SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

1 Pacific Quay
Glasgow
G51 1DZ

LETTER SENT BY E-MAIL ONLY

26 March 2024

2023/24-104

Freedom of Information (Scotland) Act 2002

Request

Please find below our response to your correspondence dated 27 February, in which you made the following request under the Freedom of Information (Scotland) Act 2002:

"I would be grateful if you could provide the following information:

In the previously provided/published DPIA's, emails and supporting documentation for the DESC service, you or your partners provided information which indicated that personal data would be processed only within the United Kingdom in Microsoft Data Centres.

In the ICO's email to the DESC partners of 9th December 2022 they identified that use of servives supported from outside of the UK would constitute an international transfer, and that the contract terms may not adhere to S.59(5) of the DPA 2018. The ICO also indicated that they would provide written guidance to the DESC partners.

I am interested to learn what clarifications, confirmations or new information may have been received since December 2022 wrt the above specifically.

I would be grateful therefore if you could provide me with the following information:

1 - A copy of any documents, emails, analysis conducted by yourself or other DESC party, or similar information in your possession which indicates or evidences that Microsoft and Axon shall not process any personal data outside of the UK - including any transfers conducted for support purposes, or as a function of their provided software and services.

OR Conversely;

2 - A copy of any documents, emails, analysis conducted by the ICO or other party, or similar information in your possession which indicates or evidences that Microsoft and Axon may process personal data outside of the UK - or conduct transfers for support purposes or as a function of their provided software and services.

NOTE: Since only one of those conditions can logically apply I am content to receive a response to either Element 1 or 2 - not both of them.

AND

3 - A copy of any guidance or communication received from the ICO wrt the DESC programme as referred to in their letter of 9th December, or other information received from them which indicates or clarifies the legal position of the DESC programme under the Data Protection Act 2018 Part 3 specifically."

On 18 March, the following clarification was provided.

"Firstly thank you for the clarification question, I appreciate the opportunity to tune this request rather than have you embark on an exercise which - as you have I think rightly assumed - is not intended to cover GDPR data.

I apologise for not making this clearer in the body text of my request, instead I relied on the header (specifying DESC) to explain the scope and I should have been much clearer.

I can confirm that for this request to the SPA I am interested only in information relating to the processing of personal data which falls under the Data Protection Act 2018 Part 3 requirements - sometimes referred to as the "LED" requirements, and within the scope of systems and processors relating to DESC operations only.

I do not at this time expect you to consider the processing of other personal data you may handle under the UK GDPR regime on other Microsoft or Axon systems UNLESS disclosures made to you relating to those services can reasonably be considered also apply to, or impact upon, the systems and services supporting or operating DESC.

For example if you received information relating to the underlying Microsoft Cloud platform, its operations, or the applicable terms of service or Data Processing Agreements that apply to, underpin, or support any DESC services or operations, such as identity services, email handling, service desk, or security logging I would consider that to be sufficiently

relevant to fall under this request. Otherwise such information can be reasonably discounted."

Response

Your request for information has been considered and the Scottish Police Authority is able to provide the following.

In relation to your first request, unfortunately, we are unable to provide you with all the information you have requested as it would prove too costly within the context of the fee regulations. The current cost threshold is £600 and we estimate that it would cost in excess of this amount to process your request.[1]

Information held in relation to your request sits over three business areas within the Authority. Key word searches carried out by the business areas for the timeframe specified in your request, since December 2022 to date, returned over 300 records.

Clarification was requested and received on 18 March in an effort to reduce the information in scope. However, it has been determined that there is no easy way to do this and each record would have to be examined in fine detail. Also, due to the nature of your request, specialist knowledge is required to review the information in scope to identify relevant information and sensitive information to be redacted in what is an ongoing commercial matter. Therefore, it has been determined that the fine level analysis required, in this case by a Lead Solicitor, as well as time required to redact at the very least personal information from most records would exceed the cost threshold.

In terms of our duty to assist, we can advise that negotiations are currently underway between Microsoft and Axon for a contract amendment that reflects the data sovereignty, UK GDPR and Part 3 Data Protection Act 2018 requirements. These negotiations are not yet complete. It is anticipated that the final document will be agreed by the end of April 2024.

To further assist, we have provided information interpreted as most relevant to your first request, and subsequent clarification, which was identified and reviewed prior to it becoming clear that the cost threshold would be exceeded. This information is provided at Appendix 1. We would caution that information in emails reflect the position at that date only as negotiations remain ongoing. Information not in scope is redacted as well as third party personal data considered to be exempt in terms of the Act. This exemption is absolute and therefore does not require application of

[1] This represents a refusal notice in terms of Section 12 of the Freedom of Information (Scotland) Act 2002 – Excessive Cost of Compliance.

the public interest test. Whilst you may have a legitimate interest in disclosure of this information, it is our view that those interests are overridden by the interests or fundamental rights and freedoms of the data subjects.

In relation to your second request, we can confirm information is held. A letter issued by the Scottish Biometrics Commissioner to Police Scotland, copied to the Authority, is provided at Appendix 2.

In relation to your third request, the Scottish Police Authority does not hold the information requested.[2] There has been no clarification to the Authority.

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

[2] This represents a notice in terms of Section 17 of the Freedom of Information (Scotland) Act 2002 - Information not held.

Appendix 1

From: [Redacted s38(1)(b)]@ico.org.uk
To: Davie, Lindsey
Cc: [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: Cloud & Part 3 [OFFICIAL]
Date: 18 May 2023 15:38:31

Afternoon Lindsey,

Thank you for providing us with the update below. We are still awaiting our final internal advice and we will update you as soon as we know more.

It would be useful to know when SPA are making any decisions about joining the pilot / roll out, and any associated timescales.

Regards,
[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen

From: Davie, Lindsey
Sent: 17 May 2023 10:31
To: Redacted s38(1)(b)]@ico.org.uk>; [Redacted s38(1)(b)]@ico.org.uk
Subject: Cloud & Part 3 [OFFICIAL]

OFFICIAL
Morning

Not sure if Police Scotland briefed you on this, but we had a meeting with Microsoft on 25th April. I had provided a briefing paper beforehand with the issues.

Their lawyers position was that they consider GDPR to be the gold standard and it was up to the customer to determine whether that was suitable in terms of the data they are processing. There was also a tacit admission that data can go outside the UK. They advised that this is the very nature of Cloud Computing and that their support is on a 'follow the sun model'. They also stated that there were a lot of other public bodies processing Part 3 data on Azure with no issues. Our IT rep at the meeting advised that we consider they are wrong and we are right. Indeed, a number of Police Forces have now made contact with the DESC project given the issues we have uncovered in a product many of them are using for Body Worn Video.

We advised Microsoft that it was our belief that the Forces in England and Wales could not ignore our due diligence, especially given the media coverage and S16 Notice from the Scottish Biometrics Commissioner. We advised that we were trying to resolve the matter for all organisations subject to Part 3.

I raised the possibility of MS providing us with a letter of comfort that stated they were compliant with Part 3 of the DPA 2018 and understood that personal

data relative to the Law Enforcement purpose would be processed on Azure. In Scotland this may be deemed to be a contract/agreement of sorts and may resolve the S59 issue. However their legal rep took the stance again that they were GDPR and it was for us to decide if that was acceptable. They also referred us to their DP Addendum from 2021. This confused us as we had been working from their updated DP Addendum every time they published a new one, most recently at the turn of the year. However, they advised that the relevant DP Addendum would be the one in place the day we signed our contract. I find this rather strange as I would have thought that any changes would apply to all customers – not just new ones. So if their Addendum was changed to reflect a change in law – it's not relevant for any customers that signed before that date?

The MS Policing Account Manager did seem to be keen to try and get a resolution and he was very open to dialogue. He asked me to do another paper, which I am working on, and we agreed to meet again – so at least the door is still open.

Is there any update from your side?

Thanks
Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: [Redacted s38(1)(b)@ico.org.uk
To: Davie, Lindsey
Cc: [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: MS DPA Comments [OFFICIAL]
Date: 14 August 2023 17:01:17

Hi Lindsey,

Thanks for sending this over. Sincere apologies for the delay in coming back to you on this specific point.

For absolute clarity- I am assuming that this addendum relates to the DESC contract? My understanding is that Microsoft is a sub processor of Axon with whom the SG have agreed a contract with? So this is a copy of the addendum issued to Axon in relation to the services that Microsoft will provide for DESC?

Or does this relate to another set of processing ?

I think it is important for us to consider DESC and the questions raised as a whole, so I've circulated this to colleagues who are looking at the legal issues raised regarding DESC and I hope we can come back to you with a comprehensive view. If I have misunderstood however, please do let me know.

In relation to DESC, could you send us the most recent version of the DPIA that you completed?

Best,

[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: [Redacted s38(1)(b)]@ico.org.uk
To: Davie, Lindsey
Cc: [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: Guidance [OFFICIAL]
Date: 03 October 2023 09:40:38

Morning Lindsey,

Following on from yesterday, in addition to the DPIA if you have an indication of timescales for decision making as to whether SPA will join the full roll out that would be useful as well.

To address the point that you make about the risk meeting. As discussed previously the view of my legal colleagues is that under the Data Protection Act 2018, law enforcement agencies may use cloud services that process data outside the UK where appropriate protections are in place. The appropriate protections are key and so as a potential controller it is important that you have completed your own risk assessment and are satisfied that appropriate protections are in place and no remaining unmitigable high risks before any processing begins.

My sincere apologies again for the delay in getting detailed responses to your questions back to you. I have passed these on in internally and whilst unfortunately I do not have a clear timescale for coming back to you please be assured that I will do so as soon as I can. In the meantime I believe you have sought your own legal advice on these points and that would be my recommendation.

Best,
[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: [Redacted s38(1)(b)]@ico.org.uk
Sent: Monday, October 2, 2023 3:19 PM
To: Davie, Lindsey
Cc: [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: Guidance [OFFICIAL]

Thanks Lindsey,

Yes please if you can share your DPIA that would be useful thank you.

Best,

[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: Davie, Lindsey
Sent: Friday, September 22, 2023 8:54 AM
To: [Redacted s38(1)(b)]@ico.org.uk>

Cc: [Redacted s38(1)(b)]@ico.org.uk>
Subject: RE: Guidance [OFFICIAL]
OFFICIAL

[Redacted s38(1)(b)]

Thanks. At this point in time I don't believe my SIRO or CEO would be minded to join. [redacted]

Happy to share my DPIA if you want to see the current version.

Regards
Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: [Redacted s38(1)(b)]@ico.org.uk]
Sent: 22 September 2023 08:26
To: Davie, Lindsey; [Redacted s38(1)(b)]@ico.org.uk>
Subject: RE: Guidance [OFFICIAL]

Hi Lindsey,

I'm afraid not as you will have seen! We have however been chasing this up internally and will revert as soon as we have something/ an updated timeframe. For clarity I am hoping to pass on some additional advice primarily on S59 and S75 safeguards.

It sounds like SPA may still be considering joining DESC ? Do you have an updated DPIA?

Best,
[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: Davie, Lindsey
Sent: Thursday, September 21, 2023 12:19 PM
To: [Redacted s38(1)(b)]@ico.org.uk>;[Redacted s38(1)(b)]@ico.org.uk>
Subject: Guidance [OFFICIAL]
Importance: High
OFFICIAL

Afternoon

In a big DESC risk meeting and everyone is asking if the ICO advice is coming today……no pressure

Regards

Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: [Redacted s38(1)(b)]@ico.org.uk
To: Davie, Lindsey; [Redacted s38(1)(b)]
Subject: RE: Microsoft Update [OFFICIAL]
Date: 14 December 2023 09:10:02

Morning Lindsey,

That sounds like positive progress on the addendum. When they say international transfers have they given you any more detail/ I'm sure you will be asking these questions anyway but you will want to ascertain what these international transfers would be. What data to which third country/ countries ? Once you have that information you can better assess the risks, what safeguards and mitigations might feasibly be put in place and whether compliance with the relevant sections of Part 3 is possible.

I'm currently in the process of pulling together some advice on some of the risks that we have discussed previously (potential access to DESC data by US law enforcement authorities without the knowledge or consent of DESC partners etc) and I am hoping to circulate this shortly.

Also happy to have a discussion if that would be helpful.

Best,
[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: Davie, Lindsey
Sent: Thursday, December 14, 2023 8:13 AM
To: [Redacted s38(1)(b)]@ico.org.uk; [Redacted s38(1)(b)]@ico.org.uk
Subject: Microsoft Update [OFFICIAL]

OFFICIAL

Morning

Quick update; We are making progress with MS now. They have agreed that their DPAdd does not include UK GDPR and Part 3 requirements, so will add these to it.

However, the real sticking point we now have is that they say they would not make international transfers without our consent…..but by signing to agree to the DPAdd they take that as consent. We have expressed our position that this is not compliant with S59, S73 or S77.

Regards

Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: Davie, Lindsey
To: [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: MS Update [OFFICIAL]
Date: 23 January 2024 10:47:00

OFFICIAL

[Redacted s38(1)(b)]

Once we get the final written document from Microsoft this will be put in front of SIRO's. If everything that they have agreed to is in this document then I expect we will move forward, but as yet we don't actually know what FS will add to DESC. I guess that scoping will begin once we get the green light.

Regards

Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: [Redacted s38(1)(b)]@ico.org.uk
Sent: 22 January 2024 08:52
To: Davie, Lindsey; [Redacted s38(1)(b)]@ico.org.uk
Subject: RE: MS Update [OFFICIAL]

Hi Lindsey,

Hope you are well ? Thank you for keeping us updated on everything, that does sound very positive in terms of the Microsoft contract. Can you let us know where you are in terms of timescales for adoption (if SPA do decide to join the rollout – from your email below it sounds like this may be more likely now?).

Best,

[Redacted s38(1)(b)]
[Redacted s38(1)(b)]
Information Commissioner's Office, Queen Elizabeth House,

From: Davie, Lindsey
Sent: Tuesday, January 16, 2024 8:48 AM
To: [Redacted s38(1)(b)]@ico.org.uk; [Redacted s38(1)(b)]@ico.org.uk
Subject: MS Update [OFFICIAL]

OFFICIAL
Morning

Hope this finds you both well. Just a quick update for MS progress.

MS have agreed, thus far, to make all the changes we have asked for in their DPAdd for Microsoft Azure. However, they have said they will do this for SPA/PSoS and Axon. I muted the point that it should be in the DPAdd for all customers, but they responded that no-one else had asked them. Obviously I

need to try and persuade them to change it for all users as we want to be able to do business with 3rd parties using Azure without having to ask them to approach ICO and ask for their terms to be changed.

So…good news for the DESC project. Our lawyers are just going to circle back this week and make sure this resolves all out concerns or whether we should buy the advanced data residency offering as well.

[redacted]

[redacted]

So bit of a mixed bag, but I kind of feel vindicated for raising the issues – getting MS to agree tochange some things for us is, in my view, a huge win and opens the door for closer working in the future.

Regards
Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: [Redacted s38(1)(b)]@axon.com
To: Davie, Lindsey
Subject: RE: Microsoft Azure [OFFICIAL]
Date: 30 January 2024 16:04:40

Just realised I did not respond to your email – apologies, and thank you for sharing.

From: Davie, Lindsey
Sent: Friday, January 19, 2024 10:18 AM
To: Redacted s38(1)(b)]@axon.com
Subject: FW: Microsoft Azure [OFFICIAL]
Importance: High
OFFICIAL

[Redacted s38(1)(b)]

Hope you are well.

[redacted]

[redacted]

[redacted]

[redacted]

See email below…having re-read I am not sure that our IT checked with you…can you just confirm that the DESC solution does not use any of the functions where they can't guarantee data sovereignty, or that no part 3 data would be in those elements.

We are hoping that MS will have a draft agreement to us in the next week and that's where the lawyers for each organisation will be able to review – it will be the first formal document from them. I didn't see any point in sending every email that we discussed small areas (some of them
NOT game changers but nice to have) until we actually got something in writing for MS to review.

[redacted]

[redacted]

[redacted]

Regards

Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

From: Perry, Chris
Sent: 07 December 2023 13:33
To: Davie, Lindsey
Subject: RE: Microsoft Response 365 [OFFICIAL]
OFFICIAL

Hi Lindsey,

The services that Microsoft detail that may store and process data outside of the specified Geo are:

Azure Cloud Services, which backs up web and worker-role software deployment packages to the United States regardless of the deployment region.

Azure Data Explorer (ADX) stores partial usage data and service traces on a central cluster located in the EU for a limited time.

Language Understanding, which may store active learning data in the United States, Europe, or Australia based on the authoring regions which the customer uses.

Azure Machine Learning, may store freeform texts of asset names that the customer provides (such as names for workspaces, names for resource groups, names for experiments, names of files, and names of images) and experiment execution parameters aka experiment metadata in the United States for debugging purposes.

Azure Databricks stores the following identity information in the United States to provide account and access management functionality to customers: username, first name, surname, and email address. This data is stored in the United States to support the global Azure Databricks platform.

Azure Serial Console, which stores all customer data at rest in the Geo selected by customer, but when used through the Azure Portal may process console

commands and responses outside of the Geo for the sole purpose of providing the Console experience inside the Portal.

Preview, beta, or other prerelease services, which typically store customer data in the United States but may store it globally.

I've completed a review of these services alongside [Redacted s38(1)(b)] and none of them will process personal or law enforcement data in any of our proposed uses of M365 and Azure including DESC.

Language Understanding, Azure Machine Learning, Azure Data Bricks and all preview, beta and prerelease services will need to be captured as not available for use as part of any future developments but that will be assured as part of the Cyber Security Assessment and accreditation of new services before they are made live. Essentially any new service we buy or build platformed in Azure will be checked to ensure that those services aren't in use.

Chris Perry
Chief Technology Officer
Digital Division
Police Scotland / Poileas Alba

From: Davie, Lindsey
Sent: Thursday, December 7, 2023 11:11 AM
To: Perry, Chris
Subject: Microsoft Response 365 [OFFICIAL]
OFFICIAL

Chris

I was hoping to do the response to MS today or tomorrow in keeping with tight timelines and my diary. Were we able to get a view from IT in respect of the technical elements that MS mentioned in their last response to us?

Thanks

Lindsey Davie
Information Management Lead
Scottish Police Authority/ Ùghdarras Poilis na h-Alba

Extracts from signed Services Contract reference 388514 between The Scottish Ministers acting through the Scottish Government (the "Purchaser") and Axon Public Safety UK Ltd (the "Service Provider") relating to the supply of the Digital Evidence Sharing Capability .

13. DATA PROTECTION

13.1 The Service Provider acknowledges that Personal Data described in the scope of Schedule 10 (Data Protection) will be Processed in connection with the Services under this Contract.

13.2 For the purposes of any such Processing, the Parties agree that the Service Provider acts as the Processor and the Purchaser acts as the Controller in respect of the Purchaser Data, each Partner acts as the Controller in respect of its own Partner Data and each Stakeholder acts as the Controller in respect of its own Stakeholder Data. Although the Parties acknowledge that the Partners and the Stakeholders may act as independent controllers when using shared infrastructure pursuant to this Contract, the Parties further acknowledge that there may be circumstances where one or more Partners and/or one or more of the Stakeholders may be joint controllers in jointly determining the purposes and means of processing Personal Data.

13.3 Both Parties agree to negotiate in good faith any such amendments to this Contract that may be required to ensure that both Parties and each Partner and Stakeholder meet all their obligations under the Data Protection Laws. The provisions of this clause 13 are without prejudice to any obligations and duties imposed directly on the Service Provider under the Data Protection Laws and the Service Provider hereby agrees to comply with those obligations and duties.

13.4 The Service Provider will, in conjunction with the Purchaser and each other Controller and in its own right and in respect of the Services, make all necessary preparations to ensure it will be compliant with the Data Protection Laws.

13.5 The Service Provider will provide the Purchaser and each other Controller with the contact details of its data protection officer or other designated individual with responsibility for data protection and privacy to act as the point of contact for the purpose of observing its obligations under the Data Protection Laws.

13.6 The Service Provider must:

13.6.1 agree and comply with the terms of the data processing provisions set out in Schedule

10 (Data Protection);

13.6.2 process Personal Data only as necessary in accordance with obligations under this Contract and any written instructions given by the Purchaser and the Partners (which may be specific or of a general nature), including with regard to transfers of Personal Data outside the United Kingdom or the European Economic Area unless required to do so by United Kingdom, European Union or Member state law or regulatory body to which the Service Provider is subject; in which case the Service Provider must, unless prohibited by that law or regulatory body, inform the Purchaser of that legal requirement before processing the Personal Data only to the extent, and in such manner as is necessary for the performance of the Service Provider's obligations under this Contract or as is required by the Law;

13.6.3 subject to clause 13.6.2 only process or otherwise transfer any Personal Data in or to any country outside the United Kingdom or the European Economic Area with the Purchaser's prior written consent;

13.6.4 take all reasonable steps to ensure the reliability and integrity of any Service Provider Representatives who have access to the Personal Data and ensure that the Service Provider Representatives:

(a) are aware of and comply with the Service Provider's duties under this clause;

(b) are subject to appropriate confidentiality undertakings with the Service Provider or the relevant Sub-contractor;

(c) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Purchaser or as otherwise permitted by this Contract; and

(d) have undergone adequate training in the use, care, protection and handling of Personal Data (and the Service Provider shall keep, for the Term and for any Termination Assistance Period, accurate records of such training and details of the content of all training courses, which shall be made available to the Purchaser immediately upon request).

13.6.5 implement appropriate technical and organisational measures including those set out in Schedule 10 (Data Protection) and in accordance with the Data Protection Laws to

protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected.

13.7 The Service Provider shall not engage a Sub-contractor to carry out Processing in connection with the Services without prior specific or general written authorisation from the Purchaser. In the case of general written authorisation, the Service Provider must inform the Purchaser of any intended changes concerning the addition or replacement of any other Sub-contractor and give the Purchaser an opportunity to object to such changes.

13.8 If the Service Provider engages a Sub-contractor for carrying out Processing activities on behalf of the Purchaser and the other Controllers, the Service Provider must ensure that the same data protection obligations as set out in this Contract are imposed on the Sub-contractor by way of a written and legally binding contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures. The Service Provider shall remain fully liable to the Purchaser and the other Controllers for the performance of the sub-contractor's performance of the obligations.

13.9 The Service Provider must provide to the Purchaser and the other Controllers reasonable assistance including by such technical and organisational measures as may be appropriate in complying with the Data Protection Laws.

13.10 The Service Provider must notify the Purchaser if it:

13.10.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

13.10.2 receives a request to rectify, block or erase any Personal Data;

13.10.3 receives any other request, complaint or communication relating to the obligations of the Service Provider or the Purchaser or any other Controller under the Data Protection Laws;

13.10.4 receives any communication from the Supervisory Authority or any other regulatory authority in connection with Personal Data processed under this Contract; or

13.10.5 receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by law;

and such notification must take place as soon as is possible but in any event within three (3) Working Days of receipt of the request or any other period as agreed in writing with the Purchaser from time to time.

13.11 Taking into account the nature of the Processing and the information available, the Service Provider must assist the Purchaser and each Controller in complying with the Purchaser's and each Controller's obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations in accordance with the Data Protection Laws. These obligations include:

13.11.1 ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the Law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events;

13.11.2 notifying a Personal Data breach to the Purchaser and the relevant Controller without undue delay and in any event no later than twenty four (24) hours after becoming aware of a Personal Data breach;

13.11.3 assisting the Controller with communication of a personal data breach to a Data Subject;

13.11.4 supporting the Controller with preparation of a data protection impact assessment; and

13.11.5 supporting the Controller with regard to prior consultation of the Supervisory Authority.

13.12 At the end of the provision of Services relating to Processing the Service Provider must, on written instruction of the Purchaser, delete or return to the Purchaser (or to one or more Controllers specified by the Purchaser) all Personal Data and delete existing copies unless UK law requires storage of the Personal Data.

13.13 The Service Provider must maintain written records including in electronic form, of all Processing activities carried out in performance of the Services or otherwise on behalf of the Purchaser and each other Controller containing the information set out in the Data Protection Laws.

13.14 The Service Provider must:

13.14.1 provide such information as is necessary to enable the Purchaser and each other Controller to satisfy itself of the Service Provider's compliance with this clause 13;

13.14.2 allow the Purchaser and each other Controller, and its and their employees, auditors,

authorised agents or advisers reasonable access to any relevant premises, during

normal business hours, to inspect the procedures, measures and records referred to in this clause 13 and contribute as is reasonable to those audits and inspections; and

13.14.3 inform the Purchaser and any instructing Controller if in its opinion an instruction from the Purchaser or instructing Controller infringes any obligation under Data Protection Laws.

13.15 If requested, the Service Provider must make such records referred to in clause 13.11 available to the Supervisory Authority on request and co-operate with the Supervisory Authority in the performance of its tasks.

13.16 The Parties acknowledge that the inspecting party will use reasonable endeavours to carry out any audit or inspection under clause 13.12.2 with minimum disruption to the Service Provider's day to day business.

Excerpt of definitions contained in Schedule 1 of the Services Contract reference 388514 between the Scottish Ministers acting through the Scottish Government (the "Purchaser") and Axon Public Safety UK Ltd (the "Service Provider") relating to the supply of Digital Evidence Sharing Capability.

"Data Controller" (or "Controller") has the meaning given in the Data Protection Laws.

"Data Processor" (or "Processor") has the meaning given in the Data Protection Laws.

"Data Protection Laws" means any law, statute, subordinate legislation regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body which relates to the protection of individuals with regard to the processing of Personal Data for so long as and to the extent to which a Party is subject including the Data Protection Act 2018, PECR, or any statutory amendment or re-enactment thereof and the UK GDPR.

Schedule 2 Part 1 of the Services Contract between the Scottish Ministers acting through Scottish Government (the "Purchaser") and Axon Public Services UK Ltd (the "Service Provider"), is the Purchaser's Statement of Requirements. Section 8 Non-functional Requirements a 8.4 Security states:
SEC-24 Personal Information
The data protection requirements are set out at Clause 13 and Schedule 10 of the Services Contract. Where Personal Data is involved, the Service Provider MUST contractually enforce all of these security conditions onto any third[1]party service providers, sub-contractors or partners who could potentially access the Purchaser Data, Partner Data or Stakeholder Data in the course of providing the service.

The required security conditions should be either ISO/IEC 27001 (Information Security Management Systems Requirements) or equivalent or HMG Cyber Essentials Plus certification or equivalent. The Service Provider must indicate the arrangements under the Data Protection Act/GDPR and ISO27018 https://www.gov.uk/government/publications/cyber[1]essentials-scheme-overview

Appendix 2

Andrew Hendry
Chief Digital Information Officer
Police Scotland
Digital Evidence Sharing Capability PS SRO
14 December 2023

cc Assistant Chief Constable Bex Smith
cc Martyn Evans, Chair of Scottish Police Authority

Dear Andrew,

Digital Evidence Sharing Capability (DESC)

On 22 April 2023, I served an Information Notice on Police Scotland under section 16 (2) of the Scottish Biometrics Commissioner Act 2020. My purpose in doing so was to ascertain whether Police Scotland are complying with the data protection elements of my statutory Code of Practice which took legal effect in Scotland after being approved by the Parliament and Scottish Ministers on 16 November 2022.

At this juncture, I also sought advice from the UK Information Commissioner (ICO) on whether the use of hyperscale cloud infrastructure provided by U.S. companies which involves biometric or genetic data is compliant with law enforcement-specific data protection rules, and specifically section 73 relating to international transfers, having regard to the potential implications of the U.S. Clarifying Lawful Overseas Use of Data Act 2018 (Cloud Act).

Police Scotland subsequently responded to the Information Notice providing the requested information. On 5 October 2023, I again wrote to Police Scotland. The purpose of that letter was threefold. Firstly, it set out my concerns about the potential risks that arise from sensitive biometric data being ingested by Police Scotland to the current Scottish Government DESC pilot in Dundee. Secondly, by setting out those concerns in writing, I hoped to assist DESC partners with post-pilot evaluation. Thirdly, setting out my juristic concerns on this matter publicly was prudent in terms of facilitating full and frank discussion between us prior to Police Scotland completing its self-assessment return relative to compliance with the statutory Code of Practice in Scotland.

As you know, assessing compliance with UK Data Protection Law is solely and properly a matter for the UK Information Commissioner (ICO). On 11 December I had an in-person meeting with the UK Information Commissioner John Edwards at Queen Elizabeth House in Edinburgh. From our discussions, the UK ICO is unlikely to opine that the uploading of biometric data to DESC by Police Scotland conflicts with UK data protection law. This is because Article 3 of the agreement between the U.S. and UK Government's on access to electronic data under the U.S. Cloud Act requires each party to the agreement to ensure that its domestic laws do not frustrate or impair the operation of the agreement.

Having regard to that determination by UKG and the ICO, and to the spirit of reciprocity in international and UK cooperation, it is also therefore my determination that the uploading of biometric data to DESC by Police Scotland is consistent with Principle 10 of the Scottish Code of Practice which requires biometric data to be protected from unauthorised access and unauthorised disclosure in accordance with UK GDPR and the UK Data Protection Act 2018.

I am also grateful for the opportunity to attend the workshop on DESC on 15 December 2023, as this will afford us the opportunity for further discussion prior to the completion of my compliance assessment on the Code of Practice over the winter.

Yours sincerely,

Brian Plastow

Dr Brian Plastow
Scottish Biometrics Commissioner