Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's Office (ICO) response to DCMS General Data Protection Regulation (GDPR) derogations call for views

1. The ICO has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), the Privacy and Electronic Communications Regulations 2003, as amended (PECR), and the eIDAS Regulations (2016). We also deal with complaints under the Re-use of Public Sector Information Regulations 2015 (RPSI) and the INSPIRE Regulations 2009. We are independent of Government and uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. We do this by providing guidance to individuals and organisations, solving problems where we can, and taking appropriate action where the law is broken.

2. The DPA is the UK implementing legislation for the current Data Protection Directive 95/46/EC (Directive). As the UK's supervisory authority for the Data Protection Directive, the ICO is a member of the Article 29 Working Party, which is made up of representatives of the 28 EU data protection authorities and the European Data Protection Supervisor, plus observers from Norway, Iceland and Liechtenstein.

3. The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. The Government has confirmed that the UK's decision to leave the EU will not affect the implementation of the GDPR next year.

General comments

4. The GDPR is part of a package, also including the Directive on data protection and law enforcement, which is intended to bring about a harmonious data protection regime across the EU. However, at various points the GDPR provides for national derogations, where Member States can introduce their own national law. Some of these derogations relate to detailed, technical matters. However, others are central to the functioning of an effective data protection regime – for example those dealing with freedom of expression versus privacy or the modification of subject access rights in differing contexts.

5. We welcome the engagement we have had with the Government to date on matters relating to GDPR implementation. The introduction of national derogations is a matter of key significance for us and we would expect continued substantive involvement in this process.

6. It is important that the national discretions available in implementing derogations are considered as part of a proportionate and risk based approach to individuals' information rights. This will ensure that an effective framework for the protection of individuals remains in place.

7. The derogations should be clear in their effect ensuring that there is an effective data protection regime where organisations who must comply understand their obligations and any modifications of these.

8. Our comments are aimed at ensuring this is the case. They are informed by our experience of regulating the current data protection regime together with feedback received from those preparing for GDPR.

9. Our general approach is to favour replicating existing arrangements under the DPA where experience shows that they work satisfactorily. This will minimise disruption and bring certainty and coherence to the data protection regulatory regime. We support the introduction of new derogations only where we believe this to be necessary for the effective functioning of GDPR or where there is a clear need.

Theme 1: Supervisory authority

10. The GDPR requires each Member State to appoint at least one independent national supervisory authority. A supervisory authority (SA) is to take the form of an individual (the 'Member' of the SA) or an authority operating through a Management Board comprising several 'Members' of the SA.

11. We propose that the role of the UK supervisory authority should be fulfilled by the Information Commissioner.

Article 53 (General conditions for the members of the supervisory authority)

12. The Information Commissioner is a corporation sole, currently appointed by the crown. The current appointment arrangements, as specified under Schedule V of the DPA, remain fit for purpose.

13. We acknowledge that these current arrangements may require some revision in order to incorporate new requirements around the requisite qualifications, experience and skills of members of the supervisory

authority. We would advise against an overly prescriptive approach in this area.

Article 54 (Rules on the establishment of the supervisory authority)

14. This Article refers to the term of the supervisory authority (Article 54.1(d)) as well as duties and obligations to which members of the supervisory authority are subject. Our views on this Article mainly relate to how existing obligations are articulated through the DPA, and the opportunity the GDPR provides to ensure these powers and safeguards remain.

15. The GDPR provides an opportunity to ensure that key powers and obligations are extended under national law to cover any other legislation regulated by the Information Commissioner, which may fall outside the scope of the current arrangements.

16. The Information Commissioner is currently appointed for a term not exceeding seven years and may not be appointed for a further term[1]; this arrangement remains fit for purpose.

17. Article 54.1(f) provides for national law to specify the conditions governing the obligations of the staff of the supervisory authority. Senior staff of the supervisory authority should be bound by similar requirements as those imposed on the Information Commissioner by Article 52.3 (incompatible actions).

18. Article 54.2 refers to a duty of professional secrecy that the Information Commissioner and her staff would be subject to with regard to any confidential information which has '*come to their knowledge in the course of the performance of their tasks or exercise of their duties*'.

19. Presently the Information Commissioner and her staff must ensure that any information received during the course of their duties can only be disclosed with lawful authority. This duty of confidence under s.59 of the DPA gives reassurance and confidence to individuals from whom the ICO require information.

20. The precise form of this obligation is subject to national law, and we would wish to continue to be actively involved in discussions around the exact form this may take.

21. Please see our later comments in relation to Article 90 (obligations of secrecy) for more detail on our views around the existing provision in s.58 of the DPA.

[1] Paragraphs 2(1) & (3)(c) Schedule 5 DPA - Amended by Protection of Freedoms Act 2012 (in force 16.3.15)

Article 58 (Powers)

22. The Information Commissioner should retain under GDPR the investigatory, corrective, authorisation and advisory powers currently provided for under DPA.

23. The Information Commissioner also seeks a power to co-operate with other supervisory authorities and enforcement bodies outside of the EEA and beyond those covered by Convention 108, in appropriate circumstances.

24. Any such power would require those other parties to be subject to appropriate safeguards such as a requirement to keep information confidential.

25. It is desirable that this formal power of wider international cooperation on data protection matters would enable the Information Commissioner and her staff to share information with such parties without falling foul of the restrictions in the GDPR derogation that is to operate as the successor to section 59 DPA.

26. By virtue of this provision the Information Commissioner would have the power to disclose information with appropriate 'lawful authority' without breaching the confidentiality requirements to be imposed by Member States under Art 54.2.

27. Assessment notice powers were granted to the Information Commissioner via the Coroners and Justice Act (2009)[2]. The ability to require certain bodies to submit to inspection of their data protection practices is, in our view, an appropriate, necessary and proportionate measure in order to ensure compliance with the regulation, and maintain the confidence of the general public.

28. These requirements should be applicable to all organisations processing personal data, including those currently covered by Regulation 5 of the Privacy and Electronic Communications Regulations (PECR) 2011. This would require amendment to s.41 (a) of the DPA to ensure that it is sufficiently broad to cover all organisations, and so that the existing safeguards apply.

29. We believe that judicial review remains an appropriate and effective safeguard in relation to the Information Commissioner and the exercise of her powers except in instances where there is a route of appeal to

[2] Coroners and Justice Act 2009 amended DPA to introduce s41a (Assessment Notices).

the Tribunal (eg against fines) in which case we consider that the current mechanisms should be retained.

Article 59 (Activity reports)

30. There is a requirement for Member States to provide that the annual report of the Commissioner must be transmitted to the national Parliament and the Government and may be required to be transmitted to other authorities as designated by national law.

31. We suggest that the reporting requirements set out under s.52 of the DPA should form the basis such requirements under the GDPR.

Article 62 (Joint operations of supervisory authorities)

32. Article 62 envisages two separate forms of joint operations and exercise of powers. UK provisions should clarify when, and in what circumstances, powers may be exercised by the staff of a data protection authority from another Member State when working in the UK.

33. Detailed cooperation arrangements could be made according to Article 62 on the basis of a case-by-case assessment. While it may be uncommon, the flexibility to permit another supervisory authority to be involved in an investigation within the UK would be helpful. We envisage that any joint operation in such circumstances, where specialist input is required or requested, would take place under the legal authority of the ICO.

34. UK domestic provisions should therefore allow officers of another supervisory authority to be seconded to the ICO and to exercise legal powers in the UK under the authority of the Information Commissioner. This would be a useful power in relation to any overseas data protection authority – or possibly other regulatory authority - not just supervisory authorities in the EU.

35. Any UK provisions should clarify whether employees of another data protection authority are able to exercise UK powers conferred on them by the Commissioner or, where UK law provides, the powers of their own foreign supervisory/data protection authority (i.e. powers under overseas legislation).

36. In the context of the provision of assistance to other data protection authorities, it could be of practical benefit to provide that the Commissioner has the power to enter into binding agreements with equivalent authorities in other jurisdictions (and not just non-binding

Memoranda of Understanding as the Commissioner may do at present).

Article 90 (Obligations of secrecy)

37. We wish to ensure that the ICO is not hampered in its ability to carry out its regulatory functions by individuals and organisations relying on obligations of confidentiality as a basis for withholding information from the regulator.

38. Section 58 of the DPA currently provides that no enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Information Commissioner with information. Anyone providing information under this provision can take comfort from the fact that the Information Commissioner and her staff, past and present, will commit an offence (see s.59 DPA) if they disclose information received in the course of their duties.

39. This is an extremely important issue for the ICO as, if it is not properly addressed, there is risk that we might be unable to access the information needed to carry out our regulatory investigations.

40. It is important to note that sections 58 and 59 of the DPA as currently drafted apply to the 'Information Acts', being the DPA and FOIA. We repeat our suggestion that any new provisions should also cover any other legislation regulated by the Information Commissioner, which may fall outside the scope of the current arrangements.

Theme 2: Sanctions

Article 36 (Prior consultation)

41. Member state law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to any processing carried out by the controller in the public interest (including processing in relation to social protection and public health).

42. We do not currently see the need for any such requirement in UK law. If the Government wishes to allow future flexibility to address any increased public concern about specific processing activities, then including a provision with an order making power to designate specific processing activities would seem to be appropriate.

Article 58 (Powers)

43. As mentioned in Theme 1 (above), it is important that the Information Commissioner continues to exercise under GDPR all the powers currently available to her under DPA, in addition to new powers as outlined above.

Article 83 (General conditions for imposing administrative fines)

44. Since receiving powers to issue monetary penalties[3] the ICO has issued over 80 penalty notices to date for serious contraventions of the DPA. These notices as issued were for a total in excess of £8 million[4].

45. At present the Information Commissioner is able to apply enforcement criteria to determine whether or not to take enforcement action.

46. It remains an important principle that any fines levied should be 'proportionate' (see Article 83.1 and Article 83.9) and that the power in Article 58.2(i) to impose administrative fines should be "in addition to or instead of measures referred to in this paragraph [(2)], depending on the circumstances of the case". The full range of enforcement corrective measures as set out in Article 58(2), from warnings to fines and orders in respect of infringements, as well as the investigative measures in Article 58(1) such as investigations in the form of data protection audits, should remain available.

47. The ICO wishes to continue to be able to itself impose administrative fines rather than requiring such penalties to be imposed on behalf of the Information Commissioner by the competent national court.

Article 84 (Penalties)

48. The Information Commissioner wishes to see the introduction of an offence prohibiting the intentional reversing or circumvention of technical or organisational measures taken to ensure that data relating to individuals (whether it be personal data, pseudonymised data or other data) are not attributable to identified or identifiable natural persons.

49. The offence should also apply where any person takes steps which reverse or circumvent de-identification measures and is reckless as to whether this results in the re-identification of individuals to whom the data relates. The offence should relate to all data whether processed by public or private bodies and to all processing, not just in respect of

[3] s55a inserted by Criminal Justice and Immigration Act 2008 ,
s55.3(a) inserted by Coroners and Justice Act 2009
[4] https://ico.org.uk/action-weve-taken/

data that is in some way published or made publicly available. The offence should be triable either way with the possibility of a custodial sentence and/or fine.

50. The Information Commissioner should also retain all current powers to issue civil monetary penalties, together with the current DPA powers relating to the execution of warrants, powers of entry and inspection, and associated powers in Schedule 9, the general provisions relating to offences in s.60, and those relating to director's liability in s.61 of the DPA.

51. Section 55 DPA type offences under the GDPR should be recordable offences (serious criminal offences).

52. The Digital Economy Act (2017) provides for the Secretary of State to require a data controller to pay a fee to the Information Commissioner by order. Such payments would replace the current notification fee specified under the DPA.

53. While the regulations under the Digital Economy Act allow for varied provisions, Government may wish to consider additional powers equivalent to the present offence of non-notification in s.21 of the DPA.

54. We draw attention to a concern around the penalty for failing to comply with Notices (in s.47 of the DPA) under GDPR. Whereas a failure to comply under DPA can be an offence, it would appear that the penalty for this will be an administrative fine under GDPR.

55. It is essential that any penalty for a failure to comply is a proportionate and suitable deterrent, in order to assist effective regulation.

Theme 3: Demonstrating Compliance

Article 40 (Codes of conduct)

56. Article 40.5 is similar to the Commissioner's existing duty provided in s.51.4 (b) of the DPA (although referred to there as 'codes of practice').

57. We believe that the GDPR tasks and powers of a supervisory authority, namely in Article 57.1(m), (p) and (q) and powers in Article 58.3(d), are sufficient to enable the code of conduct scheme to operate as required. We do not therefore suggest that this is an area requiring further national level law.

58. We do however note Article 40.6, which requires the supervisory authority to register and publish approved codes of conduct. There are no specific tasks or powers contained within Article 57 and 58 in relation to this function. It may be that the provision in Article 40.6 is sufficient. We would, however, draw attention to parallels with the Commissioner's current obligations to maintain the register of notifications under s.19 of the DPA.

59. Those provisions set out the information that the register should contain and rules around making the information available for inspection and available to the public. We recommend that there should be sufficient flexibility to set up the register of codes of conduct in the way we consider most appropriate.

ICO codes of practice

60. It should be noted that industry-led and supervisory authority approved codes of conduct issued in accordance with Article 40 of the GDPR are different to codes of practice that may be prepared by the Information Commissioner under s.51(3) of the DPA.

61. Whilst the codes of practice envisaged in s.51(4) of the DPA now appear to be covered by Article 40 GDPR, the Information Commissioner would welcome the maintenance of her powers under s. 51(3) in relation to preparing and disseminating appropriate codes of practice for guidance as to good practice. The preparation of such codes of practice is likely to fall within the tasks of Article 57.1(b), (d) and powers under Article 58.3(b).

Article 42 (Certification)

62. Certification is a voluntary process rather than a mandatory compliance obligation for controllers and processors. Supervisory authorities are required to 'encourage' the establishment of certification mechanisms, but are not required to provide them. Supervisory authorities are empowered to issue certifications under Article 58.3(f), but the GDPR does not oblige them to.

63. Tasks contained in Articles 57.1 (n), (o), and powers in 58.3(f) allow for the implementation of Article 42 by the supervisory authority. These provisions could operate effectively without further national law.

64. We note that Article 42.3 provides that certification must be available through a transparent process. The Government could consider whether a power is required in national level law to contribute to the formation of the rules around the certification process. This could take the form of provisions requiring the Information Commissioner to

prepare and issue guidance on how she proposes to exercise her task to develop a transparent certification process under Article 42.

65. This could take a similar form to current provisions under s.55c (1) of the DPA that relate to the preparation of statutory guidance on the issue of monetary penalties.

66. We are considering options for the introduction of a national level certification mechanism in accordance with Article 42. This would involve working with the national accreditation body and approved and accredited external certification bodies who would carry out the evaluation process, rather than certify processing ourselves.

67. Notwithstanding our current intentions, it may be sensible to maintain some broad options. For example, national level law could be useful if the supervisory authority were to act as a certification body. This could cover practical steps, for example, empowering the ICO to charge fees for the costs arising from the operation and administration of certification mechanisms.

Article 43 (Certification bodies)

68. We note the requirement on Member States to ensure that certification bodies are accredited by the supervisory authority and/or a national accreditation body.

69. Under Article 58.3(e), the supervisory authority has the power to accredit certification bodies. Article 57.1(q) provides that the supervisory authority *shall* conduct the accreditation of the certification body pursuant to Article 43. However, we acknowledge the potential conflict of Article 43.1(a) with the provisions in Regulation (EC) 765/2008 that appoint a sole national accreditation body (i.e. United Kingdom Accreditation Service in the UK).

70. It is important that the supervisory authority has the discretion to choose whether or not it accredits certification bodies (i.e. that this should be read as a power, not as a task).

71. In developing plans for certification under the GDPR in the UK, our preference is to work in partnership with the national accreditation body to accredit approved certification bodies, rather than carrying out accreditation itself. That said, at this early stage we would prefer the flexibility to not rule out the possibility of accrediting certification bodies in future.

72. We know that a number of other supervisory authorities would prefer to work in partnership with their national accreditation body. We are

also aware that a small number of Member States intend to include national law provisions to stipulate procedural rules relating to the accreditation of certification bodies. For example, this includes:

- To clarify who conducts accreditation of certification bodies, given the choice provided by the GDPR in Article 43.1 (the national accreditation body named in accordance with Regulation (EC) 765/2008 or the competent supervisory authority, or both); and,

- the cooperation process between the supervisory authority and the national accreditation body – including, for example, that the supervisory authorities have the right to accredit certification bodies within their jurisdiction on the basis of an expert assessment by the respective national accreditation body.

Theme 4: Data Protection Officers

73. Under Article 37.1, data controllers and processors will be required to designate a Data Protection Officer (DPO) where processing is carried out by a public authority or body.

74. As GDPR does not define 'public authority or body' there is potential for this provision to lead to uncertainty and inconsistency in its application.

75. This could be addressed by a statutory definition for the purposes of data protection legislation or via guidance. Consideration should be given to existing definitions in other statute in order to avoid confusion (e.g. definitions of public authorities in the FOIA and EIR).

76. We are mindful that the benefits of a consistent definition need to be considered against the potential burdens such a requirement could place on organisations under a common definition. An example of this is GPs and other small organisations, who currently meet the definition of public authorities under the FOIA.

77. Any provision should be sufficiently flexible, perhaps allowing for the addition of certain data controllers as required under order. Defining a public body in relation to certain types of processing or processing for a particular purpose rather than due to their legal status as public or private might be considered.

78. Some data controllers or processors may want to appoint a DPO, regardless of whether they are obliged to under GDPR.

79. The Information Commissioner does not currently envisage any circumstances other than those under Article 37.1 in which a

requirement to appoint a DPO should be expressly designated in law. However, if the Government wishes to allow future flexibility to address this issue, implementing legislation could provide for the Secretary of State to require this by order, in specified circumstances.

80. With regard to the position of the DPO, more specifically the obligation to secrecy in accordance with Member State law (Article 38.5), this obligation should perhaps be contractual rather than being expressly provided for in UK legislation.

Theme 5: Archiving and research

81. Article 89 provides for national derogations from data subject rights in relation to personal data processed for research and archiving purposes. This position is similar to the existing provision under DPA Part IV, namely the research, history and statistics exemption (s.33).

82. We think the basic principle that rights can be dis-applied where the collection of data (whether processed for scientific, historical or archival purposes) has no direct effect on any individual remains valid. This can be 'read across' to include access, rectification, restriction and objection – plus portability in the case of archival processing.

83. The exemption in s.33 DPA should be replicated as far as possible under the GDPR.

Theme 6: Third country transfers

84. This theme is in relation to Article 49, and concerns transfers of personal data outside the EEA where none of the other permitted bases for transfer apply. Article 49.1(d) refers to transfers necessary for important reasons of public interest. Article 49.4 provides that the public interest referred to in (d) shall be recognised in Union law or in the law of the Member State to which the controller is subject.

85. We would not anticipate that UK data protection legislation would seek to identify the circumstances in which transfers may be made in the public interest.

86. Instead, the provision in Article 49.4 should be read as allowing for transfers in respect of which it is possible to identify the public interest in the transfer by reference to the stated aims for which the data is being processed and consideration of whether such aims outweigh any impact such transfer might have on the fundamental rights of individuals or legal persons.

Theme 7: Sensitive personal data and exceptions

87. Article 9.2(g) states that Member States may authorise the processing of special category personal data without data subject consent for reasons of substantial public interest, subject to safeguards.

88. We have recently considered the processing of special category personal data by internet search providers for the purposes of providing access to information on the internet. It is presently difficult to identify the legal basis (e.g. a schedule 3 condition in the DPA) that can be satisfied when search engines on which the process of special categories of personal data.

89. Processing for the purpose of providing internet search facilities might be an area where processing should be authorised by Member State law where it is necessary in a substantial public interest.

90. In the interests of future-proofing UK data protection legislation, any new legislation to implement the UK derogations from the GDPR might empower the Secretary of State to authorise by order the processing of special category personal data for reasons of substantial public interest.

91. Presently, processing of special category personal data for the purposes of medical research is covered by the condition for processing as set out in paragraph 8 of schedule 3 DPA.

92. The corresponding basis for processing under GDPR (9.2(h)), although in some way more extensive, does not explicitly reference the purpose of medical research.

93. It is our understanding, from Recital 53 and Article 9.2 that this is an area subject to derogation, subject to suitable and specific safeguards. Given the clear public interest in processing for this purpose, we recommend that this is incorporated into any UK enacting legislation for GDPR.

Theme 8: Criminal Convictions

94. Article 10 permits the processing of personal data relating to criminal convictions and offences under the control of official authority or when processing is authorised by national law.

95. Information relating to the commission, alleged commission or prosecution of offences is presently considered sensitive personal data under sections 2.g-h of the DPA.

96. Our understanding is that as written, Article 10 may present difficulties for certain data controllers such as employers, when recruiting for positions not presently referenced in applicable national law.

97. At present employers can ask an applicant to disclose their criminal history when applying for a job. National law allows for safeguards in how the applicant interprets that request in their particular situation, and with reference to the status of the role advertised. These safeguards operate slightly differently in Scotland and Northern Ireland.

98. While the current disclosure regime as set out in Part V of the Police Act 1997 would meet the requirement of Article 10, this threshold is unlikely to be met by the majority of employers requiring a declaration from applicants, who cannot rely on other national law.

99. The Government may wish to consider this alongside reviews of the current safeguards to the disclosure regime (i.e. filtering).

100. We also recognise the legitimate interest that some data controllers (e.g. banks and retailers) may claim in order to retain data about ex-employees dismissed and successfully prosecuted for relevant offences (i.e. theft). Consideration is needed as to how best to address data controllers' legitimate concerns whilst protecting privacy rights.

101. We recognise the danger of unfair 'blacklisting'; however the data protection principles and other parts of the GDPR should ensure sufficient protection against that. We can see that it can be legitimate under certain circumstances for non-public authorities to retain records of individual's criminal convictions subject to proper safeguards.

102. Unduly restricting access to such data may allow individuals to censor their histories to present a misleading picture of themselves and thereby facilitate further fraud or other unlawful behaviour.

Theme 9: Rights and remedies

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

103. Under Article 17.1(e) the data subject shall have a right to erasure of personal data where erasure is required under a provision of Member State law to which the controller is subject.

104. This provision would allow erasure where for example the information in question is found to be defamatory, incites racial or other unlawful hatred or is part of a campaign of unlawful harassment.

105. It is our view that it would appear unlikely that any express reference to such prohibitions would need to be made in the UK implementing legislation. We are satisfied that the general right to erasure provides sufficient protection to individuals.

Article 22 (Automated decision making, including profiling)

106. Clarification would be welcome on whether, in the UK, the Member State law referred to in Article 22.2(b) will relate to processing carried out on the basis of Article 6.1(e) (*processing necessary for performance of a task carried out in the public interest/in the exercise of official authority*) as well as Article 6.1(c) (*processing necessary for compliance with a legal obligation*).

107. The first sentence of Recital 45 says that Member State law can cover both. If it is the Government's intention to derogate for both bases for processing, this would mean that automated decision making (ADM) could be available to public authorities when they are exercising their powers as well as when they are complying with their duties.

108. It might be envisaged that ADM could be necessary for a duty such as fraud prevention, but less obvious how it would be necessary for exercising a power. In both cases any national legislation would be required to specify suitable safeguard measures, in compliance with Article 22.2(b) and Recital 71.

109. We also note that Recital 45 says that it is a matter for Member State law to say whether Article 6.1(e) can apply to bodies other than public authorities.

110. Further clarity would be welcome on whether Government intends to legislate in this area.

Article 26 (Joint Controllers)

111. The GDPR provides that Member States can by law determine the respective responsibilities of joint data controllers.

112. The current ICO guidance relating to joint data controllers envisages joint data controllers determining their respective responsibilities between themselves. We do not believe there is a need for national law in this regard.

Article 80 (Representation of data subjects)

113. Civil society organisations already perform a valuable role in identifying information rights concerns and drawing these to the ICO's attention. This has resulted in the ICO taking formal enforcement action. If someone wishes a civil society body, for example, to lodge a complaint on their behalf with the ICO then we would consider this in our existing way.

Theme 10: Processing of children's personal data by online Services

114. The GDPR provides that a child under the age of 16 cannot give valid consent to the processing of their personal data for the provision of the service, unless the law of their Member State provides a lower age (to be no lower than 13). The use of this discretion should be consistent with wider public policy in all parts of the UK on the autonomy of the child and the age when they can acquire and exercise rights for themselves. The ICO's submission to the House of Lords Select Committee on Communications' Inquiry into Children and the Internet makes clear that, on balance, we favour an approach where even quite young children can access appropriate online services without the consent of a parent or guardian, provided organisations have other safeguards.

Theme 11: Freedom of expression in the media

115. Under Article 85 Member States shall create exemptions in relation to the processing of personal data for journalistic purposes and for academic, artistic or literary expression.

116. The ICO's view is that most of the key elements of sections 32, 45 and 46 of the DPA should remain, though reviewing whether all the exemption provisions, particularly related to enforcement, remain necessary and proportionate.

Theme 12: Processing of data

Article 6 (Lawfulness of processing)

117. Article 6.2 states that Member States may maintain or introduce more specific provisions to adapt the rules of the GDPR with regard to processing for compliance with (c) (*processing necessary for compliance with a legal obligation to which the controller is subject*) or (e) (*processing necessary for the performance of a task carried out in*

the public interest or in the exercise of official authority vested in the controller).

118. We are confident that we can assess 'legal duty' and 'public interest' on a case-by-case basis and without any need for the introduction of national law.

Article 18 (Right to restriction of processing)

119. Article 18 introduces a right for the data subject to restrict processing of their personal data. Where such a restriction has been applied the data may only be processed (otherwise than by storing the data) in limited circumstances, including where such processing is necessary for reasons of important public interest or the Union or a Member State. The existing provisions in the GDPR seem sufficient and we see no need to introduce national law.

Article 28 (Processor)

120. Articles 28.3 and 28.4 provide that processing by a processor or sub-processor is to be governed by a contract or other legal act under Union or Member State law.

121. The ICO would envisage the requirements for controller/processor contracts currently set out in Schedule 1 Part II paragraphs 11 & 12 DPA to be replicated under the new implementing legislation.

Article 29 (Processing under the authority of the controller or processor & Article 32 - Security of processing)

122. The ICO wishes the provisions set out in schedule 1 part II paragraphs 11 & 12 DPA to be replicated under any implementing legislation.

Article 35 (Data protection impact assessment)

123. We do not think it necessary to introduce derogation into UK law regarding obligations to complete a data protection impact assessment (DPIA).

124. We believe DPIAs to be a useful tool for data controllers even where there is a legal obligation to carry out the processing or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Article 37 (Designation of the data protection officer)

125. Please refer to our comments under '*Theme 4 - Data Protection Officers*' above.

Article 86 (Processing and public access to official documents)

126. Article 86 allows for the principle of public interest in access to official documents to be a consideration when applying GDPR, and requires Member States to reconcile public access to official documents with data protection rights.

127. It says that Member States may provide by law for public access to personal data in official documents held by a public authority or body, and processed for the performance of a task in the public interest, in order to allow public access to those documents.

128. It will be necessary to re-assess the provisions in the FOIA and EIRs (which provide for personal data to be exempt from the right of access where the disclosure of such information would breach any of the principles) in the light of Article 86 GDPR.

Article 87 (Processing of the national identification number)

129. Member states may further determine the specific conditions for the processing of a national identification number or any other identifier of general application.

130. We see no need at present for the introduction of any further conditions in respect of the processing of this form of personal data.

Article 88 (Processing in the context of employment)

131. Member states can (by law or collective agreements) provide for more specific rules to ensure the protection of rights and freedoms in respect of the processing of employee's personal data in the employment context, including specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.

132. We are aware of concerns relating to the processing of personal data about individuals without their knowledge in the context of recruitment exercises. The Article allows for the UK to introduce measures to regulate such processing. It may be appropriate to address these concerns in a statutory code concerning employment practices.

133. We would wish employers to follow the same data protection rules as other data controllers. Otherwise the situation could be confusing for both employers and their employees.

Theme 13: Restrictions

134. The UK may, by way of a legislative measure, restrict the scope of the obligations and rights provided for in Articles 12 to 22 (rights of the data subject) and Article 34 (communication of data breach to data subject) as well as Article 5 (data processing principles) in so far as its provisions correspond to the rights and obligations provided for in Articles 12-22.

135. In order to support data controllers when responding to data subjects exercising their Article 15 rights (Right of access), it is important that a number of restrictions as currently set out in the DPA are maintained. These are namely those described in s.7 (3) (verifying the identity of the requestor), 7(4) (personal data relating to a third party) and 8(3) (obligation to comply with subsequent identical or similar requests) and the exemptions in Part IV of the DPA.

Theme 14: Rules surrounding churches and religious associations

136. Article 91 allows for the continuation of existing church or religious association or community comprehensive rules relating to the processing of personal data.

137. We are not aware of any such rules currently being applied in the UK and therefore provisions relating to the continuation of such rules are not relevant in UK legislation.

10 May 2017