The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

24 July 2024

IC-313517-W1K5

Request

You asked us:

1. *At what point did the ICO begin drafting the guidance, and on what date was it completed?*
2. *Was the ICO's own use of Azure for LE processing considered when producing the guidance?*
    a. *What steps it has the ICO taken to address its own LE processing on Azure?*
    b. *Is the ICO constrained by Section 73(4) of the DPA from sending this type of data outside of the UK to an IT service provider?*
3. *Although the ICO outlines additional processions it believes could make the hyperscale processing of police data legal, it is very clear that the "advice we have provided is under our general duty to provide advice and support and does not constitute approval for the roll out or assurance of compliance under data protection law. The advice does not compromise our ability to use our regulatory powers in the future should any infringements come to light."*
    a. *Have either Microsoft or PSoS conducted a transfer risk assessment and is an International Data Transfer Agreement in place for DESC, as per guidance sent from the ICO? Has the ICO seen these assessments directly?*
    b. *CW has been told that both the IDTA and SCCs are mechanisms rooted in GDPR, and that it is not therefore clear how they can be applied to the strict law enforcement-specific rules laid out in Part Three – which specific provisions in either mechanism are directly related to Part Three?*
4. *Did the ICO itself seek legal advice to inform its guidance for Police Scotland and DESC partners? If so, what is the source of this advice?*
5. *Further FOI disclosures contain details of discussions between Microsoft and the Scottish Police Authority (SPA), in which the tech giant admitted it*

cannot guarantee the sovereignty of UK policing data hosted on its hyperscale public cloud infrastructure

   a. *Specifically, it showed that data hosted in Microsoft infrastructure is regularly transferred and processed overseas; that the data processing agreement in place for DESC did not cover UK-specific data protection requirements; and that while the company has the ability to make technical changes to ensure data protection compliance, it is only making these changes for DESC partners and not other policing bodies because "no-one else had asked."*
   b. *The documents also contain acknowledgements from Microsoft that international data transfers are inherent to its public cloud architecture.*
      i. *At what point did the ICO become aware of that Microsoft cannot guarantee the sovereignty of UK policing data?*

6. *Is the ICO aware of what changes have been made by Microsoft to ensure DESC compliance? If so, what are the changes?*
7. *A DPIA by the Dutch Ministry of Justice found "there is a high risk for the processing of sensitive and special categories of data… as long as the organisation cannot control its own encryption keys" – at what point did the ICO become aware that Axon holds the encryption keys and not Police Scotland?*
8. *SBC Brian Plastow has said the on-going uncertainty around police cloud deployments would benefit from a formal investigation by the ICO – has the ICO started any processes to initiate a formal investigation?*
   a. *Others separately questioned why, given everything in the public domain about how this cloud infrastructure works, the ICO has not simply conducted an audit to proactively identify, map and mitigate the various risks in police use of MS cloud. Has the ICO ever conducted an audit of any Microsoft infrastructure being used for policing purposes?*
9. *In an exchange with PSoS from April 23, the ICO said "We note that in the DPIA there seems to be two high risks that have not been reduced but have been 'accepted' and we wanted to seek clarity on these. "In our meeting of 19 January 2023 it was our understanding there were no unmitigable high risks outstanding and therefore the processing could go ahead, and the DPIA wouldn't be submitted to us under s65 [of the Data Protection Act] DPA 2018 but rather it would be provided to us informally." Highlighting the two risks, the ICO added "As you will know if you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to formally consult with us under Section 65 DPA 2018. You cannot go ahead with the processing until you have done so."*

a. *In an email from 20 January 2023 (released under a previous round of FOIs) the ICO summarised its meetings with Police Scotland from the previous December, noting that the DESC pilot would begin on 24 January and would involve live personal data; that "there will be no international transfers involved in the provision of technical services"; and that Police Scotland is "assured as the controller" that it is meeting all of the law enforcement data protection obligations.*
b. *However, it also had meetings with SPA prior to this, and was aware of the high risks identified in its DPIA. Despite his, the new FOI disclosure reveals that ICO was asking Police Scotland in April 2023 for clarification on if the risks were right, and why no formal consultation was sought.*
    i. *Did ICO take any steps confirm the assurances from Police Scotland?*
    ii. *Is there any other recorded information the ICO can provide on why it was asking for this clarification on risks nearly 3 months after the deployments, when it had already been made aware of the risks through its on-going engagement with DESC partners?*
    iii. *Can the ICO clarify the exact timeline of when it did become aware of the risks, again given they had been highlighted by other DESC partners?*
    iv. *PSoS itself cites the ongoing and close engagement with ICO as a reason for not referring the DPIA for consultation – can the ICO confirm whether it has conducted a formal consultation with Police Scotland, and if so when this occurred?*

10. *In response to press questions from Computer Weekly, the ICO said it was unable to fully respond because of the pre-election period of sensitivity - can the ICO cite the specific publicity guidance that was used to make this decision?*
    a. *Please can the ICO provide all correspondence related to Computer Weekly's press questions sent on 6 June 2024, in which the questions were directly discussed. I am happy for any personally identifiable information of ICO staff to be redacted.*

We received your request on 24 June.

We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

We do hold information within the scope of your request. I have responded using your numbering below.

1. It was decided that we would issue guidance in the form of a letter to relevant stakeholders on 24 January 2024. The letter was drafted, subject to review and sent out on 28 March 2024.

2. The ICO had undertaken legal analysis of the position as result of its own use of cloud services and this was taken into account when producing the guidance as both issues presented the same legal issues.
   a) This is outlined in our DPIA for Microsoft 365, which has been previously disclosed and is available on our website here.
   b) No, we do not consider that section 73(4) prevents the ICO or other competent authorities from transferring personal data outside of the UK to an IT provider

3. a) We do not hold this information. We have not been advised if these have been completed and have not been provided with copies.
   b) The IDTA and Addendum are capable of providing appropriate safeguards for personal data that meet the requirements of part 3. The documents do not contain specific Part 3 provisions, but these are not required provided that the documents overall provide an appropriate level of data protection.

4. The ICO sought advice from its internal legal department in producing the DESC guidance, we have already made this clear in our response to previous FOI requests.

5. b) i) We are unable to answer this question, as this could have been raised in any discussions that we have had with police forces, including as part of complaint cases, data breach reports or engagement work. We know that the first time this was ever discussed was likely to have been so long ago that we would no longer hold it due to our retention schedules. If we were to search for this information the searches would be far in excess of the 18 hours allowed under the s.12 costs limit, and we would be unlikely to find the answer because anything we do hold is likely to be pre-dated by information no longer held.

6. We hold two emails that are within the scope of this questions, these are attached. Information falling outside of the scope of the request has been redacted.

7. To the best of our knowledge this was first raised in an email to the ICO from the SPA on 26.09.2022. At the time officers were focused on understanding and answering fundamental questions about the use of cloud-based platforms under Part 3. There was an expectation that once there was clarity on what compliance looked like, the ICO would issue clear guidance that would address this and other questions. Consequently a detailed timeline was not created. The email of 26.09.2022 stated the following: "*Whilst it would seem that encryption where neither Axon nor MS can access the keys (although this is apparently not possible as Axon need to decrypt the data) may be the mitigation, in Part 3 encryption is not mentioned as a mitigating measure. It is, however, mentioned a few times in GDPR. It's unclear if this is an oversight in the legislation or if encryption is NOT a mitigation. In which case it's hard to see how this processing would be lawful."*

8. No we have not initiated any investigation of this nature. We have carefully considered whether competent authorities may use cloud-based platforms in compliance with data protection law. Our view is that they may where appropriate protections are in place. We have ensured that DESC partners have been provided with guidance on this and have been asked to implement this. Should we have any concerns that DESC has not been implemented in a compliant way, as you would expect this would be considered and actioned in line with our regulatory action policy.

9) b) i) We did not take further steps to confirm these assurances from Police Scotland, in the circumstances it would not have been proportionate to do so.

ii) We do not have any recorded information that would explain this. We have already disclosed much of our substantive correspondence with the DESC partners, which highlights the complexity of the discussions that were taking place and we have explained that we were seeking legal advice on an ongoing basis during that period.

iii) Most of the substantive correspondence where data sovereignty etc was discussed prior to the date of the ICO advice was disclosed in the previous FOI. The SPA first contacted the ICO to discuss the issue on 12 January 2022 and ongoing discussions followed with additional information and

clarity being provided at various points during the engagement. The ICO then issued interim advice to the DESC partners on 9 December 2022. Following this the ICO was engaged in ongoing discussions with the Scottish Government, SPA and Police Scotland up to the date the ICO issued its final advice in April 2024 and was seeking legal advice on an ongoing basis from its internal legal team during this time. In April 2023 the Scottish Biometrics Commissioner contacted the ICO to advise that it had served an Information Notice on Police Scotland, the discussions between the ICO and the SBC have already been disclosed.

iv) No formal consultation has been initiated or conducted. This will only be necessary if it is determined that the processing entails risks which cannot be mitigated.

10 The relevant guidance is - Pre-election period of sensitivity - House of Commons Library (parliament.uk)

a) I have attached some information which is in scope of this question. One email chain has been withheld, which is discussions between our communications teams and our legal department in which legal advice was sought and received. This is exempt under s.42 FOIA. Explanation is provided below.

Information withheld – section 42

I can confirm that we hold some information which is subject to legal professional privilege and is withheld from our response in accordance with section 42 of the FOIA.

Section 42(1) of the FOIA states:

"Information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality of communications could be maintained in legal proceedings is exempt information."
There are two types of privilege covered by the exemption at section 42. These are:

- Litigation privilege; and
- Advice privilege.

We find that the information in scope of your request is subject to advice privilege. This covers confidential communications between the client and lawyer, made for the purpose of seeking or giving legal advice.

Section 42 is not an absolute exemption, so we must consider whether the public interest favours withholding or disclosing the information.

The factors in favour of lifting the exemption include:

- The public interest in the ICO being open and transparent;
- The public interest in transparency about how the ICO complies with civil service guidance around communications during the pre-election period.

With the public interest factors in favour of maintaining the exemption including:

- The disclosure of legally privileged information threatens the important principle of legal professional privilege;
- Maintaining openness in communications between client and lawyer to ensure full and frank legal advice;
- The disclosure of legal advice could have a chilling effect on both policy officers and legal advisers by dissuading them from discussing such matters in the future in the knowledge that it could potentially be made public;
- These discussions are recent and live given that the ICO is still dealing with requests and press enquiries around DESC and the use of Microsoft Cloud Services;
- It is important that the ICO is able to seek advice about managing its comms during a pre-election period without fear of that advice being disclosed. Disclosure of such advice could threaten

Taking into account the above factors we conclude that the public interest lies in maintaining the exemption.

This concludes our response.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full review procedure on our website.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can raise a complaint through our website.

Your information

Our privacy notice explains what we do with the personal data you provide to us, and sets out your rights. Our Retention and Disposal Policy details how long we keep information.

Yours sincerely

Information Access Team
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email