Response to the Department of Culture, Media & Sport call for views on the UK implementation of the General Data Protection Regulation (GDPR) derogations

The Information and Records Management Society (IRMS) is the foremost professional association for all information professionals, regardless of their professional or organisational status or qualifications. Formed in 1983 and with a clear commitment to inclusivity across the profession, IRMS now has 1200 members in over 30 countries and territories world-wide and in all sectors of the business world- both public and private.

Our Mission

To provide leadership in records and information management with the aims of:

- Championing the status of information and records management through representation, external liaison & promotion
- Supporting professional development through sharing knowledge and expertise;
- Promoting all aspects of good information and records management practice.

To do this, the Society supports and promotes activity across the profession- everything from Group Events to a podcast programme and publishing a professional 'journal' 6 times a year- as well as being active in advocacy for the profession and engaging in mutually-beneficial collaborations with other organisations for the benefit of both our membership and the wider profession.

Theme 1: Supervisory Authority
Article 51 - Supervisory Authority **Article 53 - General conditions for the members of the supervisory authority** **Article 54 - Rules on the establishment of the supervisory authority** **Article 58 - Powers** **Article 59 - Activity reports** **Article 62 - Joint operations of supervisory authorities** **Article 90 - Obligations of secrecy**
The IRMS believes that clarification is needed on how far does this rule applies, i.e. while we agree that the supervisory authority cannot be involved in court decision making, personal information processing operations surely would come under the supervisory authority jurisdiction? Also this seems to contradict Article 10 which states that processing relating to criminal convictions/offences shall be carried out only under the control of official authority or when authorised by Union/member state law. See also Theme 8 Criminal Convictions.
Theme 2: Sanctions

Article 36 - Prior consultation
Article 36 (4)&(5) allows for the UK Government to legislate for Data Controllers to consult with the Supervisory Authority in additional circumstances to that of 'high risk' and those outlined in Article 36 (1). IRMS believes that further clarification should be given here as to exactly when this would apply, especially as some of the categories listed would require prior consultation for any processing for that purpose (Social protection for example).
Article 58 - Powers
The IRMS currently does not have a view with regards to UK derogations under Article 58.
Article 83 - General conditions for imposing administrative fines
Article 83 (7) allows for member states to lay down rules for when and how administrative fines are imposed on Public Authorities. The IRMS recognises that there is a need for the Public Sector to demonstrate compliance and be transparent with Data Subjects on their compliance however fines of up to £20million (or Euros) poses risks for the financial stability and ability to provide vital services should such a fine be imposed. The IRMS would therefore recommend that an administrative fine 'system' for Public Authorities is developed and this takes in to account the grounds for issuing of a fine but also the lack of funds available to Public Authorities. The current approach of 'carrot and stick' should remain with fines only being explored where the authority is failing to engage with requirements.
Article 84 - Penalties
Article 84(9) allows the UK Government to lay down additional rules and penalties with regards to any infringements of the requirements of the GDPR and derogations. Currently under the Data Protection Act 1998 it is a criminal offence to knowingly and wilfully take or sell Personal Data without authorisation of the Data Controller (a section 55 offence). This can even carry with it a prison term in some circumstances. The IRMS believes this provision is a vital protection and deterrent to prevent people from looking to steal Personal Data or try to engage in the Personal Data black market. As the GDPR is looking to offer more and better protections over Personal Data there should be something within UK law to prevent the theft and misuse of Personal Data, ideally by having this as a criminal offence.

Theme 3: Demonstrating Compliance

Article 40 - Codes of conduct

Overall the IRMS believes that the creation of more detailed Codes of Conduct for aspects of the GDPR are welcome. We believe that focus should be placed on codes of practise in these respective areas and the codes should be endorsed / made in collaboration with an appropriate professional boy / trade association.

- Information & Records Management (building on the standards outlined in the Section 46 Code of Practice for example)
- Register of Processing Activities
- Subject Access Requests
- GDPR Risk Management (Information Risk)

Article 42 - Certification

The IRMS does not have a view with regards to UK derogations under Article 42 however we do believe any certification scheme should be based on industry input in order to ensure it is useful and valuable.

Article 43 - Certification bodies

While the IRMS has no major preference for how this is achieved we believe that in order for the Certification to have value the certification and its certifiers should be separate (as happens with certification to ISO standards for example). Therefore if the ICO was to create the certification scheme and requirements, another body/bodies should via an official means (licencing for example), offer auditing and certification to that standard.

Theme 4: Data Protection Officers

Article 4 - Definitions

Article 10 (and throughout the Regulation) makes mention of ‘official authority’. We believe it would be beneficial for a definition to be included in the Definitions (Article 4) or member state legislation.

Article 37 - Designation of the data protection officer

The IRMS believes that in order to support the requirement of 'suitable qualifications' that the UK Government and/or Information Commissioners Office agree and publish a list of acceptable UK qualifications to hold.

Currently there are numerous qualifications a DPO could hold with regards to Data Protection, including it being a subject in a wider legal degree. Some clear standards on the suitable qualifications (as a minimum for example) would offer a clear requirement and skills plan for future DPOs.

Article 38 - Position of the data protection officer

Currently Article 38(5) states that the DPO will be bound by member state laws on professional secrecy. In that regard, does that mean that a DPO's advice or other would be covered by Legal Professional Privilege or Professional Confidentiality and therefore not releasable under Subject Access or Freedom of Information requests? The IRMS believes there should be some clarity around this point and how it interacts with other UK legislation (FOI and/or SAR provisions for example) so that entities can ensure their records are created and managed with this in mind.

Theme 5: Archiving and Research

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Under the current Data Protection Act 1998 the archiving condition (section 33) outlines the conditions for which this applies but also what requirements of the DPA do not apply in that processing purpose. Under the GDPR Article 89 (2)&(3) allow for the UK Government to legislate on outlining how the rights outlined in Articles 15, 16, 18, 19, 20 and 21 would apply to the Personal Data processed under these conditions / purposes.

The IRMS believes that this legislation should, at the very least, match the protections offered to archiving services under the Data Protection Act 1998. Some clarity would also be beneficial where there is no 'national statute' to archive information that is not deemed a public record but does have some historical (national or local) value, including private organisations who want to create their own archives which contain personal data such as a local community organization which may have letters from citizens or personal pay information.

Theme 6: Third Country Transfers

Article 49 - Derogations for specific situations

The IRMS currently does not have a view with regards to UK derogations under Article 49.

Theme 7: Sensitive personal data and exceptions

Article 9 - Processing of special categories of personal data

The IRMS currently does not have a view with regards to UK derogations under Article 9.

Theme 8: Criminal Convictions

Article 10 - Processing of personal data relating to criminal convictions and offences

The GDPR currently does not offer protections over the processing of Personal Data for the prevention and detection of crime. If the Data Protection Act 1998 is repealed this will leave a gap in the protections and requirements of the processing of Personal Data for this purpose. The IRMS therefore believes that legislation should be drafted to cover this gap and that at the very least the same protections and requirements of the DPA should be in place.

This could include, but is not limited to, ensuring that the prevention and detection of crime is a clear ground for processing, that does not require data subject consent. This would also include provisions around Section 29 & 31 requests and how they would now need to interact with the GDPR requirements, again maintaining a need to not notify or seek consent of the Data Subject when processing or responding to the request.

We also believe that within the ‘employment processing’ related legislation, there should be clear provisions around the processing of Special Categories of Personal Data for the purpose of DBS checks. Currently we believe the provisions in the GDPR for this are too vague, especially where the processing concerns criminal record information.

Theme 9: Rights and Remedies

Article 17 - Right to erasure ('right to be forgotten')

The IRMS believes that the definition used in Article 17 (3)(c) for ‘public health’ should be clearly defined, as there are several functions that the UK calls ‘public health’ that would not seem to meet the implied definitions under the GDPR.

There should also be controls in place to prevent those who make requests to Companies House who have owned a company that has gone into administration from being granted the right to be forgotten. Company laws should therefore be changed to reflect the fact they have a company is

a matter of public record and the particulars of that company (including when and how it went into administration) should also be public in order to protect others and the economy.

Article 22 - Automated individual decision-making, including profiling

The IRMS currently does not have a view with regards to UK derogations under Article 22.

Article 26 - Joint controllers

Under the GDPR we are losing the definition of 'Data Controllers in common'. This is often very useful in situations where the point of data collection could be the same, but the purposes for each controller were very different. For example, in an application for social care assistance, the assistance may be offered by 2 different entities especially if one aspect of the care assistance requires specialist experience. Under the GDPR we would need to, in that arrangement, be joint controllers for everything we both collect together or separate out the data collection so it is clear they are very different. In a social care context this can then be very long and confusing for data subjects and then means that entities need to police each other in what they are doing with that Personal Data. Something which, again in a Social Care & Health context, neither entity is likely to have the resources to achieve.

The IRMS therefore believes that any derogation law should outline a suitable definition that allows for Data Controllers in common (including outlining that they can be responsible for different purposes and not each other's).

Article 80 - representation of data subjects

The IRMS currently does not have a view with regards to UK derogations under Article 80. However some steps should be implemented to stop 'ambulance chasers' looking to make quick bucks on GDPR breaches (no matter the size or impact).

Theme 10: Processing of Children's Personal Data by Online Services

Article 8 - Conditions applicable to child's consent in relation to information society services.

The IRMS believes that UK legislation should allow for the age of consent to be lowered to 13, as allowed under Article 8 (1). We also believe that some provision should also be made for the current Gillick competency test so that should a child of below 13 years of age, engage with services that are offered by various means, including online, the processing would not require consent if they are deemed to be Gillick Competent.

Our concern is that having different standards with regards to when child consent is needed and what that consent is, especially in the context of any online care, counselling or medical support, may lead to conflicts between different areas of UK legislation which may then also affect the ability to act in the child's best or vital interests.

Theme 11: Freedom of Expression in the Media

Article 85 - Processing and freedom of expression and information

The IRMS currently does not have a view with regards to UK derogations under Article 11.

Theme 12: Processing of Data

Article 6 - Lawfulness of processing

Overall, the IRMS does not have any pressing views or evidence in regards to the above Article 6 and its derogations. However we do believe that the derogations for the processing of Personal Data for employment purposes should be in place as soon as possible. This should include provisions for processing of personal data for payroll purposes clearly outlined as part of employment processing purposes.

Article 18 - Right to restriction of processing

The IRMS believes that it should be made clear in UK law that where processing is done under the grounds of legal statute, where original records of Personal Data are needed to verify compliance with those obligations, rights to restriction, deletion or correction cannot apply either fully or in part. More information on each restriction is outlined in theme 13.

Also, in Article 18 (2) there is the term 'with the exception of storage'. Does this mean that personal data held in storage does not have to be restricted or does this refer to further processing of data held in storage? UK supporting legislation should therefore make this clear.

Article 28 - Processor

The IRMS does not believe that UK derogation outlined in Article 28 (3) & (4) would be required here. Article 23 (3) currently outlines what a data processing agreement should contain and currently there are sufficient standards in UK contract law to define what a contract is and how it should be enforced.

Article 29 - Processing under the authority of the controller or processor
The IRMS currently does not have a view with regards to UK derogations under Article 29.
Article 32 - Security of processing
The IRMS currently does not have a view with regards to UK derogations under Article 32.
Article 35 - Data protection impact assessment
With regards to Article 35 (10), the IRMS does not have any pressing views or evidence in regards to the above or any derogation needed in this context. However, with regard to Article 35 (4) & (5) we believe the supervisory authority should move quickly to publish a list of what sort of processing would require a DPIA, including a clear definition of what would be classed as 'high risk' processing in their view.
Article 37 - Designation of the data protection officer
The IRMS currently does not have a view with regards to UK derogations under Article 37.
Article 86 - Processing and public access to official documents
The IRMS believes that changes in guidance and possible Freedom of Information Act 2000 wording would be required in order to ensure that the FOIA continues to interact well with the GDPR and any UK supporting legislation for employment and crime data processing. As many of our members are from public authorities subject to Freedom of Information requirements it is important that this is implemented from 25 May 2018 so that they can continue to meet both their GDPR and FOI obligations.
Article 87 - Processing of the national identification number
Currently the UK does not have a national ID number, outside of a National Insurance Number or NHS number. Therefore, with regards to Article 87 (1), the IRMS does not have any pressing views or evidence in regards to the above or any derogation needed in this context, other than to ensure current standards are maintained.
Article 88 - Processing in the context of employment

Currently, the DPA is not clear on employment contracts and the provision of a clear consent. Where processing is required by law, consent is not needed and that should continue to be the case. However where processing is required in order to employ someone, manage their employment and manage their ongoing training and development, under the GDPR definitions, consent given in an employment contract would not be valid.

The IRMS believes that a UK derogation on employment processing should make it clear that the legal grounds for processing is the provision of employment by contract and then outline steps that an employer would need to take to balance that lack of 'effective consent'. This could include requirements on what to include in an employment contract or notice through to outlining what information is and is not needed to meet basic employment purposes. This may therefore require either a specific HR DPA or edits to current employment related laws to make this clear. In any event, the final requirements should be made clear as soon as possible as currently time is limited to get any changes needed implemented before May 2018.

Theme 13: Restrictions

Article 23 - Restrictions

The IRMS believes that the restrictions and 'exemptions' of the Articles 12 to 22, 35 and 5 should, in so far as possible, offer at least the same exemptions as the current Data Protection Act. For each Article we have summarised the key requirements below;

Article 5: Principles
The DPA currently allows for elements of the principles to not be applied to processing where certain conditions are in place. For example, if an accusation of crime has been suspected and it is not permitted under law to advise the accused at that point, you can therefore not advise them that you are processing such data on them and indeed sharing it (anti-money laundering being an example). Any UK derogations should therefore mirror the exemptions outlined in the DPA currently.

Article 12: Transparency
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes.

Article 13: Information provided to Data Subject if collected directly
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes.

Article 14: Information provided to Data Subject if collected indirectly
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes. The IRMS also believes that limitations on the extent of this requirement should be placed. For example, in a social care context it is often the case that Personal Data on a neighbour of a data subject that may collect their shopping for them in captured in a Social Worker assessment of

care need. Under the GDPR we would then be processing that neighbours information, would we then need to inform them of this? Given the resource implications this has we don't believe this has any value either for the Data Subject concerned or our obligations under the GDPR.

Article 15: Right of Access
Under the Data Protection Act 1998 the below exemptions from providing Personal Data in a Subject Access Request are believed to be important in order to protect various interests.

Schedule 7(10) – Legal Professional Privilege;
Schedule 7(1) – Confidential References;
Section 38 (2) - Information requested under another enactment;
Section 30(3)(b) – Health and Social Work exemption;
Schedule 7(7) – Intentions in regards to negotiations
Schedule 7(5) - Management Forecasts;

Article 16: Right of Rectification
Any restrictions on the right to rectification should offer the same level of protections as the Data Protection Act 1998. For example, where information on a care need referral was recorded on the day the referral was made, which then turns out to be inaccurate for one reason or another, we as the Data Controller and entity responsible for responding to that care referral need to be able to demonstrate that appropriate actions were taken based on that information. There therefore needs to be an exemption to the right to rectification (and erasure) that allows Data Controllers to still process that original record but ensure that it is not used for other purposes (like delivery of current care needs for example).

Article 17: Right of Erasure
Similarly with Article 16 above and 18 below, any restrictions on the rights on erasure, rectification or restriction should interlink where the processing by the Data Controller is based on statutory requirement. Any derogation should make clear that what Personal Data remains exempt is defined and evidenced by the Data Controller as being needed in order to demonstrate compliance with that statute and/or statutory duties.

Article 18: Right to Restriction
Similarly with Article 16 and 17 above any restrictions on the rights on erasure, rectification or restriction should interlink where the processing by the Data Controller is based on statutory requirement. Any derogation should make clear that what Personal Data remains exempt is defined and evidenced by the Data Controller as being needed in order to demonstrate compliance with that statute and/or other statutory duties.

Article 19: Notification of Right to Erasure
The IRMS believes that where, in Article 19 (1), the requirement to notify other entities of a requirement to delete personal data use the term 'disproportionate effort', this should be clarified either in guidance, codes of practice or derogation legislation. As a provider of a range of services, some of which involve other partners and suppliers, if a requirement was to inform each and every provider and third party, this would involve a lot of effort and take longer than a 20 day period (for example). We believe that it should also be outlined where responsibility lies for the request to delete being enforced. I.E., if a request is not actioned by a third party that we have

informed, what responsibility do we have over that as the controller that first received the request?

Article 20: Right to Data Portability
The IRMS currently does not have a view with regards to UK derogations under Article 20.

Article 21: Right to Object
The IRMS currently does not have a view with regards to UK derogations under Article 21.

Article 22: Automated Individual Decision Making & Profiling
The IRMS currently does not have a view with regards to UK derogations under Article 22.

Article 35: Data Protection Impact Assessment
Similar to theme 12 above, it should be made clear by the supervisory authority what situations require a DPIA to be completed, and therefore by implication which ones do not. It should also be made clear where and when consultation with Data Subject's would be appropriate and when not.

Theme 14: Rules surrounding Churches and Religious Associations

Article 91 - Existing data protection rules of churches and religious associations

The IRMS currently does not have a view with regards to UK derogations under Article 91.

Additional question: cost impact

In the context of the derogations above, what steps should the Government take to minimise the cost or burden to business of the GDPR?

The UK economy is facing a period of unprecedented change with some of the effects known and some unknown at this point. Various sectors are already feeling budgetary pressures for various reasons therefore even with best will in the world they may not have the funds available to make all of the necessary changes. Costs can be minimised through early decision making, allowing entities time to plan and implement properly. Efficiencies can also be realised through making best use of processes already in place, and reducing unnecessary beaurocracy.

The IRMS therefore believes that through Central Government, the ICO and organisations like ourselves and others, best practice and standards should be promoted and shared widely in order to give the chance for all entities regardless of budget to engage (rather than just the threat of monetary penalty).