

Deputy Chief Constable Speirs  
Police Scotland Headquarters  
Tulliallan Castle  
Kincardine  
FK10 4BE

**By email only:** [dccprofessionalism@scotland.police.uk](mailto:dccprofessionalism@scotland.police.uk)

**Cc:** [REDACTED]

2 April 2024

Dear Deputy Chief Constable Speirs

I am writing to you as you have been in touch with the ICO's Scotland office regarding using cloud service providers (as processors) under Part 3 of the Data Protection Act 2018 (**DPA**). In this letter, references to Sections are to Sections of the DPA.

### **ICO view on transfers to processors under Part 3 DPA**

Our view is that law enforcement agencies may use cloud service providers that process personal data outside the UK in accordance with Part 3 DPA, subject to appropriate protections (see below).

### **How to make a transfer to an overseas cloud service provider under Part 3 DPA**

Where you are making a transfer to an overseas cloud service provider (as processor), usually you will need to meet the requirements of Section 75 (Transfers on the basis of appropriate safeguards). There are two main ways you can comply with this:

- First, where UK GDPR adequacy regulations apply, in most cases you will be able to rely on Section 75(1)(b) that you have assessed all the circumstances and decided that appropriate safeguards exist to protect the data; or

- Second, by relying on a Section 75(1)(a) "legal instrument containing appropriate safeguards for protection of personal data" which binds the recipient of the data.

We consider that the IDTA or the Addendum to the EU SCCs (the "Addendum") are capable of meeting this requirement. However, you are responsible for carrying out due diligence to ensure that in the specific circumstances of your transfer, and in particular the often-sensitive nature of Part 3 data, the IDTA or Addendum does provide the right level of protection.

You may find it helpful to look at our transfer risk assessment (TRA) guidance and TRA Tool, which can be adapted for Part 3 transfers. In particular your starting point for Question 2 of the TRA Tool, regarding the level of risk in the data, will be high harm risk for criminal investigations data.

### **Where you are contracting with a UK based cloud service provider**

If you are contracting with a cloud service provider (as a processor) which is a UK company, our view is that you are not making an international transfer. However due to the nature of cloud services, that UK cloud service provider will be making international transfers to its global network of sub processors.

### **Your responsibility for understanding the onward transfers made by your cloud service provider to its sub processors**

Whether or not you are making an international transfer to your cloud service provider (as processor), the nature of cloud services means that it is very likely that there will be further international transfers by the cloud service provider to its sub processors.

Your responsibility (under Section 59) is to ensure that the cloud service provider only engages overseas sub-processors with your authorisation and is giving you sufficient guarantees that it has in place "appropriate technical and organisational measures that are sufficient to secure that the processing will (a) meet the requirements of [Part 3] and (b) ensure the protection of the rights of the data subject."

As part of your due diligence, for those sub-processors which are not in a country with the benefit of a UK GDPR adequacy regulation, you will need to be satisfied that the cloud service provider's contracts with its sub processors contain a Section 75 appropriate safeguard. In the same way that you can make restricted transfers under Part 3, a cloud service provider will be able to rely on the IDTA or Addendum, provided they carry out a TRA.

### **Due diligence when entering into a contract for cloud services**

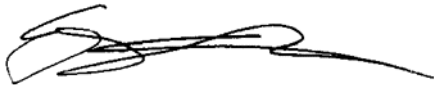
You may find it helpful to consider the following (non-exhaustive) questions with regard to international transfers to or by your cloud service provider:

1. Can you identify with certainty which specific legal entity you are contracting with. You should be able to find this in your contract documentation.
2. If your cloud service provider is not a UK entity and you are not relying on an applicable adequacy regulation, as part of the contractual documentation, is there an IDTA or an Addendum? Have you carried out a TRA which confirms that the IDTA or Addendum will provide the right level of protection for your international transfers?
3. Looking at your contract documentation, check the cloud service provider's list of sub processors and the countries they are located in. Is the cloud service provider obliged to update you if that list changes, so that you have the option to object or exit the contract?
4. How is the cloud service provider ensuring that its international transfers to its sub processors (including sub-sub processors of every level) meet Part 3? Does the cloud service provider give you contractual commitments that it will enter into the IDTA or Addendum with its sub processors, and carry out TRAs where no applicable adequacy regulation applies?
5. Consider what other checks would be proportionate, in particular taking into account the reputation of the cloud service provider and the volume and nature of the personal data which is being sent. For very sensitive information, you may want to carry out your own TRA regarding the restricted transfers made by the cloud service provider.

6. Check if you are required to carry out a DPIA (see Section 64). Even if there is no legal requirement, it is still good practice and can be helpful for you to verify and evidence compliance with Part 3.

We are aware that clarifying amendments to Part 3 DPA have been tabled under the Data Protection and Digital Information Bill, intended to provide greater legal certainty in relation to international data transfers for controllers and processors transferring personal data for law enforcement purposes. We are monitoring the position and intend to publish further guidance once the Data Protection and Digital Information Bill receives Royal Assent. Please do keep an eye on our website and social media for further guidance and communications regarding use of cloud services and international transfers.

Yours sincerely,



Emily Keaney  
Deputy Commissioner - Regulatory Policy  
Information Commissioner's Office