Sent on 3 May 2017 to DCMS at GDPRCallforViews@culture.gov.uk

Theme 1 - Supervisory Authority

- Article 51 - Supervisory Authority

In general, most of the provisions on the establishment and set up of the ICO as per Schedule 5 of the DPA 98 should remain the basis for the ICO being the independent supervisory authority. However, DCMS may want to consider amending some provisions as set out below.

- Article 52(4) - necessary resources, premises and infrastructure
  - Relevant provision in DPA 98 - Section 18(5): notification fees

DCMS should consider retaining and enhancing the independence of the ICO by providing for the establishment of a scheme for organisations to pay an annual fee to the ICO, with which they can fund their data protection work.

- Article 53 - general conditions for the members of the supervisory authority
  - Article 53(1): appointment procedure

DCMS may want to consider reforming the appointment procedure to make sure the ICO is accountable and reports to Parliament, rather than to DCMS. This would help ensure independence.

  - Article 53(2): qualifications, experience and skills

DCMS should use the opportunity in this article to revisit the assessment procedure for future Commissioners to make sure a suitably qualified person is appointed. Some previous commissioners had to take the first year or two to get up to speed which is not an ideal situation.

- Article 54 - rules on the establishment of the supervisory authority
  - Articles 54(d) and (e): term of the Commissioner
  - Relevant provision in DPA 98 - Schedule 5, section 2, para 3C (inserted by Protection of Freedoms Act 2012):

"A person appointed as the Commissioner may not be appointed again for a further term of office."
It may be wise to use the opportunity provided by GDPR article 54(3) to amend this provision to say that a second term will be considered on a case-by-case basis. It would seem sensible to allow for a competent, well-regarded and well-functioning Commissioner to continue their position, if that would be in the best interests of the ICO and society. Depending on the circumstances at the time, stability and continuity may be preferable to a change of Commissioner.

- Article 58 - powers
  - Article 58(3)(c): prior authorisation

This article allows member states to decide if any processing carried out by a controller should be subject to prior authorisation where that processing is for the performance of a task carried out in the public interest, including processing in relation to social protection and public health.
DCMS may want to consider implementing this provision to make sure that both public and private bodies carrying out processing for these purposes appropriately consider data protection risk and mitigating solutions.

- Article 58(4): supervisory authority powers to be subject to appropriate safeguards, including effective judicial remedy and due process

Presumably this links to article 78 and the right to a judicial remedy against a supervisory authority. In practice it may be sensible to make sure there is a mechanism for companies and individuals to appeal ICO decisions with subsequent recourse to the Information Tribunal.

- Article 58(5): supervisory authority to have the power to report infringements to judicial authorities and where appropriate, to start or be involved in legal proceedings

This provision appears to exist to support supervisory authorities in countries where enforcement is dealt with by another body, such as a public prosecutor. If the ICO can take enforcement action directly, including going to the Information Tribunal or another court, then this should suffice.

- Article 58(6): supervisory authority may be given additional powers

DCMS should consult with the ICO as to whether they think additional powers are needed, but it may be enough to make sure the law allows for additional powers as and when needed.

The following sections of article 58 do not directly have member state derogations listed, but experience of the current regime could lead to improvements in some areas.

- Article 58(1)(a): requesting information

This is essentially the same as the current information notice provided for in section 43 of the DPA 98. However, section 43 requires there to be a complaint submitted to the ICO under section 42. DCMS should consider using the opportunity provided by article 58(1)(a) to remove this requirement and allow the ICO to request relevant information from a controller, processor or representative when it is necessary and appropriate.

- Article 58(1)(b): audits

This provision will presumably replace the current sections 41A and 41B of the DPA 98 allowing the ICO to audit any controller, processor or representative. This expansion will provide a level playing field and allow the ICO to audit any organisation where an audit is warranted, rather than just a limited number of public-sector bodies.

- Articles 58(1)(d) and 58(2)(a): notifying controllers and processors of possible infringements

These two articles would appear to lead to the same outcome, and reflect the current practice, of informing a controller of a complaint and whether they are likely or not likely to have breached the Act following a section 42 request for assessment. It would appear that article 58(1)(d) is intended to notify a controller or processor that there is a suspected infringement (which may or may not have come from a complaint) and article 58(2)(a) is intended to allow a pre-emptive notification by the ICO to a controller or processor if they become aware of practices that look more likely than not to breach the Regulation.

One aspect of these powers that GDPR can help improve is the current ICO practice of contacting organisations following a complaint. The ICO seems to either write to an organisation following a complaint to say that the organisation is in breach and must explain itself; or it writes to an organisation with the result of its investigation to say it has likely breached or likely not breached the law. This would seem to be the wrong way round! The ICO should not presume the individual's view prevails while it is investigating a complaint and wants to hear the organisation's view. And

once it has investigated, the organisations needs a more definitive result than ‘likely or unlikely’; it should be confirmation of either a breach or no breach.

These articles could also cover the situation where a company has engaged with the ICO about some particular processing activity and the ICO can follow up that meeting where necessary to clarify that a particular course of action or implementation would likely breach the Regulation. This would allow the ICO to put a controller / processor on notice that ignoring advice given verbally in a meeting would likely lead to a breach, and it would empower DPOs to lead their company towards the more privacy-friendly course of action.

- Article 59 - activity reports

No comments. This reflects the annual report obligation under section 52 DPA 98.

- Article 62 - joint operations of supervisory authorities

Some individual supervisory authorities already have MoUs in place to work together, but some have been unable to due to restrictions in their national laws. This provision at least helps EU supervisory authorities by putting joint investigation operations on a legal footing. It would seem sensible to maintain this provision beyond Brexit to allow the ICO to continue to take part in joint operations where necessary.

- Article 90 - obligations of secrecy

This is a sensible provision and should be considered along with the provisions on reconciling data protection with freedom of information law so the provisions are harmonious.

Theme 2 - Sanctions

- Article 36 - prior consultation

This connects to article 58(3)(c) in terms of prior consultation for certain processing. Article 36(4) makes sure that those driving through potential legislation involving personal data processing also appropriately consider data protection risk and mitigating solutions.

- Article 58 - powers

This article has already been covered in theme 1 above.

- Article 83 - general conditions for imposing administrative fines
  - Article 83(7): fines for the public sector

It can be counter-productive to fine the public sector, given the money goes to the Treasury, and given they are not generally profit-led. However, it is important for a level playing field that the ICO has the ability to fine all organisations where appropriate, even if in practice they decide to use non-financial penalties more often with certain sectors or public bodies.

  - Article 83(8): appropriate process and judicial remedy

This article links to article 78, which provides that there should be an effective judicial remedy against a decision of a supervisory authority. As the supervisory authority’s decisions are binding and have legal effect, it is important that controllers and processors subject to fines under article 83 have the ability to challenge the fine and underlying decision, and to have the matter decided by the Information Tribunal or a court.

- Article 84 - penalties

This article provides DCMS with the opportunity to finally implement a long-standing (but never implemented) aspect of current law where deliberate or negligent activities (section 55 offences under the DPA 98) attract a criminal penalty. This would be particularly helpful to target those who deliberately wind up companies found to be in breach of the law and restart them under another name.

Theme 3 - Demonstrating compliance

- Article 40 - codes of conduct

The member state derogation in this article seems limited to encouraging the development of codes under article 40(1). Appropriately developed codes can only be a helpful addition to the data protection landscape.

- Article 42 - certification

The member state derogation in this article seems limited to encouraging the development of certifications under article 42(1). Appropriately developed certification schemes can only be a helpful addition to the data protection landscape.

- Article 43 - certification bodies

No comments.

Theme 4 - Data Protection Officers

- Article 4 - definitions

There does not appear to be any mention in this article of either member state derogations or any mention of the DPO, so it is not clear why it has been included.

- Article 37 - designation of the data protection officer
  - Article 37(4): member states can determine other circumstances when a DPO is required

The only member state derogation in this article would seem to be 37(4) where member state law could require a DPO in additional circumstances to those set out in 37(1). DCMS should not introduce further provisions to make a DPO mandatory, given the inflexible nature of some of the DPO provisions, which could prove difficult or counterproductive for start-ups, charities and SMEs in particular. Requiring a DPO across the board or in additional circumstances to those already listed in the article could be counterproductive, as this could lead to a DPO being a box-ticking compliance exercise. Instead it is a better approach to encourage companies not legally required to have a DPO to make sure they have appropriate staff to be able to comply with the Regulation and demonstrate compliance in a way that suits their operations, size and so on. Flexibility allows companies to appoint an appropriate person or people to achieve the same aims but in a way that fits their company structure and activities, and allows DPOs greater flexibility in the roles they choose to pursue at different stages of their career.

- Article 38 - position of the data protection officer

The only member state derogation in this article would seem to be 38(5) where DPOs are to be subject to member state law on confidentiality and secrecy. It is not clear what this provision aims to achieve beyond the usual confidentiality requirements employers place on employees.

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
  - Article 89(2): processing for scientific or historical research purposes or statistical purposes - derogations from the rights in Articles 15 (access), 16 (correction), 18 (restriction) and 21 (object)

DCMS should consider implementing derogations under this article for statistical purposes processing in a way that maintains the existing DPA 98 section 33 research exemption. This would prevent there being a barrier to innovation and allow companies doing valuable big data analysis, modelling and statistical analytics to carry out activities that do not lead to decisions or measures about individuals and do not cause damage or distress to individuals, without having to include this data when considering requests to exercise the rights listed. In particular with machine learning, it can be impossible to extract, correct, restrict or otherwise not process the specific data of an individual; and even more so once data has been used to train or create a model.

  - Article 89(3): processing for archiving purposes in the public interest - derogations from the rights in Articles 15 (access), 16 (correction), 18 (restriction), 19 (notification of correction, restriction or deletion), 20 (data portability) and 21 (object)

No comments.

Theme 6 - Third Country Transfers

- Article 49 - derogations for specific situations
  - Article 49(4): important public interest purpose recognised in UK law

Traditionally public interest purposes relate to processing carried out by government bodies, but this article provides an opportunity to expand this to identify what the UK Government considers to be an important public interest so that private as well as public sector bodies can transfer personal data where appropriate. As well as obvious considerations such as those found in article 8(2) of the EU Convention on Human Rights (national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others), DCMS could consider including things such as the fight against doping in sport, and expand the crime prevention aspect to include detection and prosecution.

It may also be helpful to develop some kind of criteria / checklist or assessment process against which an organisation could determine if the public interest criteria is met. This would also assist with articles 6(e) and 9(g) (legal basis for processing); article 17(3)(b) (when the right to erasure does not apply); article 18(2) (when restricted data can be processed); article 20(3) (when the right to data portability does not apply); article 21(6) (when the right to object does not apply); article 35(9) (when a DPIA seeking individual views may be prejudicial); article 36(5) (when prior authorisation is needed); article 49(5) (transfers); and article 86 (public access to documents).

  - Article 49(5): limits to the transfer of specific categories of personal data to a third country or an international organisation for important public interest purposes

To date neither the government nor the ICO has seen fit to bring in blanket restrictions on certain categories of personal data being transferred outside the EU. It is not clear to me that there is a

need to do this now. It would seem to be a provision that will encourage data localisation within the EU, which is not a desirable outcome.

Theme 7 - Sensitive personal data and exceptions

- Article 9 - processing of special categories of personal data
  - Article 9(3): member state law safeguards for processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

The only comment I have on this is to make sure there is no legal gap that prevents employers from carrying out occupational health assessments and reviews.

  - Article 9(4): member state ability to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health

This is a crucial derogation but appears to limit member states to maintaining or introducing conditions for processing sensitive data only in relation to genetic, biometric or health data. The UK has brought in a number of additional conditions for processing sensitive data under the DPA 98 that it is important to maintain.

Existing conditions for processing that relate to health, biometrics or genetic data and should be maintained are as follows.

SI 2000/417:
4 - counselling, advice and support services
5 - insurance business
7 - equality of opportunity (although this is wider than health as it also includes religious or similar beliefs)

DCMS should consider adding additional conditions for processing to cover the following.

- Where the processing of sensitive data is the entire point of the product / service that the individual has chosen to engage with, and so where the requirements for explicit consent (particularly as regards the recent ICO guidance) are unworkable. For example, health and fitness trackers, biometric identity products and services, DNA genetic testing kits.

- Employment context: consent is not considered valid in an employment context, and there may not be adequate provisions in employment law to cover sensitive data processing. For example, biometric access controls for certain high-security buildings or areas.

The other existing UK conditions for processing sensitive data that do not concern health, biometric or genetic data, but which DCMS should seek to maintain if possible, are as follows.

DPA 98 - Schedule 3
7 - administration of justice
7A - fraud prevention (this is particularly crucial to many businesses)

9 - race or ethnic origin for equality of opportunity monitoring

SI 2000/417:
1 - prevention or detection of an unlawful act in the public interest
2 - protection of the public against dishonesty or malpractice in the public interest
3 - combination of 1 and 2 in relation to the special purposes
8 - political opinions for legitimate political activities
9 - research purposes (as per section 33 DPA 98) in the public interest
10 - functions conferred on a constable by any rule of law

2002/2905 as amended by SI 2010/2961: elected representatives

SI 2009/1811: prisoner information to inform an MP about the prisoner and arrangements for the prisoner's release

SI 2012/1978: Hillsborough disaster: this is wider than health and may or may not continue to be needed.

Theme 8 - Criminal convictions

- Article 10 - processing of personal data relating to criminal convictions and offences
  - Article 10: member states can authorise processing of personal data relating to criminal convictions.

As this type of personal data will be separated out and no longer one category on the list of sensitive data processing, it is crucial for DCMS to make sure legitimate uses of this type of data are able to continue. In particular, as a minimum, DCMS should look to replicate the fraud prevention condition for processing for criminal offence data (found in the DPA 98, schedule 3, section 7A).

Separating out criminal record data might though bring benefits as it would allow DCMS to expand the fraud prevention legal basis to include diligence, KYC and AML checks. If this is considered, bear in mind that those who provide the data and services need to be able to use this legal basis as well as the companies carrying out the checks (not all of whom will be directly subject to AML laws and so cannot use GDPR art 9(2)(g) as their legal basis).

DCMS should also make sure that there is a condition for processing criminal offence data in an employment context, both as regards appropriate vetting and the ability to retain information for an appropriate amount of time in a personnel file. GDPR art 9(2)(b) relating to employment law obligations could be replicated for criminal offence dta, providing UK employment law contains these obligations or permissions and meets the requirements of 'providing for appropriate safeguards for the fundamental rights and the interests of the data subject'. Otherwise, DCMS may want to look at replicating the existing employment law condition for processing in DPA 98, schedule 3, section 2.

UK law has an existing condition for processing criminal offence data that DCMS will probably want to maintain:

SI 2006/2068: criminal conviction or offence caution data relating to an indecent photograph or pseudo-photograph of a child necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or for cancelling that payment card

Theme 9 - Rights and Remedies

- Article 17 - right to erasure ('right to be forgotten')
  - Article 17(3)(b): exemption from the right where there is a member state law requiring processing

Presumably, any existing UK laws requiring the retention of data will allow a company to use this exemption to avoid having to delete certain data if requested by an individual exercising the right to erasure. I am not aware of any gaps where a new UK law is needed to require data retention.

- Article 22 - automated individual decision-making, including profiling
  - Article 22(2)(b): exemption from provision where the decision is authorised by a member state law which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests

DCMS may want to consider sectors where automated decisions are made as part of risk assessment and make sure that their practices continue to be legal. For example, with regard to initial and ongoing corporate due diligence that involves checking individuals against watchlists and sanction lists. The safeguards could include that individuals flagged during diligence are referred to individuals for a final decision, where the flag reason requires further analysis. For example, an individual flagged as being established in a country with which the UK is not allowed to trade could legitimately be refused as a customer following automated screening against such a list. However, an individual flagged for fraud convictions or allegations may require further analysis to determine if the flagged issue is relevant or not in the circumstances. Another example would be in relation to risk scoring in the credit and insurance sectors. Safeguards here could include greater transparency as to the data or types of data used to calculate the score, and the ability for an individual to appeal against a decision.

- Article 26 - joint controllers
  - Article 26(1): responsibilities of joint controllers that are determined by member state law

DCMS may want to consider making sure that GDPR rights and responsibilities are built into contracts, bids and tender rules, and other arrangements involving joint controllership between government departments, public sector bodies and in public-private partnerships.

- Article 80 - representation of data subjects
  - Article 80(2): member states may provide that, even if there is no complaint from an individual, a non-profit body has the right to complain to the supervisory authority if it considers that individual rights have been infringed by a controller / processor or legal decision of the supervisory authority

This provision would allow DCMS to provide for non-profit bodies meeting the description in article 80(1) to complain to the ICO on behalf of individuals in general, where no specific individual has complained. This is a proactive ability for a non-profit to flag GDPR infringements or negative impacts on individuals from a supervisory authority decision, in addition to being able to represent specific individuals with specific complaints. DCMS may want to consult established civil society organisations specifically on this point to understand whether they face barriers to effective participation in the debate and resolution of issues, that enabling this provision would remove.

Theme 10 - Processing of children's personal data by online services

- Article 8 - parental consent in relation to a child's use of information society services
  - Article 8(1): member states can lower the age at which parental consent is needed from 16 to no lower than 13

DCMS should lower the age in the UK to 13. This would be consistent with many other rules globally on when parental consent is needed and reflects the current market of online services which are generally only offered to those 13 and above. However, there is a potential gap in that where processing is based on consent under GDPR art 6(1)(a), children under the relevant age need parental consent. But where processing is based on consent under GDPR art 9(2)(a) (sensitive data), no parental consent is needed. This would impact children under the relevant age accessing and availing of online products and services relating to their health or that use biometrics, and relates back to the points made earlier on article 9.

Theme 11 - Freedom of expression in the media

- Article 85 - processing and freedom of expression and information
  - Article 85(1): member states to reconcile the right to the protection of personal data with the right to freedom of expression and information

Presumably, the FOI Act 2000 (in particular section 40, part VII and schedule 6) will need references to the DPA 98 replaced with references to the GDPR to implement this article.

  - Article 85(2): for processing of personal data for journalistic purposes, academic, artistic or literary expression purposes member states can provide exemptions or derogations from the principles, rights, controller and processor obligations, transfers, independent supervisory authorities, cooperation and consistency and specific data processing situations

DCMS will presumably want to maintain the current exemption in section 32 of the DPA 98, but should consult the ICO, as they will be able to demonstrate how it has and has not worked effectively to date, so it can be improved.

Theme 12 - Processing of data

- Article 6 - lawfulness of processing
  - Articles 6(2) and 6(3): member states may maintain or introduce more specific provisions in law for the grounds in art 6(1) (c) (legal obligation) and (e) (public interest or exercise of official authority)

See related comment on public interest above under theme 6. DCMS may want to clarify 'a legal obligation' to make sure the UK's common law approach is accommodated.

- Article 18 - right to restriction of processing
  - Article 18(2): restricted data can only be processed for reasons of important public interest

See related comment on public interest above under theme 6.

- Article 28 - processor

The only reference in this article to member state derogations appears to be the reference in 28(3) and (4) to a legal act other than a contract that governs the processor or exists between the

controller and processor. It is not clear what this might refer to, but presumably in the UK context it could include legal gateways and data sharing arrangements between government / public bodies that do not require a contract to be signed between the parties. DCMS will therefore need to make sure that the processor obligations are incorporated where relevant into these other governance methods.

- Article 29 - processing under the authority of the controller or processor

The only member state derogation in this article appears to be the possibility for member state law to override the controller's instructions and require certain processing of a processor. Presumably this is to accommodate things like statutory retention periods for certain data. I don't think there is a gap that requires further derogations here.

- Article 32 - security of processing

The only member state derogation in this article appears to be the possibility in 32(4) for member state law to override the controller's or processor's instructions and require certain processing of a natural person working for the controller / processor. The obligation in the provision is though on the controller / processor to take steps to make sure this is the case. I'm not sure what circumstances this would cover, but I don't think there is a gap that requires further derogations here.

- Article 35 - data protection impact assessment
  - Article 35(10): member states can provide that a DPIA is still necessary for processing using the legal bases of 'legal obligation' or 'public interest / exercise of official authority' where the origin of the legal basis is an EU or member state law that itself regulates the processing, even where a DPIA has already been done as part of a general impact assessment in the context of the adoption of that legal basis

This would seem to be a derogation to accommodate one or more member states who wished to keep certain existing provisions in their national law. It is not clear what it could apply to in the UK context given our common law approach.

- Article 37 - designation of the data protection officer

See comments on this article already made in theme 4 above.

- Article 86 - processing and public access to official documents

The derogation in this article appears to be another aspect of reconciling FOI and DP law and so should be dealt with in the same way as the other articles on this topic.

- Article 87 - processing of the national identification number

DCMS could consider using this provision to better regulate UK ID numbers such as the National Insurance number, as it is not currently clear what uses can be made of this number, when and by whom.

- Article 88 - processing in the context of employment
  - Article 88(1) and (2): provide more specific rules and safeguards

DCMS may want to consider the opportunity this provision brings to tie together the various GDPR provisions relating to or affecting the employment context. This could provide companies with certainty about what is and is not acceptable processing of personal data for employment purposes. DCMS should consider asking the ICO to update its employment practices code and

supplementary guidance as a priority and to use article 88 GDPR to give it legal status and provide the specific rules and safeguards.

Theme 13 - Restrictions

Article 23 permits member states to legislate domestically measures which restrict the application of various rights and duties under the Regulation. The restrictions may apply to all of the individual rights in articles 12-22, and to the data protection principles in article 5 in so far as they correspond to the Article 12-22 rights. The scope of Article 23 effectively continues similar restrictions that exist under the Current Directive and which were used in the Data Protection Act 1998 (DPA) to shape appropriate exemptions from the requirements of the DPA where that was permissible.

- Article 23 - restrictions

DCMS should look to maintain the restrictions in the DPA 98 that align with possibilities for restrictions in GDPR. Some of the GDPR exemption reasons are wider than the corresponding exemptions in the DPA 98.

  - (a) National security

DPA 98: section 28

DCMS should use the opportunity of this provision to clarify that the exemption only applies to processing necessary to safeguard national security, and is not a blanket provision to cover all processing done by the security and intelligence services, as not all of it will relate to national security. Presumably there will also need to be a link to Directive 2016/680.

  - (b) Defence

DPA 98, schedule 7(2) - this covers the armed forces

  - (c) Public security

DCMS may consider public security as sometimes aligned with national security, as per section 28, and sometimes aligned with prevention and detection of crime, as per section 29.

  - (d) Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

DPA 98: section 29(1)(a) and (b), 29(2)-(3)

Presumably there will need to be a link to Directive 2016/680. Both this Directive and GDPR provide an opportunity to reinforce the case-by-case approach to what we know as the section 29 exemption, as over time it has become used incorrectly by various organisations, including law enforcement, as a blanket provision or legal gateway for disclosures to law enforcement or for those purposes.

  - (e) Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security

Taxation: DPA 98 section 29(1)(c), 29(2)-(5)

Health, education and social work: DPA 98, section 30

  - (f) Protection of judicial independence and judicial proceedings

DPA 98, section 35. DCMS could consider expanding this exemption to cover processing other than disclosure that is required for legal proceedings.

- (g) Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions

DCMS could cover this by adding to DPA 98, section 31.

- (h) Monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g)

Regulatory function: DPA 98, section 31 but would need expanding and rewording.

- (i) Protection of the data subject or the rights and freedoms of others

DCMS may consider this to be partly covered by the 'vital interests' condition for processing, and partly covered by the disclosure obligations involving third-party personal data. However, DCMA may want to consider a specific exemption on this topic, particularly as regards disclosure of personal data.

- (j) Enforcement of civil law claims

DPA 98, section 35

Current DPA 98 exemptions with no apparent GDPR alignment that DCMS should attempt to maintain:

Section 33A: manual data held by public bodies. There is a link to the scope and the need to amend the current definition as regards 'filing system' to align with GDPR article 4(6). There does not appear to be an option in GDPR to provide for exemptions just because the data is manually processed. Consultation with the public sector may though indicate that an exemption is no longer necessary as most records are now electronic.

Section 34: data made public under a legal obligation. GDPR art 14(5)(c) has this exemption but only from transparency and only where the data have not been obtained from the individual.

Section 35A: Parliamentary privilege

Schedule 7: general exemptions relating to a variety of topics

DCMS should use the opportunity of GDPR to remove the notions of the 'subject information provisions' and 'non-disclosure provisions' and instead indicate clearly in the relevant sections of the law what exemptions from which provisions apply.

Theme 14 - Rules surrounding Churches and Religious Associations

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

No comments.