SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

1 Pacific Quay
Glasgow
G51 1DZ

LETTER SENT BY E-MAIL ONLY

6 May 2024

2024/25-006

Freedom of Information (Scotland) Act 2002

Request

Please find below our response to your correspondence dated 9 April, in which you made the following request under the Freedom of Information (Scotland) Act 2002:

"You were recently kind enough to respond to a request (Your Ref: 2023/24-104) in which you were able to make only a partial disclosure on the grounds of encountering a cost barrier.

I am very grateful for the information provided since it highlighted some material which I would like - in a new and more focussed request - to now receive.

Request Element 1:
I would be grateful if the SPA can provide me with a list of any Microsoft Cloud Services identified by them as not operating fully within the UK, or requiring international transfer of customer data during their discussions with the Authority, or as a result of any other direct disclosures in the past year made by Microsoft to the SPA.

In addition, I was recently made aware by the Scottish Government of a letter sent to them from the ICO on or around 2nd April of this year relating to guidance on the use of Cloud Services which may include international transfers under Part 3 of the DPA 2018.
This was after the date of my last FOISA request to you, in which you identified you had received no updated guidance, and I therefore believe it is legitimate to ask this follow up.

Request Element 2:
Because I am aware Scottish Government have received a letter from the ICO on 2nd April, and I believe SPA may also have been sent one as a DESC participant, I would like to receive a copy of any letter received by SPA between the time of my last request (27/02/24) and this current one.

I hope these follow ups will not be unduly burdensome, and do not envisage any need for further follow up once these have been dealt with."

Response

The Scottish Police Authority has considered your request and is able to provide the following.

Request Element 1:
I would be grateful if the SPA can provide me with a list of any Microsoft Cloud Services identified by them as not operating fully within the UK, or requiring international transfer of customer data during their discussions with the Authority, or as a result of any other direct disclosures in the past year made by Microsoft to the SPA.

Microsoft 365 – Microsoft have advised that they cannot guarantee data sovereignty for M365.

Microsoft Azure – Microsoft advised in an email dated 21 November 2023 to the Authority that,

- Microsoft will not store or process customer data outside the customer-specified Geo (e.g. UK) without your authorisation.
- Your authorisation is given by accepting the Microsoft Data Processing Agreement (DPA), which specifies the conditions and purposes for data transfers outside the Geo.
- Microsoft cannot accept specific consent on a case by case basis as this would be impossible to operationalise.
- However, we make an exception for Azure Core Online Services where we commit to store Customer Data at rest within the Geo selected by the customer (Product Terms -> Privacy and Security Terms -> Location of Customer Data at Rest for Core Online Services):

> *Microsoft Azure Core Services. If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services are "non regional" may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations. Refer to the Microsoft Trust Center (which Microsoft may update from time to time,*

but Microsoft will not add exceptions for existing Services in general release) for more details.

- Most Azure services are regional and you can specify the region into which the service will be deployed. Please see here Data Residency in Azure | Microsoft Azure for the list of regional and non-regional services to help with your risk analysis, depending on the services you have.
- For regional Azure Core Online Services, Microsoft will only transfer Customer Data (with customer consent as provided in the DPA) outside of the selected Geo (e.g. UK):
    - For the small number of services specified in the Trust Centre: Data Residency in Azure | Microsoft Azure (i.e. Preview, beta, or other pre-release services and Azure Serial Console for console commands and responses); or
    - If accessed remotely by Microsoft personnel (including subprocessors) located outside the Geo, but this is only with the Customer's authorisation. When authorization is needed, Microsoft personnel would contact the customer using the customer's contact information for the Azure account.
- Given Police Scotland's data transfer concerns, we can provide an additional amendment for Azure Core Online Services to:
    - Commit to store and process Customer Data within your selected Geo (i.e. UK), subject to the exceptions as listed in the Amendment itself (network paths, remote access from personnel with your authorisation, non-regional services). So this expands the Product Terms "Storage at Rest" commitment to store Customer Data at rest to include location of both storage and processing.
    - Confirm in writing that Microsoft personnel (including subprocessors) located outside the Geo may remotely operate data processing systems in the Geo, but will not access Customer Data without authorization by the Customer.
- Microsoft may copy customer data between regions within a given Geo for data redundancy or other operational purposes. For example, geo-redundant storage replicates Blob, File, Queue and Table data between two regions within the same Geo for enhanced data durability in case of a major datacentre disaster. This means that Customer Data could be replicated between London and Cardiff (as regions in the UK Geo) but not outside of the UK. However, please note that to maintain resiliency, Microsoft uses variable network paths that sometimes cross Geo boundaries but replication of Customer Data between regions is always transmitted over encrypted network connections. "

We would also refer you to our previous FOI response 2023/24-104, see email of 7 December at page 15.

Request Element 2:
Because I am aware Scottish Government have received a letter from the ICO on 2nd April, and I believe SPA may also have been sent one as a DESC participant, I would like to receive a copy of

any letter received by SPA between the time of my last request (27/02/24) and this current one.

Please see information held at Appendix 1.

Right to Review

If you are dissatisfied with the outcome of your request you can ask for a review within 40 working days. You must specify the reason for your dissatisfaction and submit your request by email to foi@spa.police.uk or by letter to Scottish Police Authority, 1 Pacific Quay, Glasgow, G51 1DZ.

After review, if you remain dissatisfied, you can appeal to the Scottish Information Commissioner within six months. You can apply online, by email to enquiries@itspublicknowledge.info or by letter to Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS.

Should you wish to appeal against the Commissioner's decision, you can appeal to the Court of Session, only if you think the law has not been applied correctly.

This response will be posted to our Disclosure Log in seven days' time.

Yours faithfully

SPA Corporate Management

Appendix 1

Lindsey Davie
Information Management Lead
Scottish Police Authority

By email only: Lindsey.Davie@[redacted]

2 April 2024

Dear Lindsey

Thank you for coming to us with your concerns around the cloud based Digital Evidence Sharing Capability (DESC) system and its compliance with Part 3 of the Data Protection Act 2018 (DPA 2018).

We have engaged with the SPA and the DESC partners during the course of the pilot development, implementation and the development of the roll out.

During that period, understanding of the data flows involved has developed and we recognise the work that DESC partners have undertaken to document data flows and controller and processor relationships.

Our understanding is that DESC will be rolling out nationally, subject to certain contractual amendments being made. Police Scotland (PS) and the Crown Office and Procurator Fiscal Service will join the rollout first, followed by the Scottish Courts and Tribunal Service and finally the Scottish Police Authority (SPA) will join in due course.

As we have previously advised our view is that, under the DPA 2018, law enforcement agencies may use cloud services that process data outside the UK where appropriate protections are in place. I now provide a letter from ICO Deputy Commissioner, Emily Keaney setting out further detail on the steps that we expect competent authorities to take when using cloud based platforms.

As you will be aware, the controllers involved with the DESC platform are responsible for ensuring that the DESC system is compliant with data protection law prior to its roll out and should therefore consider the attached advice and act on it as appropriate. We have provided feedback to PS on their DPIA that they can share with you as appropriate.

For the avoidance of doubt 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.

The US Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act)

The US Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act) provides two additional pathways by which US public authorities can seek access to personal data for US national security and law enforcement purposes. These supplement the existing Mutual Legal Assistance Treaty (MLAT) process which is well established but can take many months.

The first pathway is for a US public authority to serve a qualifying lawful US order on an organisation which falls within US jurisdiction. Such orders require the organisation to provide information in its possession, custody, or control regardless of where in the world that information is stored. Information processed by a UK company may be accessed via this pathway by an order served directly on the UK company (if US jurisdiction can be established) or indirectly by an order served on the US parent company (if it can be established that the US parent company has the necessary possession, custody, or control of the requested data).

The second pathway is for a US public authority to serve a qualifying lawful US order on a UK communication service provider under the UK-US Data Access Agreement entered into by the UK and US governments. This Agreement incorporates additional safeguards, in particular preventing access to data relating to individuals located in the UK and the use of obtained data in death penalty cases.

We do not consider that organisations (including competent authorities operating under Part 3 Data Protection Act 2018) must stop using cloud services because of concerns over the CLOUD Act and data protection compliance. The CLOUD Act does not alter an organisation's obligations under data protection law. Whichever pathway is used, UK data protection law provides safeguards for individuals and each request must be considered individually on its merits. For both pathways, in practice recipients of requests may find they need to open a dialogue with the US public authority making the request (or with the U.S. Department of Justice's Office of International Affairs for orders made under the UK-US DAA), for example, in order to clarify or verify the legality of the request and ensure their response complies with UK data protection law.

If you require clarity on any of the points on the above or in the accompanying documents we would be happy to discuss further.

Yours sincerely
Jenny Brotchie
Regional Manager Scotland

For information about what we do with personal data see our privacy notice at http://www.ico.org.uk/privacy-notice

Lindsey Davie
Information Management Lead
Scottish Police Authority

By email only: Lindsey.Davie@[redacted]

2 April 2024

Dear Lindsey

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