Annex - Summary of GDPR derogations in the Data Protection Bill

The majority of the provisions in the General Data Protection Regulation (GDPR) will automatically become UK law on 25 May 2018. However, the Data Protection Bill gives us the opportunity to implement a number of flexibilities and derogations which, we believe, will ensure the whole data protection system is tailored to meet the UK's specific circumstances and ambitions.

The following table sets out the flexibilities and derogations in the Bill, the article of the GDPR to which it corresponds, and the UK's reason(s) for choosing, if applicable, to deviate from the GDPR's default position.

GDPR Article	Description	The government intention
Article 4 - definitions	Article 4 contains definitions of terms used in the GDPR. These include what is meant by terms such as 'controller', 'processor' and 'consent' as well as many others. Article 4(7) sets out the definition of 'controller' which is the legal or natural person that determines the purposes and means of the processing of personal data. The current wording of Article 4(7) may make it operationally harder to identify the data controller in certain circumstances.	The GDPR allows the UK to specify who the controller should be, or the criteria to nominate a controller in specific circumstances. We will ensure it is straightforward to identify the data controller by maintaining the DPA as far as possible whilst remaining consistent with the GDPR definition.
Article 6 - lawfulness of processing	For an organisation to process an individual's personal data, there are certain conditions that need to be met. This article lays down those conditions for the processing to be considered 'lawful'. For example, the conditions include an individual giving consent, entering into a contract or an organisation processing data in the public interest. Schedule 2 to the DPA contains equivalent provision to Article 6 of the GDPR.	Article 6(1) of the GDPR is directly applicable and offers little by way of derogation. However, it does allow Member States to make more specific rules regulating the processing of data for public interest purposes. The policy aim is to reflect the DPA as far as possible and continue to provide clarity as to what processing for 'public interest purposes' means, to ensure that organisations are able to continue lawfully processing data. The government will do this by replicating the wording of paragraph 5 of Schedule 2 to the DPA. The term 'public authority' is not defined in the GDPR. A number of respondents to the Call for Views asked for a definition of public authority to be provided. For clarity and legal

		certainty we plan to base the definition on that in the Freedom of Information Act 2000.
Article 8 - conditions applicable to child's consent	Article 8 sets out the conditions applicable for a child's consent in relation to 'information society services'. Where a child is under 16, processing will be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The DPA is silent on this matter.	The GDPR allows the UK to set the age at which a child may consent to the processing of their personal data by those offering information society services to an age between 13 and 16. The government will set the age at which a child can consent to the processing of data for the purposes of the provision of information society services at 13 years old. The government is not persuaded that setting the age at 16 would create any additional protections for children for the reasons given in Chapter 3 of this document.
Article 9 - processing of special categories of personal data	Article 9 sets out the circumstances under which 'special categories' (sensitive personal data under the DPA) of data can be processed. Processing these 'special categories' is generally prohibited as they cover sensitive personal matters including racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership. The GDPR has introduced two additional 'special categories'; genetic and biometric data. Schedule 3 to the DPA permits the processing of sensitive personal data in certain listed circumstances. Examples are where the processing is on the basis of explicit consent, or without consent for medical purposes by health professionals.	The GDPR allows the UK to expressly set out the conditions and safeguards that will allow the processing of 'special categories' of data to continue. The UK will provide for processing under Article 9 so that, in so far as possible, all 'special category' processing currently carried out in reliance on Schedule 3 DPA, currently known as 'sensitive personal data' can continue. The policy aim is to reflect the DPA as far as possible. The government will implement the derogations available to ensure that organisations that currently process sensitive personal data in compliance with the DPA can continue to do so under the GDPR.
Article 10 - processing of personal data relating to criminal convictions and offences	Article 10 restricts the 'processing of personal data relating to criminal convictions and offences' Criminal convictions and offences or related security measures based on Article 6(1) can only be processed 'under the control of official authority', or if processing is	The GDPR allows the UK to authorize the processing of personal data relating to criminal convictions and offences otherwise than by a public body or authority

	specifically authorised, with the necessary safeguards to protect individuals' rights and freedoms. A full register of criminal convictions can only be kept under the control of official authority. In the DPA, criminal convictions data is incorporated into the definition of sensitive personal data and is subject to the processing conditions for sensitive personal data in Schedule 3. Any person or organisation can process the data provided conditions in Schedule 3 are met.	The government intends to exercise the derogation as there are many organisations that would not be classed as an 'official authority' who currently process criminal convictions data. For example, employers process criminal convictions data as part of their pre-employment checks and insurers process criminal convictions data for anti-fraud purposes. These bodies will need legal certainty to ensure they can continue the processing of criminal convictions and offences data under the new law. The policy aim is to reflect the DPA as far as possible. The government will therefore implement Article 10 by mirroring relevant provisions under Article 9(2) in order to provide grounds for processing otherwise than under the control of official authority.
Article 22 - automated individual decision making	Article 22 gives individuals the right to object to decisions made about them solely on the basis of automated processing, where those decisions have legal or other significant effects. Solely automated processing means where there is no human intervention, for example, when data is entered into a computer about an individual's spending habits and debt, which then processes the data to calculate creditworthiness. The DPA provides similar safeguards against automated decision making. These include an individual being informed about and being able to object to solely automated processing, as well as ask that a decision made through that process be reconsidered.	The GDPR allows the UK to specify additional circumstances and safeguards when solely automated processing may take place. With a fast moving pace of technology driving automated decision making with algorithms and artificial intelligence, it is important to maintain a narrow list of exemptions that protect individuals' rights. The government believes that safeguards within the DPA (Section 12(2)(b) of the DPA) could be adapted to be applied to circumstances where a person does not consent to processing and where it is not necessary for the purpose of a contract. We will therefore apply these additional safeguards which GDPR does not otherwise provide for.
Article 23 - restrictions	Article 23 allows Member States to introduce restrictions to the rights and obligations in the GDPR where it is a necessary and proportionate measure required to safeguard an important public interest objective. The DPA has similar restrictions on rights and obligations where in the public interest.	The GDPR allows the UK to introduce exemptions from transparency obligations and an individual's rights. The government's objective is to preserve the effect of the exemptions in the DPA to the extent permitted under the GDPR. We consider that most are compatible with GDPR requirements, subject to necessary

		adjustments. Where it is considered necessary we will extend those exemptions to any new rights. We will maintain the approach adopted under the DPA whereby the exemptions exist for various purposes only, and not entity or sector.
Article 43 - certification bodies	Certification schemes exist to encourage and demonstrate compliance with data protection standards. Article 43 sets the criteria and procedure for accrediting certification bodies. Article 43(1) requires Member States to 'ensure' that certification bodies are accredited by a supervisory authority. There is no current equivalent provision to Article 43 in the DPA.	The government intends to make the ICO and the UK National Accreditation Service (UKAS) the certification bodies. Certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification and need to notify the ICO and/or UKAS of the reasons why certifications have been granted or revoked.
Article 49 - derogations for specific situations	The GDPR imposes restrictions on the transfer of personal data outside the European Union to other countries or international organisations where there is no 'adequacy decision' in place or appropriate safeguards. This is in order to ensure that the level of protection of individuals provided by the GDPR is not undermined. The DPA similarly restricts data transfers. Schedule 4 to the DPA sets out instances where the transfer of personal data to third countries can occur. This includes where the transfer is necessary for reasons of substantial public interest. An 'adequacy decision' is when the EU Commission determines that a non-EU country ensures an adequate level of protection of personal data.	The UK can permit the transfer of personal data to a third country in the absence of an adequacy decision when this is done for 'important reasons of 'public interest'. The government will legislate to provide an order making power that allows the Secretary of State to specify circumstances where a transfer of data is necessary for reasons of substantial public interest, as well as circumstances in which a transfer of data is not deemed to be necessary for reasons of substantial public interest.
Article 52 - independence	Article 52(4) to (6) relate to resourcing, staffing and financial control of supervisory authorities. The article imposes a requirement on Member States to ensure that supervisory authorities are properly resourced. The DPA provides for similar measures in this area.	The GDPR allows the UK to lay down specific rules on the resourcing, staffing and financial control of the ICO. We will make provision to ensure the ICO has adequate resources.

Article 53 - general conditions for the members of the supervisory authority	Article 53 requires the appointment of members of supervisory authorities to be appointed by way of a transparent procedure, each member to meet the conditions required for the performance of their duties and for a member's dismissal to occur only in specific cases. Equivalent provision exists in the DPA including grounds for dismissal.	The GDPR allows the UK to determine the conditions required for the performance of Information Commissioner. The existing grounds for dismissal in the DPA will be amended to avoid conflict with the GDPR. The government will impose a duty on the Secretary of State to determine what the conditions required for the performance of the role of the Commissioner should be.
Article 54 - rules on the establishment of a supervisory authority	Article 54 concerns the rules on the establishment of the supervisory authority. The DPA provides for the establishment of the ICO and other areas relating to the appointment of the Information Commissioner. The DPA does not currently provide for suitably qualified Commissioners.	The GDPR allows the UK to make rules in several areas relating to the ICO and members. The aim is for the Information Commissioner to continue to be the sole supervisory authority for data protection in the UK, and the designated national supervisory authority for the UK. The government will ensure that future Commissioners are suitably qualified in terms of the GDPR to perform their role effectively, and make it a requirement for the Secretary of State's preferred candidate to appear before the relevant select committee for a pre-appointment hearing. The government will retain the term of office for the Commissioner as a maximum of seven years, and prohibit reappointment. Further the government will impose a duty on the Commissioner to issue a code of conduct.
Article 57 - tasks	Article 57 provides a comprehensive list of tasks given to the supervisory authorities of Member States. These include things like enforcing the law, handling complaints and conducting investigations. Section 51 of the DPA provides equivalent provision.	The GDPR allows the UK to ensure that the tasks of the ICO currently provided by the DPA are incorporated into the new law. The government will legislate to reflect section 51(7) DPA (voluntary audits) and section 42 DPA (requests for assessment) to allow the ICO to continue performing fundamental tasks. The policy aim is to reflect the DPA 1998 as far as possible.

Article 58 - powers	Article 58 concerns the powers afforded to a supervisory authority. 58(2) provides for a supervisory authority's corrective powers, which are wide ranging. 58(4) provides for safeguards to be put in place under domestic law in respect of all of the ICO's powers listed. These powers are fundamental to the ICO's functions, and include issuing warnings, reprimands and orders to organisations in breach of the law. 58(6) gives Member States a discretion to provide by law for supervisory authorities to have additional powers. The DPA has provision for the large majority of the powers conferred by the GDPR.	The GDPR allows the UK to establish civil sanctions and penalties which can be exercised by the ICO or the courts for the enforcement of the new law. The policy aim is to reflect the DPA 1998 as far as possible. The government will include provision in the new bill under Article 58(4) (linked to Article 90) that outlines the safeguards which apply to the ICO's use of its investigatory powers. The government will also insert a clause replicating the position set out in section 58 of the DPA, in order to ensure continuity in terms of the status of the ICO's powers to request personal data/information when carrying out its investigatory role as against other enactments and rules of law which prohibit disclosure of information. Outlining the safeguards which apply to the ICO's use of its investigatory powers should provide real clarity for the ICO as to the extent of their powers.
Article 59 - activity reports	Article 59 states that each supervisory authority is required to present an annual report to Parliament, government and other authorities as designated by member state law. The reports are also to be made public.	The UK will need to ensure that the new law provides obligations for the delivery of annual reports. The government will legislate to ensure that annual reports be laid before each House of Parliament. The Commissioner will also continue to be able to lay before each House other reports relating to ICO functions as appropriate.
Article 61 - mutual assistance	Article 61 concerns the mutual assistance between supervisory authorities (SA), in particular information requests and supervisory measures. There is an obligation to provide mutual assistance, except where the SA lacks competence; or compliance with the request would be contrary to EU law or the law of the Member State of the requested SA. Mutual assistance covers inspections, investigations and the exercise of authorisation powers	The government will ensure that the ICO have the ability to provide mutual assistance and share information with authorities beyond the UK upon leaving the EU. This would include incorporating the spirit of Article 50 GDPR as domestic law. The ICO will also be provided with the power to share information with regulators other than data protection authorities, such as consumer protection and financial conduct authorities, both in the UK and abroad.

	The article also provides for 'purpose limitation', which concerns information that has been exchanged by supervisory authorities, the use of which is expressly limited to the purpose for which it was requested. Section 54 of the DPA governs certain functions of the ICO in relation to its dealings with the EU Commission, supervisory authorities of other EEA states and designated authorities of other signatories to Convention 108.	
Article 62 - joint operations of supervisory authorities	Further to Article 61, Article 62 provides for an obligation for joint operations/investigations between supervisory authorities 'where appropriate'. An SA has the right of participation, and an obligation to invite another SA of any Member State where the controller or processor has an establishment; or of any SA in which a 'significant number of data subjects' are likely to be 'substantially affected by processing operations'.	The government will enable the ICO to second members or staff from supervisory authorities of other Member States involved in joint operations and for the secondee to exercise the powers of the host supervisory authority or their parent supervisory authority, as permitted by Member State law.
Article 78 - right to an effective judicial remedy against a supervisory authority	Article 78 provides that all individuals, controllers and processors have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision. Art 78 has two key parts: ● Art 78(1) gives an individual the right to an effective judicial remedy against a legally binding decision of the ICO which concerns them; and ● Art 78(2) gives an individual the right to an effective judicial remedy where the ICO does not handle a complaint, or does not inform them within 3 months of the progress or outcome of the complaint.	The UK is required to ensure there is a specific right to a judicial remedy if the ICO does not update an individual on progress with their complaint within three months, or does not handle their complaint. The right for a controller or processor to appeal to the Tribunal over certain decisions, with other decision subject to challenge by judicial review will be retained through Article 78(1). The policy aim for Art 78(2) is to create a statutory right for an individual to apply to the Tribunal for an order that the ICO must handle their complaint and/or update them on the progress or outcome of the complaint within three months, if the ICO has failed to do so. The government will create a statutory right to apply to a Tribunal if the ICO fails to take any action to investigate an individual's complaint,

	The right under Art 78(2) does not have an equivalent in the DPA.	or the ICO fails to inform the individual of the progress or outcome of their complaint.
Article 79 - right to an effective judicial remedy against a controller or processor	Art 79 gives an individual the right to an effective judicial remedy against a data controller or data processor where the individual considers that the processing of their personal data has infringed their rights under the GDPR. The DPA gives individuals the right to apply to court for an order against a data controller in certain circumstances.	The UK is required to ensure that individuals have an effective judicial remedy where he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR. The policy aim is to reflect the DPA, as individuals currently have a right to an effective judicial remedy. The government will ensure that individuals are able to bring a claim before the courts when their rights under the GDPR have been infringed, in the same way as they can currently bring a claim before the courts for infringements of certain sections of the DPA. The courts before which the claim must be brought will be the county court or High Court in England and Wales and Northern Ireland, and the Court of Session or sheriff in Scotland.
Article 80 - representation of data subjects	Article 80 allows individuals to have the right to mandate a not-for-profit body, organisation or association (such as a consumer protection body) to exercise rights and bring claims on their behalf. These rights include the right to lodge a complaint with the ICO (Art 77); the right to an effective judicial remedy against the ICO (Art 78); and the right to an effective judicial remedy against a data controller or processor. Article 80 is a new provision, with no direct equivalent in the DPA.	The policy aim is to ensure that individuals are able to exercise their rights to authorise non-profit organisations to deal with claims on their behalf, and that such organisations can collect damages awarded on individuals' behalf. The government will legislate to ensure that individuals are able to exercise their rights to authorise non-profit organisations to deal with claims on their behalf.
Article 82 - right to compensation and liability	Article 82 gives any person who has suffered material or non-material damage as a result of an infringement of the GDPR the right to receive compensation from the controller or processor. Section 13 of the DPA provides that an individual who suffers damage by reason of a data controller's contravention of the	The policy aim is to reflect the DPA 1998 as far as possible. The UK will ensure that a person is able to claim compensation for material or non-material damage in the county court or High Court in England, Wales and Northern Ireland and the Court of Session or sheriff in Scotland, in the same way as they can currently claim

	DPA is entitled to compensation for that damage.	compensation under the DPA.
Article 83 - general conditions for imposing administrative fines	Article 83 makes provision in relation to the imposition by the ICO of administrative fines for the infringements of certain provisions of the GDPR.	The GDPR allows the UK to make rules to fine public authorities and bodies if domestic law does not provide for administrative fines, and specify to what extent they might be fined. The government will replicate the existing processes and safeguards applicable to civil monetary penalties under the DPA.
Article 84 - penalties	Article 84 requires Member States to lay down rules on penalties for breaches of the GDPR other than administrative fines. These penalties must be effective, proportionate and dissuasive. Data protection law in the UK has always been accompanied by criminal offences. There are various provisions under the DPA that provide for criminal offences, including but not limited to sections 21, 22, 24, 47, 55, 56 and 59.	The GDPR allows the UK to specify the penalties for infringements of the law that are not subject to administrative fines. The government will retain most but not all existing offences under the DPA 1998, with some modifications and extensions and will also create some new offences. The government intends to: Reproduce offences in the DPA which remain fit for purpose, including offences relating to unlawful disclosure of personal data obtained by the ICO in connection with their investigations, and offences relating to enforced subject access (e.g. where an employer asks a prospective employee to obtain personal data to which the organisation wouldn't normally be entitled) Extend the offence of unlawfully obtaining personal data (under s.55 of the DPA) so that it covers unauthorised 'retention' of data and introduce a new defence for journalistic activity. Extend an offence in the Freedom of Information Act 2000 (altering records with intent to prevent disclosure) so that it applies to all data controllers and processors, not just public authorities. Amalgamate three separate offences in the DPA which relate to obstructing the Information Commissioner's investigations into a single offence of obstruction.

		Create new offences relating to re-identifying anonymised or pseudonymised data. All offences will be/become recordable.
Article 85 - processing and freedom of expression	Article 85 requires Member States to introduce exemptions to the GDPR where necessary to 'reconcile the right to the protection of personal data...with the right to freedom of expression and information.' The article makes provision for processing that is carried out for journalistic purposes, or for the purposes of academic, artistic or literary expression. Exemptions or derogations are permitted for a similarly defined category under section 32 DPA. The two GDPR additions that article 85 provides are protection to the freedom of expression ***and information*** and also academic expression alongside the other purposes.	The GDPR allows the UK to provide exemptions to article 85 to find the right balance between the protection of personal data and the right to freedom of expression. The policy aim is to reflect the DPA 1998 as far as possible. The government believes that section 32 DPA sets a good standard and should be used as a baseline for implementing the GDPR. This view was supported by the majority of respondents to the Call for Views that commented on the derogation.
Article 86 - Processing and public access to official documents	Article 86 allows the principle of public access to official documents to be taken into account when applying the GDPR. The rights and protections afforded under the GDPR, and in particular under Art 15 and Chapter III, are therefore balanced by the acknowledgement that Union or Member State law may nonetheless permit the disclosure of personal data held by public entities or private entities performing public tasks. These opposing rights, on the one hand the protection of personal data and on the other hand the disclosure of that personal data, are already enshrined in several UK laws, particularly the Freedom of Information Act (FOIA) 2000.	The policy aim is to reflect the DPA and FOIA as far as possible. The current UK public access regimes provide public entities with the duty to disclose personal information in the public interest and this will continue as we consider it is compatible with the GDPR under Art 86.
Article 89 - safeguards relating to processing for archiving purposes	Article 89 permits processing of personal data for scientific and historical research, statistical purposes or archiving in the public interest, if appropriate technical and organisational safeguards are in place to protect personal information from misuse.	The government intends to replicate the position under the current law as far as possible. By ensuring that all the derogations available for research organisations under Articles 89(2) and (3) are set out clearly in UK law the

	Section 33 of the DPA exempts processing for research purposes from the subject access provisions in section 7 of the Act, providing that the processing does not support decisions about individuals or cause them substantial damage or distress.	government will be providing research organisations with a similar degree of flexibility as they currently have under the 1998 Act. The government intends to exercise derogations in Articles 89(2) and (3) so that research organisations do not have to comply with an individual's rights to access (Art. 15), rectify (Art.16), restrict further processing (Art. 18) and object to processing (Art. 21) where this would seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure. The government will also invoke two further derogations which are only available for archiving organisations, namely the obligation to alert third parties with whom the data might have been shared of any changes made by an individual (Art. 19), and the right of individuals to transfer their data to another provider (Art.20).
Article 90 - obligations of secrecy	Article 90 is concerned with obligations of secrecy (confidentiality) in relation to investigations by supervisory authorities. It allows Member States to pass national rules that reconcile the protection of personal data (in the form of powers of access) with confidentiality obligations. These rules can only apply in relation to personal data which a controller or processor has received as a result of an activity covered by an obligation of confidentiality. UK law does not have an obligation of secrecy, however there are equivalent obligations in the form of duties of confidence and legal professional privilege. If the ICO or Information Tribunal needs information for the discharge of their duties under the DPA, there is no law that prohibits the person who has that information from disclosing it.	The policy aim is to reflect the DPA as far as possible. The ICO is subject to a statutory prohibition against disclosure of information disclosed to them. The government does not want to introduce national law under Article 90 as this would limit the ICO's power to obtain information and reduce the ICO's ability to effectively regulate the sector. Article 90 could apply to a large number of organisations e.g. health service bodies, the police, legal profession and social work bodies. The government believes that the current practice adopted by the ICO achieves a fair balance between the need for the ICO to be able to regulate effectively and individuals' rights. The government will replicate existing DPA provisions and will legislate to include a provision equivalent to section 58 of the DPA, to clarify that those asked to provide the ICO

		with information under Articles 58(1)(a),(e) or (f) can do so without being found to have breached existing duties of confidence or non-disclosure requirements in other legislation. The existing rule set out in section 58 DPA overrides any law which would otherwise prevent the disclosure of data to the ICO such as LPP.

Department for Digital, Culture, Media and Sport
7 August 2017