes that they are provided *normally for remuneration*, this does not capture publically funded health or social care online services, for example Patient Online. ● Furthermore, as this provision only applies where the basis for lawful processing is consent, where organisations apply 6(1)(e) '…*in the public interest or the exercise of official authority*…' the service is out of scope on this criterion. ● Preventative or counselling services offered directly to a child are also out of scope. Please refer to IGA's guidance on consent.

What's new in the GDPR	Impact for health and social care organisations
5. Processing of special categories of personal data: Article 9; Article 4(13–15) definitions	
What's new Article 9 defines *special categories* of personal data, and lists conditions that are available to lift the prohibition on processing of this data. Special categories are analogous to sensitive personal data under the DPA, with the conditions having equivalent function to those of Schedule 3. ● Genetic data and biometric data are added to the list of special categories (Arts. 4(13, 14)). ● The definition of health data is more specific than that of the DPA: *'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status' (Art. 4(15)).* ● Data relating to criminal convictions and offences is ***not*** a special category (see note on Article 10). ● Explicit consent is one of the conditions available for processing special categories data, but as with the DPA there are alternatives. ● The condition including medical purposes (Art. 9(2)(h)) is broader than the equivalent in the DPA to the extent that it expressly includes social care, but narrower to the extent that it does not expressly include medical research. ● Public Health gets a separate, specific condition for increased clarity (Art. 9(2)(i)). ● Processing necessary for archiving in the public interest, research or statistical purposes (Art. 9(2)(j)) is permitted subject to safeguards set out in Article 89(1), (for example data minimisation and pseudonymisation where the purposes can be fulfilled). Such processing must have a basis in UK law.	**Impact** Health and social care providers and commissioners will be able to use Article 9(2)(h) '…*health or social care*…'. ● The condition relating to health and social care (Art. 9(2)(h)) is similar to but more extensive than 'medical purposes' under the DPA to the extent of expressly including social care. ● As social care is included in Article 9(2)(h), uncertainty over the applicability of 'medical purposes' is removed. ● However as medical research is no longer expressly included, it will be necessary to rely on another condition such as Article 9(2)(j), processing for 'scientific or historical research purposes' or otherwise find an alternative condition, for example explicit consent. ● Whilst genetic data is a new special category, and member states may legislate specifically on this, there is no intention at present to do so. ● Organisations will need to ensure that they understand the application of the legislation to the categories of staff data that is held. For Article 9(2)(h) to apply, safeguards required by Article 9(3) must be met, in particular that: ● '…*data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy*…' ● '…*or a person subject to an obligation of secrecy under Union or Member State Law*…' The obligation of secrecy will be met by the common law duty of confidence. The DPA18 will clarify this. Registered health and social care will be covered, also non-registered staff such as auxiliary nurses, trainee social workers, and others with a duty of confidence such as patient administration and hospital porters (transporting records being 'processing'), also staff in arms' length bodies whose statutory function requires the processing of personal data. Similarly, organisations engaged in public health or research activities will be able to apply a condition other than Article 9(2)(a) '*explicit consent*'.

What's new in the GDPR	Impact for health and social care organisations
5. Processing of special categories of personal data: Article 9; Article 4(13-15) definitions (continued)	
What's similar Health data remains a special category of data (known as sensitive personal data in the DPA), meaning processing of this type of data requires that specified conditions are met. ● Explicit consent is one of the conditions available for processing special categories data, but there are alternatives, for example: – *'…necessary…in the field of employment…'* (Art. 9(2)(b)) – *'…vital interests and subject incapable of consenting…'* (Art. 9(2)(c)) – *'…health or social care…'* (Art. 9(2)(h)).	
6. Processing of personal data relating to criminal convictions and offences: Article 10	
What's new Personal data relating to criminal convictions and offences is not a special category under the GDPR. The processing of such data by law enforcement agencies is covered by a separate Directive (2016/680) and will form part of UK law via a distinct part of the new DPA18. **What's similar** This is a new requirement.	**Impact** As the crime directive does not cover the processing of such data by other organisation types, domestic legislation is required to support such processing, for example: ● pre-employment checks on criminal convictions ● counter-fraud ● regulatory purposes, for example in deciding whether to register someone to carry out a health or social care service ● serious case review ● investigation of mental health related or domestic homicide ● multidisciplinary reviews ● in the context of safeguarding boards ● offender management, for example someone is being released from prison and needs mental health input ● risk management and public protection in care settings ● violent patient or service user marker schemes. The new Data Protection Act will provide a basis for these activities, using the flexibility available in Article 10.

What's new in the GDPR	Impact for health and social care organisations
7. Transparency and fair processing: Articles 12–14	
What's new The GDPR is much more prescriptive on the requirements for information to be provided to data subjects, with increased emphasis on transparency. The current ICO guidance on privacy notices gives an indication of what is required. The requirements for responses to requests in relation to subjects' rights are specified. There is no longer a requirement for notification / registration with the ICO in the same way, although the Digital Economy Act and DPA18 will enable some form of equivalent scheme by allowing secondary legislation to be introduced on fees payable by data controllers to the ICO. Article 12 establishes the responsibilities of the data controller to provide information to data subjects relating to processing (fair processing), and in response to requests relating to subjects' rights (for example, subject access): ● Information should be '…*in a concise, transparent, intelligible, easily accessible form, using clear and plain language, in particular for any information addressed to a child*…' Articles 13 and 14 go on to list information that must be provided to subjects where personal data are, or are not collected from the data subject respectively. These are much more extensive and specific than those in the DPA. The only exemption from the provision of information where the data are collected for the subject is that the subject already has the information. Where the data has not been collected from the subject there is more leeway – if the provision of the information *proves impossible* or would involve *disproportionate effort*, with further qualification. However where this applies the controller is required to protect subjects' rights and freedoms, in particular, by making information publicly available.	**Impact** Organisations will need to make sure that their privacy notices and other measures for the provision of fair processing information comply with: ● the transparency requirement in Article 12 ● the specific requirements for information to be provided in Articles 13 and 14. Provider organisations and others that collect personal data directly from the data subject will face the challenge of ensuring that the information listed in Article 13 is provided to the subject at the time when the data are collected. ● The DPA allows for the information to be provided or made readily available '*so far as practicable*' as soon as possible afterwards. ● This flexibility is not available under the GDPR. ● The only exemption is where the subject already has the information. Commissioners and other organisations that process personal data that they have not obtained from the data subject, particularly for secondary uses will need to: ● assess and document whether the provision of information directly to subjects is *impossible* or would require *disproportionate effort* (Art. 14(5)(b)) ● if applying this exemption, ensure that their fair processing web pages meet the requirements of Article 14.

What's new in the GDPR	Impact for health and social care organisations
7. Transparency and fair processing: Articles 12–14 (continued)	
What's similar Article 5(1)(a) says that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. As currently, certain restrictions are available to these rights. Article 23 allows for derogation, for example in: ● (1)(d) *'the prevention, investigation, detection or protection of criminal offences'* ● (1)(e) *'…general public interest…public health and social security.'* Such measures must be '*necessary and proportionate…in a democratic society*'. (Art. 23(1)).	
8. Right of access by the data subject: Article 15	
What's new ● Information must normally be provided free of charge in response to a subject access request. ● A charge may be made if the request is '*manifestly unfounded or excessive*' as per Article 12. ● There may be a reasonable charge for further copies requested. ● The timescale for responding to requests has been reduced from 40 days to one calendar month, subject to the ability to extend this time (Art. 12(3)) by a maximum of two calendar months. ● More extensive information to be provided, in addition to the personal data. **What's similar** Subject access rights under the GDPR largely remain similar to the existing subject access rights under DPA, i.e. right to obtain, confirmation that their data is being processed, access to their personal data, and other specified information The exemptions from subject access will be retained under the DPA as permitted under Article 23.	**Impact** Organisations will need to: ● make budgetary adjustment to accommodate free responses to subject access requests ● revise their subject access policy and procedures: – removal of fees in most cases – circumstances where a fee may be charged – provision of supplementary information as specified in Article 15. ● publish their procedures in their transparency notices. For organisations that are complying with the good practice requirement to respond within 21 days, there will be little impact in this legal reduction. The provisions of the subject access modification orders are expected to be incorporated within the DPA18, for example: ● exemption from provision of information where this '.. *would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person*' ● requirement to consult the '*appropriate health professional*' ● exemption from non-disclosure of the identities of health professionals who have either contributed to the record or the care of the subject.

What's new in the GDPR	Impact for health and social care organisations
9. Right to rectification: Article 16	
What's new ● Data subjects have the right to require data controllers to rectify inaccurate personal data. ● Organisations must reply to requests within one calendar month (Art. 12) subject to the ability to extend this time (Art. 12(3)) by a maximum of two calendar months. **What's similar** ● Under the DPA, organisations should make sure that data are accurate (Principle 4). ● Courts may require rectification of inaccurate data. ● *'Inaccurate'* is not defined. ● The ICO is of the view that opinions are by nature accurate to the person holding the opinion, so a professional opinion is defined as accurate.	**Impact** Organisations will need to: ● review or establish procedures to respond to requests for inaccurate personal data and within the timeframe stipulated (one calendar month) ● review current procedures for inserting notes into disputed records, rather than permanently amending data ● publish their procedures in their privacy notices.

What's new in the GDPR	Impact for health and social care organisations
10. Right to erasure ('right to be forgotten'): Article 17	
What's new The right to erasure applies in specified circumstances, for example: ● where processing is based on consent (Arts. 6(1)(a) or 9(2)(a)), the subject withdraws consent, and there is no other legal grounds for processing ● the data subject objects and there are no overriding legitimate grounds for processing (see conditions for right to object) ● the personal data have been collected in relation to information society services (see Article 8) ● where the personal data are no longer necessary for the purposes for which they were collected ● where the personal data have been unlawfully processed. **What's similar** ● Under the DPA, erasure can be required of a data controller, but only by a court order.	**Impact** Given the fact that systems incorporate amendment history, audit trails, system backups and, for example, mark patients' records as 'deducted' rather than deleting them, there will be some difficulty achieving full and permanent erasure. However this right does not apply where the basis for processing is necessary, for example: ● compliance with a legal obligation (Art. 17(3)(a)) or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ● health or social care purposes (Art. 9(2)(h)) supported by compliance with Article 9(3) (see above) ● reasons of public interest in the area of public health (Art. 9(2)(i)) ● Article 89(1) (Art. 9(2)(j)) – archiving, research, or statistical purposes where the objectives of that processing seriously impaired or rendered impossible if the right applied. There should be little impact for organisations provided consent is not used as a basis for processing under Articles 6 or 9.

What's new in the GDPR	Impact for health and social care organisations
11. Right to restriction of processing: Article 18	
What's new Data subjects have the right to require data controllers to restrict processing where: ● accuracy is contested by the data subject ● processing is unlawful and the subject opposes erasure ● the data controller no longer needs the data, but the subject requires it to be kept for legal claims ● the data subject has objected, pending verification of legitimate grounds. **What's similar** Under the DPA, blocking can be required of a data controller, but only by a court order.	**Impact** Organisations will need to: ● establish procedures to receive and assess requests for restriction on processing and lift the restriction and inform the subject once the matter has been resolved ● implement the necessary restriction and technical implementation measures required to ensure that the data can only be processed, with the subject's consent – apart from storage alone; such measures could include: – temporary removal of access to all or part of a record – prevention of amendment or deletion of the data – temporary removal to a separate data store – indication on the system that restriction is in place. ● publicise these procedures in their information notices. Such procedures might benefit from inclusion in a general 'subjects' rights' procedure suite.
12. Right to data portability: Article 20	
What's new Data subjects have the right to receive personal data about them in a '…*commonly used and machine readable format*'. This right is only available: ● where the processing is based on consent (Arts. 6(1)(a) or 9(1)(a)) and ● the processing is automated. **What's similar** This is a new right.	**Impact** This will only impact data that are being processed with consent as the legal basis under Articles 6(1)(a) or 9(1)(a).

What's new in the GDPR	Impact for health and social care organisations
13. Right to object: Article 21	
What's new Data subjects have a right to object to processing, '*on grounds relating to his or her particular situation*' where processing is based on: ● 6(f)'*legitimate interests*' (not available to public authorities), or ● 6(e)'*task carried out in the public interest or in the exercise of official authority vested in the controller*'. And the data controller must respect the objection unless they can demonstrate compelling legitimate grounds which override the individual's rights or for the establishment, exercise or defence of legal claims. In the case of processing for scientific or historical research or statistical purposes pursuant to Article 89(1), the right to object need not be respected where the processing is necessary for the performance of a task carried out for reasons of public interest. **What's similar** Under the DPA, there is a right under Section 10 for a subject to require a data controller to cease or not to begin processing personal data about them. However, this is dependent on specified reasons: that the processing is/will cause unwarranted and substantial damage or distress, whereas the Directive and GDPR only provide for a threshold of 'compelling legitimate grounds'. Where data is being processed for direct marketing purposes, the right to object is absolute. The right to object does not apply where the individual has consented, the processing is necessary to comply with a legal obligation or to protect the vital interests of the individual.	**Impact** Organisations that are public authorities (see above) will often use condition 6(1)(e) as their condition for lawful processing. However the right can be overridden where the controller can demonstrate: '...*compelling legitimate grounds for the processing which overrides the rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims*' If organisations comply with the new national opt out policy, this should in practice cover most if not all cases where the legal right to object is engaged.

What's new in the GDPR	Impact for health and social care organisations
14. Automated decision-making, including profiling: Article 22	
What's new Article 22 gives the right to the data subject: '*not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her*'. This provision applies to the decision, not the execution of the automated processing to which the subject may object under Article 21. ● This does not apply in cases where it is necessary for contractual purposes, or based on the data subject's explicit consent or where is it authorised by UK or EU law: '…*to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*'. **What's similar** Section 12 of the DPA establishes the right for a subject to require that no decision is made by automated means alone, by a notice in writing. The GDPR provision does not require this written notice.	**Impact** Organisations that conduct automated processing will need to make sure that no decision is taken based on such processing without an opportunity being offered to the subject to object to the process and at least obtain human intervention. Organisations will need to: ● ensure that their policies and procedures for introducing new processing include data protection impact assessment of automated processing including profiling, and the conditions under which decisions are made ● establish procedures to ensure that subjects have an opportunity to object before decisions are made, for example before automated communications are made, or records updated automatically. Organisations that conduct risk stratification will need to ensure that their processes comply.

What's new in the GDPR	Impact for health and social care organisations
15. Article 25 – Data protection by design and default	
What's new ● Organisations must incorporate technical and organisational measures to ensure compliance with the data protection principles in both the design and operation of data processing activities. ● Adopting appropriate policies is specifically mentioned as is the use of pseudonymisation (to ensure compliance with data minimisation obligations). ● Appropriate technical and organisational measures to ensure that only personal data that is necessary for each specific purpose of processing are processed. **What's similar** This is a new provision. However the ICO has published privacy by design guidance on this as good practice.	**Impact** Organisations will need to: ● conduct a review of their processing activities to ensure that they are operating in compliance with the GDPR ● focus on particular areas that will include data minimisation through, for example pseudonymisation and appropriate access controls ● ensure that their policies on the introduction of new processes, procurement etc. include requirements for data protection impact assessment for *high risk* processing (as per Article 35), and procedures for assuring business as usual processing. Organisations employing the ICO guidance on privacy by design are likely to be in line with new requirements. Please refer to: ● ICO's guidance on privacy by design ● IGA's guidance on accountability and governance.
16. Article 30 – Records of processing activities	
What's new The GDPR requires that: ● data controllers and processors maintain records of their processing activities ● the information must be included in these records (Art. 30). This supports an organisation's accountability and ability to demonstrate compliance, and generates information to incorporate in transparency information provided to subjects.	**Impact** Although a new obligation, health and social care organisations should already be maintaining information asset registers and information flow maps as required by the information governance toolkit. These obligations do not apply to an organisation employing less than 250 people unless other conditions are met: ● the processing carries a high risk to the rights and freedoms of a data subject, or ● special categories data, for example health data are being processed. The second condition will apply to smaller organisations such as GP Practices who will therefore need to have records of processing activities in place.

What's new in the GDPR	Impact for health and social care organisations
17. Article 35 – Data protection impact assessment	
What's new ● The Regulation makes it obligatory to perform a prior impact assessment in particular during the use of new technologies *where the processing is likely to result in a high risk* to the rights and freedoms of data subjects. ● Data protection impact assessment (DPIA) will in particular be required for automated processing, processing on a large scale of special categories of data (includes health and genetic data) and systematic monitoring of a public area (CCTV, for example). ● There is a list of essential elements of the DPIA. ● However, *'a single assessment may address a set of similar processing operations that present similar high risks'.* ● After the impact assessment has taken place, in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remain high), the data controller must consult the ICO as per Article 36. **What's similar** This is a new requirement and accompanies *data protection by design and default* in Article 25. If your organisation is already employing ICO's guidance on privacy impact assessments, then you are likely to be in line with new requirements.	**Impact** Organisations will need to: ● review their policies and procedures on the introduction of new processes, procurement etc., to ensure that an auditable decision is routinely made as to whether a data protection impact assessment is required ● ensure that a data protection officer is involved at an early stage in all new systems or information processes. There may be little impact on health and social care organisations if your organisation is already employing ICO's guidance on privacy impact assessments. The ICO is required to establish a list of the kind of processing activities that will require a DPIA and those which will not – guidance from the ICO is therefore expected. Please refer to ICO's guidance on privacy impact assessments.

What's new in the GDPR	Impact for health and social care organisations
18. Articles 37–39 – The data protection officer	
What's new Public authorities and organisations engaged in systematic monitoring or processing special categories data on a large scale must appoint a data protection officer, though several authorities or organisations may appoint a single officer in certain circumstances. The data protection officer must be independent (although they can be a member of staff or contractor) and needs to have *'expert knowledge of data protection law and practices'*, as per Article 38 (position of the data protection officer), and the ability to perform the tasks specified in the GDPR: ● provision of advice to the organisation on compliance obligations, and when data protection impact assessment is required ● monitoring compliance with the GDPR and organisational policies ● co-operating and liaising with the information commissioner ● taking into account information risk when performing the above. Further requirements of the role are: ● that the data protection officer directly reports to the highest management level of the organisation ● that there is timely involvement of the data protection officer in all data protection issues ● that the data protection officer is supported by the necessary resources and is able to maintain expertise ● that the data protection officer is not pressurised by the organisation as to how to perform his or her tasks, and is protected from disciplinary action when carrying out those tasks ● where the data protection officer performs another role or roles, that there is no conflict of interest.	**Impact** Organisations that are defined as public authorities in the Freedom of Information Act 2000 are public authorities for the purposes of the GDPR and DPA18. These organisations must appoint a data protection officer. Please refer to IGA's guidance on the role of the data protection officer.

What's new in the GDPR	Impact for health and social care organisations
18. Articles 37–39 – The data protection officer (continued)	
The role of the data protection officer may be shared by multiple organisations that are *'public authorities'* taking into account organisational structure and size, and may be either a member of staff or may fulfil the tasks on the basis of a service contract, provided there is no conflict of interest. The data protection officer should have a good understanding of the organisation's business, and how it processes personal data. **What's similar** Although most organisations will have a data protection officer or similar role, this is a new legal requirement.	
19. Pseudonymisation: Article 4(5)	
What's new ● For the first time the process of pseudonymisation is explicitly defined in the Regulation: *'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'.* ● Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. **What's similar** This is a new definition.	**Impact** ● The fact that pseudonymised data may, depending on the risk of identification, qualify as personal data does not mean that processing is prohibited; it means that processing needs to have an established lawful basis and otherwise comply with the GDPR. ● Article 11 gives exemption to subjects' rights: *'…where the controller can demonstrate that it is not in a position to identify the data subject…'*

What's new in the GDPR	Impact for health and social care organisations
20. Administrative fines: Article 83	
What's new Article 83 introduces two levels of fines on the type of infringement. Each individual case will be reviewed and due regard will be given to the context, including: ● *'nature, gravity and duration'* of the infringement ● the intentional or negligent character of the infringement ● action taken by the controller to mitigate the impact on data subjects ● previous infringements ● the degree of cooperation with the ICO in order to remedy the infringement ● the categories of personal data affected, etc. First level of fine relates to infringements of the obligations in the following articles where fines of up to 10,000,000 Euros or 2% of total worldwide turnover can be given: Art. 8 Conditions applicable to child's consent in relation to information society services Art. 11 Processing which does not require identification Art. 25 Data protection by design and by default Art. 26 Joint controllers Art. 27 Representatives of controllers or processors not established in the Union Art. 28 Processor Art. 29 Processing under the authority of the controller or processor Art. 30 Records of processing activities Art. 31 Cooperation with the supervisory authority Art. 32 Security of processing Art. 33 Notification of a personal data breach to the supervisory authority Art. 34 Communication of a personal data breach to the data subject	**Impact** Data controllers and processers must pay due regard to the strengthened powers of the regulatory body in penalising those who are not adequately complicit with the GDPR. These powers: ● have two levels depending on article and severity ● allow for a wider range of cases that can be reviewed ● allow fines to be greater and/or proportional to the organisation's worldwide turnover.

What's new in the GDPR	Impact for health and social care organisations
20. Administrative fines: Article 83 (continued)	
Art. 35 Data protection impact assessment Art. 36 Prior consultation Art. 37 Designation of the data protection officer Art. 38 Position of the data protection officer Art. 39 Tasks of the data protection officer Art. 42 Certification Art. 43 Certification bodies Second level of fine relates to infringements of the obligations in the following articles where fines of up to 20,000,000 Euros or 4% of total worldwide turnover can be given: Art. 5 Principles relating to processing of personal data Art. 6 Lawfulness of processing Art. 7 Conditions for consent Art. 9 Processing of special categories of personal data Arts. 12 to 22 Data subjects' rights Arts. 44 to 49 Transfers of personal data to a recipient in a third country or an international organisation The ICO is required to ensure that the imposition of such fines is proportionate and dissuasive. For further details please refer to accompanying guidance titled *Data protection accountability and governance.* **What's similar** The ICO as the supervisory authority has the power to impose fines.	

Sources and further reading

Accountability and governance (Information Commissioner's Office)

Anonymisation (Information Commissioner's Office)

Article 29 Working Party: Guidelines on data protection officers ('DPOs')

Article 29 Working Party: Guidelines on the right to 'data portability'

Conducting privacy impact assessments code of practice (Information Commissioner's Office)

Information Governance Alliance (IGA) (Information Commissioner's Office)

Key areas to consider (Information Commissioner's Office)

Overview of the General Data Protection Regulation (Information Commissioner's Office)

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now (Information Commissioner's Office)

Privacy by design (Information Commissioner's Office)

Privacy notices, transparency and control: a code of practice on communicating privacy information to individuals

The General Data Protection Regulation (GDPR) – Guidance on accountability and organisational priorities (Information Governance Alliance)

The General Data Protection Regulation – Guidance on consent (Information Governance Alliance)

The General Data Protection Regulation – Guidance on lawful processing (Information Governance Alliance)

The General Data Protection Regulation – Guidance on the role of the data protection officer (Information Governance Alliance)

The General Data Protection Regulation – Implementation checklist (Information Governance Alliance)