EVALUATION OF THE GDPR UNDER ARTICLE 97 – QUESTIONS TO DATA PROTECTION AUTHORITIES / EUROPEAN DATA PROTECTION BOARD

ANSWERS FROM THE UK SUPERVISORY AUTHORITY

The General Data Protection Regulation ('GDPR') entered into application on 25 May 2018, repealing and replacing Directive 95/46/EC. The GDPR aims to create a strong and more coherent data protection framework in the EU, backed by strong enforcement. The GDPR has a two-fold objective. The first one is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The second one is to allow the free flow of personal data and the development of the digital economy across the internal market.

According to Article 97 of the GDPR, the Commission shall submit a first report on the evaluation and review of the Regulation to the European Parliament and the Council. That report is due by 25 May 2020, followed by reports every four years thereafter.

In this context, the Commission shall examine, in particular, the application and functioning of:

- Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC; and
- Chapter VII on cooperation and consistency.

The GDPR requires that Commission takes into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources. The Commission may also request information from Member States and supervisory authorities. As questions related to Chapter VII concern more directly the activities of the DPAs, the present document focuses primarily on that aspect of the evaluation, while also seeking their feedback on Chapter V related issues.

We would be grateful to get the replies to the questions (in English) at the following e-mail address: JUST-EDPB@ec.europa.eu.

Please note that your replies might be made public.

When there are several DPAs in a given Member State, please provide a consolidated reply at national level. In the context of the preparation of the evaluation report, and following the input from other stakeholders, it is not excluded that we might have additional questions at a later stage.

I. CHAPTER V

The GDPR provides that the adequacy decisions adopted by the Commission under Directive 95/46 remain in force under the GDPR until amended, replaced or repealed. In that context, the Commission is tasked to continuously monitor and regularly evaluate the level of protection guaranteed by such decisions. The 2020 evaluation provides a first opportunity to evaluate the 11 adequacy decisions adopted under the 1995

Directive. This does not include the decision on the Privacy Shield that is subject to an ad hoc annual review process and the Japanese adequacy decision that was adopted last year under the GDPR and is also subject to a specific evaluation exercise (the first one will be in 2021).

1. **Has any stakeholder raised with your authority any particular question or concern regarding any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is not covered by this evaluation process)?**

The ICO was involved in Working Party 29 throughout the process that supported adequacy decisions under the 1995 Directive. Therefore any issues raised with us by stakeholders informed our engagement as the process took place and concluded. We have no further points to add at this stage.

2. **Does your authority have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?**

As stated above, the ICO has been involved in Working Party 29 throughout the process that supported adequacy decisions under the 1995 Directive. Therefore our understanding of individual country's data protection systems informed our engagement as the process took place and concluded. We have no further points to add at this stage.

3. **In your view, should any third country or international organisation be considered by the Commission in view of a possible adequacy decision?**

Whilst we would not propose specific countries or organisations we would suggest that criteria such as where digital flows lie, the volume and importance of trade with the EU and law enforcement factors should be taken into account when prioritisation decisions are made.

II. CHAPTER VII

The GDPR provided for one single set of data protection rules for the EU (by a Regulation) and one interlocutor for businesses and one interpretation of those rules. This "one law one interpretation" approach is embodied in the new cooperation mechanism and consistency mechanisms. In order to cooperate effectively and efficiently the GDPR equips the Data Protection Authorities (thereafter the DPA/DPAs) with certain powers and tools (like mutual assistance, join operations). Where a DPA intends to adopt a measure producing effects in more than Member State, the GDPR provides for consistency mechanism with the power to ask for opinions of the European Data Protection Board (EDPB) on the basis of Article 64(1) and (2) GDPR. In addition, in situations where the endeavour to reach consensus in the cases of one-stop shop (OSS) does not work (i.e. there is a dispute between the DPAs in specific cases), the EDPB is empowered to solve the dispute through the adoption of binding decisions.

In this context, the Commission finds it appropriate to request the views of the DPAs / EDPB on their first experiences on the application of the cooperation and consistency mechanisms. To this aim, the Commission established the list of questions below, in order to help the DPAs framing their input. It is understood, that the Commission is also interested in any comments the DPAs may have which goes beyond the answer to the questions and which concerns the application of the two above-mentioned mechanisms.

1. Cooperation Mechanism

1.1. OSS – Article 60

a. Has your DPA been involved in any OSS cases? If so, in how many cases since May 2018?

The UK has been involved in 18 cases where it is the LSA and 20 where it is a CSA.

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them

One obstacle that sometimes arises is due to the different investigative methods used by other Supervisory Authorities (SAs). The ICO has a very high volume of cases and therefore adopts a pragmatic approach to resolve these matters in the most efficient manner. Occasionally this may mean that where a minor infringement may have occurred (e.g. late response to a right of access request) we may simply remind the data controller of their obligations and ask that they respond to the complainants request. Other SAs may experience smaller numbers of cases or for other reasons wish to perform a more in-depth legal analysis of the case at hand. This can often lead to elongated timescales where the ICO would accept an expedited response if it resulted in a resolution for the data subject. Additionally this can also result in different approaches by SAs (e.g. fines or reprimands) to individual cases.

c. How would you remedy these problems?

The ICO favours to continue having open and honest discussions amongst SAs and greater transparency in investigative approaches to manage expectations and promote consistent outcomes.

d. Is your national administrative procedure compatible with the OSS? (e.g. do you identify a clear step which can be referred to as a "draft decision"…?

Yes, the ICO creates assessments of cases which are notified to controllers when the officer is in a position to do so. To accommodate the OSS mechanism, before these are issued to the controllers, these assessments are considered draft decisions for IMI cases and are shared through the cooperation mechanism.

.. Are the parties heard before you produce such draft decision?)

In complaint cases the ICO will assess information (evidence) provided by the complainant and, if sufficient, will raise the data protection concern with the controller. The controller has a right to respond to the complaint raised and can provide their understanding of the situation. The ICO will then consider the information provided by both parties to determine whether an infringement of the GDPR has taken place.

e. Were you in the situation of the application of the derogation provided for in Article 56(2) GDPR (so-called "local cases", i.e. infringements or complaints relating only to an establishment in your Member State or substantially affecting data subjects only in your Member State)?

The ICO has both requested to handle cases locally and has accepted requests from other SAs to handle cases locally. We support the local case handling process and believe it has an effective role to play in order to reduce the burden on some authorities who receive very high volumes of cases from other EU countries.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?

Timescales of resolution to data subject complaints have been a re-occurring theme. However, the ICO is sympathetic to SAs who are receiving high volumes of cases or who are not as familiar with high volume complaint handling pre-GDPR. We have noted a possible overuse of informal consultations to update on cases where a draft decision could simply be issued and reviewed. As previously noted, where the ICO is seeking a resolution for its complaints, we feel the difference in approach over complaint handling is delaying some cases where the ICO could (and would) accept a simpler resolution i.e. simply a notification to the controller in question.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?

Yes, to provide information to other authorities via a secure channel. Specifically Voluntary Mutual Assistance.

b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?

We have not used the Mutual assistance to monitor the actions taken by another authority.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?

Yes, it allows for the secure transfer of information to other authorities and to raise questions. Our only concern may be the volume of GDPR policy-based questions we have received in the past about our interpretation of the legislation. The ICO has published a significant amount of guidance and often the answers to these questions are available via publications on our website. We appreciate other SAs would like to know how each member state interprets the GDPR, but it can often take time to monitor, track and provide responses to these queries.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?

The use of this tool requires that a case register for the controller in question first be set up. Sometimes where there is no case register, the SA will set one up in order to ask questions. We think it should only be the LSA who sets up and manages case register entries for controllers in their jurisdiction. There is no simple way to remedy this. Indeed if you allow for Article 61 requests to be triggered on an ad-hoc basis then you wouldn't have them all linked back to one central register.

1.3. Joint operations – Article 62

a. Did you ever use this tool (both receiving staff from another DPA or sending staff to another DPA) in the case of carrying out and investigation?

At the present time, the ICO has not used Article 62 to receive or send staff to another authority for the purpose of carrying out an investigation.

However, the principles set out in Article 62 are something the ICO views as a positive tool and one which it actively seeks opportunities to deploy.

Outside of Article 62, the ICO has facilitated both subject matter and case specific secondments of staff with other DPAs and have found these to be mutually beneficial to our operational work.

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?

No.

c. Is it effectively facilitating your work? If yes, how? If not, why?

As stated previously, we have not used Article 62. However, we can see a range of benefits to doing so and are actively seeking opportunities to work with other DPA's jointly, by way of using this tool. We see particular opportunities to leverage investigative skills, technical expertise and benefit from increased bandwidth of available resources in the event where there was a suitable case for which to use Article 62.

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?

As stated previously, we have not used Article 62 before. However, we anticipate the following potential challenges in respect of the use of Article 62 in practice:

- The legal authority and basis for delegation of the Commissioner's powers (in the case of the ICO) to the seconded person in order for them to act on her behalf in conducting investigations;
- Putting in place appropriate controls regarding the exchange of information (in the case of the ICO – determining how section 132 of the Data Protection Act 2018 will operate in practice for seconded staff)
- Potential cost, resilience and resourcing challenges that arise.

2. Consistency mechanism

2.1 Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)?

Yes the ICO has submitted cases for decision by the Board under Article 64(1) to request opinions of Binding Corporate Rules (Article 47), Data Protection Impact Assessments (35(4), Accreditation Certification for Codes of Conduct (Article 41(3) and Additional Accreditation Certification (Article 43(1)(b)).

b. Did you ever submit any draft decision to the Board under Art 64(2)?

No

c. Did you have any problems by complying with the obligations under Article 64(7) GDPR, i.e. taking outmost account of opinion of the EDPB? If so please describe them.

No- we have not received any unfavourable responses to the triggered articles and any additional actions required had already been discussed with the relevant individuals (ICO and EDPB) via phone or email.

For the BCR we obtained a positive opinion, therefore we had no comments to make and communicated to the Board that we intended to follow the opinion of the Board.

However we are mindful that, should this not be the case and an opinion is communicated that we do not intend to follow or we intend to amend our draft opinion, the timeframe of 2 weeks would be insufficient to comply in the case of BCRs in our view.

For the DPIA an initial EDPB response suggested errors in our opinion. However subsequent discussion with relevant individuals resolved the issue in ICO's favour.

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?

Yes- All documents required to provide the relevant context to the decision would be added into the IMI system as part of the supporting information depending on the nature of the decision.

e. Were there any issues concerning the translations and/or any other relevant information?

No.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?

For the most part, yes. However requirements of local legislation of each SA may impact on this. Expectations of different SAs regarding outcome (i.e. when to fine, reprimand) can also highlight differences in approach.

2.2 Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?

No.

b. Which documents were submitted to the EDPB?

Not applicable.

c. Who prepared the translation, if any, of that documents and how much time did it take to prepare it? Were all the documents submitted to the EDPB translated or only some of them?
Not applicable.

2.3 Urgency Procedure – Article 66

a. Did you ever adopt any measure under urgency procedure?

No.

3. Exchange of information: Standardised communication

a. What is your experience with the standardised communication through the IMI system?

No issues noted.

4. **European Data Protection Board**

a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?

ICO participates in all EDPB Subgroups and task forces.

For the EDPB, ICO was previously a co-rapporteur on:

- EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects
- EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)
- EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation
- EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation
- EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - version adopted after public consultation

Contributions to other EDPB Documents include:

- EDPB Statement 2/2019 on the use of personal data in the course of political campaigns
- Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan
- EDPB pleading before the CJEU in Case C-311/18 (Facebook Ireland and Schrems) - 9th July 2019

In addition, ICO had been a Lead Rapporteur or Co-rapporteur on WP 29 Guidelines endorsed by EDPB:

- Guidelines on consent under Regulation 2016/679, WP259
- Guidelines on transparency under Regulation 2016/679, WP260
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251
- Guidelines on Personal data breach notification under Regulation 2016/679, WP250
- Guidelines on the right to data portability under Regulation 2016/679, WP242

- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248
- Guidelines for identifying a controller or processor's lead supervisory authority, WP244
- Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
- Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253

b. *For the EDPB Secretariat*: Can you provide an indicative breakdown of the EDPB Secretariat work and allocation of resources (full-time equivalent) according to the tasks listed in Article 75?

5. Human, technical and financial resources for effective cooperation and participation to the consistency mechanism

a. How many staff (full-time equivalent) has your DPA? Please provide the figures at least for 2016, 2017, 2018, 2019 and the forecast for 2020.

2016	409
2017	439
2018	505
2019	680
2020	714

b. What is the budget of your DPA? Please provide the figures (in euro) at least for 2016, 2017, 2018, 2019 and the forecast for 2020.

2016	Euro 26.3m
2017	Euro 28m
2018	Euro 30m
2019	Euro 52m
2020	Euro 61m (forecast)

c. Is your DPA dealing with tasks beyond those entrusted by the GDPR? If yes, please provide an indicative breakdown between those tasks and those entrusted by the GDPR.

List of legislation we cover (as set out in ICO Regulatory Action Policy):

- Data Protection Act 2018 (DPA);
- General Data Protection Regulation (GDPR);
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);
- Freedom of Information Act 2000 (FOIA);
- Environmental Information Regulations 2004 (EIR);
- Environmental Protection Public Sector Information Regulations 2009 (INSPIRE Regulations);
- Investigatory Powers Act 2016;
- Re-use of Public Sector Information Regulations 2015;
- Enterprise Act 2002;
- Security of Network and Information Systems Directive (NIS Directive); and
- Electronic Identification, Authentication and Trust Services Regulation (eIDAS).

Whilst we have not undertaken a formal breakdown of activity against these legislative requirements, it should be noted that the recent (since 2017) increase in ICO staff complement and budget was undertaken to ensure we are able to fully discharge our GDPR oversight function.

d. How would you assess the resources from your DPA from a human, financial and technical point of view?

ICO is assessed to have the appropriate human, financial and technical resources to enable it to fully discharge its regulatory responsibilities under GDPRP and UK legislation.

More specifically, is your DPA properly equipped to contribute to the cooperation and consistency mechanism? How many persons work on the issues devoted to the cooperation and consistency mechanism?

Yes, the ICO is properly equipped. As well as the ability to reach out to the wider ICO we have also established focused roles to allow full and effective contribution to the cooperation and consistency mechanism. These roles act as conduit and coordination point and include:

- A manager whose role includes the oversight and operationalisation of the system.
- A lead intelligence officer whose role includes IMI handling but also has wider responsibility within the intelligence function.
- A complaints case officer who is trained to generate complaint cases received by the ICO in the IMI system alongside their investigative role.
- As of the end of November 2019, one lead case officer who will be dedicated to undertaking international cases received via the IMI.
- A Principal Policy adviser and Senior Policy Officer also involved in coordination of these procedures regarding coordination at EU level/ cooperation issues discussed at EDPB.

6. Enforcement

a. How many complaints (excluding request for information) did you receive since May 2018? What kind of communication with you/request do you qualify as a complaint?

The total number complaints to the end of November 2019 since 25th May 2018 is 64,667.

In addition to complaints, this year-to date, the ICO's Investigation Team has opened 1,333 cases relating to potential infringements of the GDPR / DPA2018, the majority of which have been reported to the ICO proactively in accordance with Article 33.

There is no clear definition of a complaint defined in the UK Data Protection Act 2018. However the act mirrors the wording of the GDPR in that it allows data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the GDPR. In this context the DPA 2018 provides that the Commissioner must take appropriate steps to respond to the complainant, inform the complainant of the outcome of the complaint, inform the complainant that they have a right to approach a tribunal if 3 months have passed with no action been taken, and if asked to provide the complainant with further information about how to pursue the complaint. The DPA 2018 states that appropriate steps to respond to the

complaint include investigating the subject matter to the extent appropriate. It is intentionally broad and gives the Commissioner discretion in this area.

b. Which corrective powers did you use since May 2018?

Since the implementation of GDPR and in relation to the GDPR/DPA 2018 the ICO has issued[1]:

- 3 'Notices of Intent' in relation to its intention to issue monetary penalties in accordance with Article 83 of the GDPR;
- 2 Enforcement Notices
- 6 preliminary Enforcement Notices, which signal an intention to move to an Enforcement Notice, under consideration;
- 16 reprimands across a wide variety of sectors;
- 4 warnings;

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?

No. Although we do not have a formal outcome of our complaints as "amicable settlement" we do try and reach an informal agreement between the data subject and the data controller to resolve matters when it is appropriate to do so. For example, where the data subject is yet to receive a response to an access request, but there is no indication that the data controller is not going to reply.

d. How many fines did you impose since May 2018? Please provide examples.

At the time of writing, the ICO has several potential fines in the latter stages of consideration, but final penalty notices have not yet been issued.

e. Which attenuating and or aggravating circumstances did you take into account?

The ICO considers mitigating or aggravating circumstances in line with Article 83 and its Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf)

7. Additional questions from EU Commission

a. National statistics on data breaches (from 25 May 2018 until 30.11.2019)

14,000 personal data breaches were reported the 12 months post implementation of GDPR, a 300% increase on the previous year.

[1] **Definitions:**
Notice of intent: intent to issue a financial penalty (not defined in legislation)
Assessment Notice: "The Commissioner may by written notice (an "assessment notice") require a controller or processor to permit the Commissioner to carry out an assessment of whether the controller or processor has complied or is complying with the data protection legislation". (DPA 2018; Part 6; Section 146; subsection 1)
Enforcement Notice: "Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person— (a)to take steps specified in the notice, or (b) to refrain from taking steps specified in the notice, or both". (DPA 2018; Part 6; Section 149; subsection 1)

Until 30 November 2019, we have received approximately 21,000 reports.
Around 37% of breaches reported came from the following three sectors:

- Healthcare – 18%
- Education – 13%
- Finance/Insurance and Credit – 6%

b. National initiatives to give guidance to SMEs or any other specific support to the SMEs.

An overview of the ICO's SME Specific guidance and support can be found via https://ico.org.uk/for-organisations/business/

Specific support for SMEs includes:

- A micro business resource page: https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/
- A number of small business FAQs for different sectors (small hospitality businesses; small retailers): https://ico.org.uk/for-organisations/in-your-sector/business/#FAQS
- A self-assessment for small business owners and sole traders: https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/
- A number of data protection self- assessment checklists for these areas:
    1. Controllers checklist
    2. Processors checklist
    3. Information security
    4. Direct marketing
    5. Records management
    6. Data sharing and subject access
    7. CCTV

  https://ico.org.uk/for-organisations/data-protection-self-assessment/

- A privacy notice template: https://ico.org.uk/media/for-organisations/documents/2259798/pn-template-microbusiness-201908.docx
- An advice helpline for small organisations: https://ico.org.uk/global/contact-us/advice-service-for-small-organisations/
- A checklist on Subject Access Requests for SMEs: https://ico.org.uk/for-organisations/business/sar-checklist-for-smes/