General Data Protection Regulation (GDPR) - Gap Analysis

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
1. Data Protection Principles The Data Protection Act principles are revised down to 6 but are broadly similar to the current principles: • fairness, lawfulness and transparency • purpose limitation; • data minimisation • data quality • security • integrity and confidentiality A new accountability principle makes Data Controllers responsible for demonstrating compliance with the Data Protection principles.	No	1. Review current Data Protection policies, codes of conduct and training to ensure these are consistent with the revised principles. 2. Undertake an information audit to understand what data is held, where it is held, in what format it is held, where it is obtained from, basis for holding it (consent/legal basis). 3. Identify means to *"demonstrate compliance"* i.e. How we are meeting the requirements, following codes of conduct as they are issued, paper trails of decisions relating to data processing and, where appropriate, privacy impact assessments.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
2. Lawfulness of processing/further processing The grounds for processing personal data under the GDPR are broadly the same as now. However, there are new limitations on the use of consent and the processing of children's data (see sections 3 and 4 below). There are specific restrictions on the ability to rely on "legitimate interests" as a basis for processing and some clarification as to when this may be used. There is a non-exhaustive list of factors to be taken into account when determining whether the processing of data for a new purpose is incompatible with the purposes for which the data was initially collected.	Yes Consent is more restrictive. 6(1)(f) Necessary for the purposes of legitimate interests This ground can no longer be relied on by public authorities processing personal data in the exercise of their functions.	1. Ensure we are clear about the grounds for lawful processing: check these will still be applicable under the GDPR. 2. Review information sharing agreements for any that rely on legitimate interests and amend, to show either proper legislative basis or consent. 3. Where relying on consent, ensure quality of consent meets new requirements i.e. clear, unambiguous, and properly recorded. 4. Consider whether new rules on children's data are likely to affect us (more under point 4) 5. Ensure that internal governance processes will enable the Trust to demonstrate how decisions to use data for further processing purposes have been reached, and that all relevant factors have been considered.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
3. Consent Consent is subject to additional conditions under the new GDPR. • There is an effective prohibition on consents and the offering of services which are <u>contingent</u> on consent to processing. • Consent must also now be separable from other written agreements, clearly presented and as easily revoked as given.	Yes Article 4(8) new GDPR defines *"the data subject's consent"* as *"any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, which signifies agreement to personal data relating to them being processed"*. Recital 25 suggests that this may be signified by: *"ticking a box when visiting a… website, choosing technical settings… or by any other statement or conduct which clearly indicates… the data subject's acceptance of the proposed processing of their*	Complete review of the consent process. Need to be sure where we are relying on consent as the basis for lawful processing, that: • consent is active, and does not rely on silence, inactivity or pre-ticked boxes; • consent to processing is distinguishable, clear, and is not "bundled" with other written agreements or declarations; • supply of services cannot be made contingent on consent to processing which is not necessary for the service being supplied; • data subjects are informed that they have the right to withdraw consent at any time, but that this will not affect the lawfulness of processing based on consent before its withdrawal; • there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;		

	personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent." Explicit consent is still required to justify the processing of sensitive/special categories of personal data, unless other legislative conditions (including provision of care where consent is implied/life or death etc) apply.	• separate consents are obtained for distinct processing operations; and • the organisation does not rely on consent where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority). Need to look at how consent is captured and stored. How can users withdraw consent and for this to be actioned within systems		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
4. Children There are a handful of child-specific provisions in the new GDPR, particularly in relation to grounds for processing and notices. Children are identified as *"vulnerable individuals"* and deserving of *"specific protection"*. The GDPR does not prescribe the age at which a person is considered to be a child. Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorised by a person with parental responsibility for the child. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit - which may be no lower than 13).	The current Act does not contain any specific restrictions on processing children's data, and rules on children's ability to consent have been drawn from national laws. The major provision in relation to children is Article 8, which requires parental consent to be obtained for <u>information society services offered</u> directly to a child under the age of 16 – although this ceiling can be set as low as 13 by a Member State, and only applies where the processing would be based on the child's consent. The controller is also required, under Article 8(1a) GDPR,	1. This is <u>likely only</u> to affect us if we are offering what the new act describes as "information society services directly to children". I would read this as social media type services, although this definition could be expanded. 2. We will just need to assess which national rules will apply in terms of age and ensure that appropriate parental consent mechanisms are implemented, including verification processes. 3. Keep a watching brief of national legislation for offline data processing relating to children's data. 4. Where services are offered directly to a child, ensure notices are drafted clearly with a child's understanding in mind.		

	to make *"reasonable efforts"* to verify that consent has been given or authorised by the holder of parental responsibility in light of available technology. This only affects certain online data – offline data will continue to remain subject to usual Member State rules on capacity to consent. Article 8(1) is also not to be considered as affecting the general contract law of Member States regarding the validity, formation or effect of a contract with a child. Organisations will still need to consider local laws in this area			

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
5. Sensitive data and lawful processing "Special categories of personal data" now expressly include "genetic data" and "biometric data" where processed "to uniquely identify a person". The grounds for processing sensitive data under the GDPR broadly replicate those under the current Act, although there are wider grounds in the area of health and healthcare management. There is also a broad ability for Member States to adduce new conditions (including limitations) regarding the processing of genetic, biometric or health data.	Genetic data (*new*); and biometric data where processed to uniquely identify a person (*new*). Interestingly, data relating to criminal convictions and offences are not categorised as *"sensitive"* for the purposes of GDPR. The rules under the GDPR in relation to data concerning criminal convictions and offences provides that such data may be processed only under the control of official authority or where the processing is authorised by Union law or Member State law that provides adequate safeguards.	1. Ensure we have clarity about the grounds relied on when processing sensitive/special categories of data, and check these grounds will still be applicable (possibly drawn out through Info Audit). 2. Where relying on consent, ensure the quality of consent meets new requirements in relation to the collection of consent (see section 3 above) 3. Consider whether rules on children are likely to affect us, (see section 4 above). 4. If we process substantial amounts of genetic, biometric or health data, ensure we keep up-to-date on national developments as Member States have a broad rights to impose further conditions - including restrictions - on the grounds set out in the GDPR.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
6. Privacy Notices Controllers must provide information notices, to ensure transparency of processing. • Specified information must be provided, and there is also a general transparency obligation. • Much of the additional information will not be difficult to supply – although it may be hard for organisations to provide retention periods • There is an emphasis on clear, concise notices.	No – it formalises really what we should always have had. The principle of *"fair and transparent"* processing means that the controller must provide information to individuals about its processing of their data, unless the individual already has this. The controller may also have to provide additional information if, in the specific circumstances, this is necessary for the processing to be fair and transparent. The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language.	1. Audit existing privacy notices, review and update them. Look at the ICO guidance on this. 2. For data which is collected indirectly, ensure that a notice is given at the appropriate time i.e. websites 3. Work with relevant partners who may collect data on our behalf to assign responsibility for notice review, update and approval.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
7. Subject access, rectification and portability Data controllers must, on request: • confirm if they process an individual's personal data; • provide a copy of the data (in commonly used electronic form in many cases); and • provide supporting (and detailed) explanatory materials. Data subjects can also demand that their personal data be ported to them or a new provider in machine readable format if the data in question was: 1) provided by the data subject to the controller; 2) is processed automatically; 3) is processed based on consent or fulfilment of a contract. The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained	We need to provide confirmation whether his/her personal data are being processed; • to access the data (i.e. to have a copy); and • to be provided with supplemental information about the processing. As with all data subject rights, the controller must comply "without undue delay" and "at the latest within one month", although there are some possibilities to extend this. The controller must also use reasonable means to verify the identity of the person making the request – but must not keep or collect data just so as to be able to meet subject access requests.	1. Review the organisation's processes, procedures and training - are they sufficient to understand the SAR rights as this will impact on time and compliance. 2. Develop template response letters, to ensure that all elements of supporting information are provided i.e. covering the detailed supporting information. 3. Can we provide data in a portable format (CSV etc). It may be necessary to develop formatting capabilities to meet access requests. 4. Consider if the data relates to more than one data subject and how to address the difficulties this raises 5. Consider developing data subject access portals, to allow direct exercise of subject access rights. 6. Ensure that the function is adequately resourced and able to meet the 1 month response timescale.		

to the individual. Access rights are intended to allow individuals to check lawfulness of processing and the right to a copy should not adversely affect the rights of others.	These points are particularly pertinent to online services. No £10 charge.			

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
8. Right to object There are rights for individuals to object to specific types of processing: • Direct marketing; • Processing based on legitimate interests or performance of a task in the public interest/exercise of official authority; and • Processing for research or statistical purposes. Only the right to object to direct marketing is absolute (i.e. no need to demonstrate grounds for objecting, no exemptions which allow processing to continue). There are obligations to notify individuals of these rights at an early stage - clearly and separately from other information. Online services must offer an automated method of objecting.	No	1. Audit privacy notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'. 2. For online services, ensure there is an automated way for this to be effected. 3. Review marketing suppression lists and processes (including those operated on behalf of the organisation by partners and service providers) to ensure they are capable of operating in compliance with the GDPR.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
9. Right to erasure and restrict processing More extensive, and unclear, rights are introduced: a right to be forgotten (now called erasure) and for processing to be restricted. Individuals can require data to be 'erased' when there is a problem with the underlying legality of the processing or where they withdraw consent. The individual can require the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the individual objects to erasure. Controllers who have made data public which is then subject to a right to erasure request, are required to notify others who are processing that data with details of the request. This is a new wide-ranging and challenging obligation	Yes	1. Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them. 2. Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved, or indeed to delete data is required.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
10. Governance obligations The GDPR requires all organisations to implement a wide range of measures to reduce the risk of their breaching the GDPR and to prove that they take data governance seriously. These include accountability measures such as: Privacy Impact Assessments, audits, policy reviews, activity records and appointing a data protection officer a ("DPO"). For those organisations which have not previously designated responsibility and budget for data protection compliance, these requirements will impose a heavy burden.	Yes	1. The organisation needs to assign responsibility and budget for data protection compliance. 2. Organisation needs to appoint a DPO and to make arrangements for reporting structures. i.e. the need for the DPO to be autonomous, how this sits with other workloads etc. 3. Supervisory authorities will expect a line direct to the board/senior mgt and the job specification for those designated with DPO responsibilities will need to be created. 4. The DPO will need to ensure that a full compliance programme is designed incorporating features such as: Privacy Impact Assessments, regular DP audits, policy reviews and updates, and training and awareness raising programmes. 5. Audit existing supplier arrangements and update template RFQ's and procurement contracts to reflect the GDPR's data processor obligations.		

		6. Monitor the publication of supervisory authorities / EC and industry published supplier terms and codes of practice to see if they are suitable for use by the organisation.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
11. Privacy by design	Some Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities.	Adopting appropriate staff policies is specifically mentioned, as is the use of pseudonymisation (to ensure compliance with data minimisation obligations).		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
12. Breach notification In case of an incident defined as, *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*	72 hrs to notify of a breach. Larger fines. Exemption if: • The breach is unlikely to result in a high risk for the rights and freedoms of individuals; • Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or • This would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed)	Develop and update internal breach/incident notification procedures, including incident identification processes and incident response plans.		

New regulation requirement	Any significant changes?	What work is required	Team/Dept/ System	Owner
13. Transfer of personal data Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area ("EEA")) continue to be regulated and restricted in certain circumstances. Breach of the GDPR's data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines can be imposed (up to 4% of annual turnover).	No	1. Review and map key international data flows (info audit) 2. Review questions included in standard procurement templates and contract clauses to ensure that information about a supplier's proposed transfer of personal data for which you are responsible is understood and conducted in a compliant way. 3. Contractual clauses may need re drafting, monitor progress of Privacy Shield development.		