SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

1 Pacific Quay
Glasgow
G51 1DZ

LETTER SENT BY E-MAIL ONLY

6 March 2023

2023-015

Freedom of Information (Scotland) Act 2002

Request

Please find below our response to your correspondence dated 6 February, in which you made the following request under the Freedom of Information (Scotland) Act 2002:

It is now well over a year since it was announced in the press that the Scottish Government would bring in a new digital Evidence platform (DESC) based on Axon Technology, which sits on the Microsoft Azure Public cloud.

I would be grateful if you would provide me with the following information relating to this project and its current status from your orgnsiations perspective as a listed participant:

1 - A copy of the Data Protection Impact Assessment(s) conducted on the AXON 'Evidence.com' and digital evidence management cloud services under the terms of s64 of the Data Protection Act 2018, to include any and all of the following families of Axon services in use or planned for deployment for DESC.

Please note:
A DPIA should not in general contain any specific information of security measures requiring redaction before release, but I am aware that some Policing and Justice organisations do include this information in their DPIAs.

Reasonable redaction of such information strictly to the extent necessary to maintain the security of Police or Justice operations (if this is included in the DPIA) is acceptable.

General redaction of core information relating to relevant DPIA content required to evidence achievement against statutory obligations would however be unacceptable and should be unnecessary since its release is obviously and materially in the public interest and confirmation that public and citizen interests will be suitably protected under the law is the core function of a DPIA.

2 - A copy of the specific terms of service applied within the contract between Axon and the Authority relating to Data Protection Act Part 3; or confirmation that their standard Terms of Service have been applied without modification.

3 - Details of any sub-processor engaged by Axon as part of their DESC service delivery and the countries in which data shall or may be processed.

If element 4a below is not in place please apply element 4b - one of them should be applicable, but both cannot be:

4a - Copies of any specific diligence material, contractual terms or other undertakings from Axon and their sub-processors that they will not transfer any personal data processed for a Law Enforcement purpose by the Authority outside of the UK without the Authorities prior written and specific approval in each instance, as required under S59(7) go the Act;

OR -

4b - Copies of the guidance issued by the Authority to any officers and staff relating to the steps and procedures required by the Authority (under DPA 2018 s.77) before the upload of personal data processed for a Law Enforcement purpose to any Axon cloud services where an undertaking not to transfer the data outside of UK has not been given in contract.

5 - Copies of the communications between the authority and the ICO, and/or other professional or advisors, which informed the creation of the DPIA and/or supported decisions around the procurement or use of the Axon evidence.com related products for the processing of personal data for a Law Enforcement purpose by the Authority.

Response

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

1. The Data Protection Impact Assessment is provided as **Appendix 1**.

2. There is no contract in place between Axon and the Scottish Police Authority. Therefore, this represents a notice in terms of Section 17 of the Freedom of Information (Scotland) Act 2002 - Information not held.

   In terms of our duty to assist, I can advise that the Scottish Government contracted with Axon Public Safety UK Ltd to deliver the new Digital Evidence Sharing Capability service (DESC). This information may, therefore, be available by contacting the Scottish Government at Request information - gov.scot (www.gov.scot)

   In addition, the contract details were provided on the Scottish public contracts register at the following link: https://www.publiccontractsscotland.gov.uk/Contracts/Contracts_View.aspx?id=670801

3. A table of sub-processors and country of origin is provided as **Appendix 2**.

4A. As stated at 2 above, there is no contract between Axon and the Scottish Police Authority. DESC was procured by the Scottish Government. Therefore, this represents a notice in terms of Section 17 of the Freedom of Information (Scotland) Act 2002 - Information not held.

4B. No guidance has been issued to staff as no personal data is being uploaded by the Authority. Therefore, this represents a notice in terms of Section 17 of the Freedom of Information (Scotland) Act 2002 - Information not held.

5. The relevant communications between the Authority and the Information Commissioner are attached as **Appendix 3**. Some of this information is considered to be exempt under Section 38(1)(b) Personal data of a third party. Disclosure would contravene the data protection principles in Article 5(1) of the General Data Protection Regulation and section 34(1) of the Data Protection Act 2018. This exemption is absolute and therefore does not require the application of the public interest test.

Advice provided by Kings Counsel is held and is considered exempt under S36(1) 'Confidentiality of Communications'. This exemption applies because the information refers to legal advice and disclosure would breach legal professional privilege. Legal advice privilege covers communications in which legal advice is sought or given and where a legal adviser is acting in their professional capacity.

This exemption is non-absolute and requires the application of the public interest test. Therefore, consideration has been given as to whether the public interest favours disclosing the information or maintaining the exemption.

Public Interest Test

The public interest factors in favour of disclosure is that:

- It could contribute to transparency and allow scrutiny of advice provided.

The public interest factors in favour of maintaining the exemption being:

- The general public interest inherent in this exemption is strong due to the importance of the principle behind legal professional privilege. Disclosing legally privileged information threatens that principle;

- It is vital to maintain and safeguard legal professional privilege, ensuring the confidentiality of communications between legal advisers and their clients, in order to ensure access to full and frank legal advice;

On balance, our conclusion is that maintaining the exemption outweighs the public interest in disclosure.

Right to Review

If you are dissatisfied with the way in which your request has been dealt with you are entitled, in the first instance, to request a review of our actions and decisions

Your request must specify the matter which gives rise to your dissatisfaction and it must be submitted within 40 working days of receiving this response - either by email to foi@spa.police.uk or by post to Corporate Management Team, Scottish Police Authority, 1 Pacific Quay, Glasgow, G51 1DZ.

If you remain dissatisfied following the outcome of that review, you are thereafter entitled to apply to the Office of the Scottish Information Commissioner within six months for a decision.

You can apply online, by email to enquiries@itspublicknowledge.info or by post to Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS.

Should you wish to appeal against the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

As part of our commitment to demonstrate openness and transparency in respect of the information we hold, an anonymised version of this response will be posted to the Scottish Police Authority Freedom of Information Disclosure Log in seven days' time.

SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Data Protection Impact Assessment – Digital Evidence Sharing (DESC)

Step 1: Identify the need for a DPIA

Please ensure you read the SPA DPIA SOP prior to completing this document. Appendix A (attached) contains information on when to conduct a DPIA. If you are in ant doubt you MUST contact SPA Information Management

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Digital Evidence Sharing Capability (DESC) project is funded by the Scottish Government (SG) for Criminal Justice partners including the Police Service of Scotland (PSoS), Scottish Police Authority (SPA), Crown Office and Procurator Fiscal Service (COPFS), Scottish Courts and Tribunals Service (SCTS) and the Defence community as vital stakeholders.

The Scottish Governments Justice and Strategy unit have led on the procurement of the IT solution (AXON Public Safety UK) with PSoS, SPA, COPFS and SCTS actively collaborating through individual internal governance routes. PSoS is the lead delivery partner. All Criminal Justice partners will collaborate to develop the IT solution with Axon in order to meet the needs of the Criminal Justice partners to process digital evidence through the justice process.

DESC aims to create a digitally enabled workforce to deliver an end to end service for the collection, management and sharing of digital evidence from crime scene to court, for all Criminal Justice partners.

The intended outcomes of DESC include improved justice for victims and witnesses through more effective investigation and preparation of digital evidence, improved disclosure processes promoting early case resolution, streamlining the process of capturing, storing and sharing digital evidence and managing significant increases in demand and volume as more information is created and made available digitally.

DESC will provide the capability to collect and securely share digital evidence between Criminal Justice partners. It will provide a reliable and secure repository for evidential content and meet the service requirements of each of the Criminal Justice partners. This includes collecting and certifying evidence in line with legislative requirements, reviewing evidence, sharing evidence and the retention and disposal of content.

Digital evidence will include public and private space CCTV, body worn video, evidential calls to police control room, police interviews, photographs/videos of; victims, accused, crime scenes, documents and fingerprints. It will also process digital evidence from computers/mobile devices and digital evidence from devices such as dash cams and video doorbells submitted by the public.

Evidence will be collected from both internal and external sources, ingested to DESC via internet link and via workstations on the Police Scotland Network. The ingested data will be certified as a true copy of the original. Subsequent edits and versions will be certified as a copy.

DESC users can view evidence including relevant metadata and certificates from a range of devices. Evidence can be downloaded/transferred from DESC to other systems if required. DESC users can edit/clip files, obtain still images, redact, compile files into one

and create bookmarks whilst ensuring the integrity of the original file. Users can restrict files and folders, securely share files and folders (cases) with approved users (individuals, groups and organisations) and, in addition, they can securely share with external users and third parties (e.g. Defence Agents).

DESC data can be removed when authorised for removal, such as release following disposal of case, data created in error, data assessed as non-evidential. Users can restore data in line with solution (Axon Evidence) storage rules. DESC audit logs can be produced in respect of users, organisations and evidence history including edits and sharing. Users can restrict files and folders (cases) relating to sensitive investigations and OFFICIAL SENSITIVE data can be shared with authorised users across the DESC partnership and if required external users. Evidence ingested to DESC can subsequently be presented in Court in a playable format supportive of trial environments.

Axon Evidence will store reference numbers, notes, metadata and allow users to set record retention periods against ingested evidence. The relevant DESC administrators / users can control user access and restrict files/folders.

Axon will be a Data Processor and there will be instances where SPA will be a Data Processor on behalf of COPFS. A Data Processing Agreement (DPA) is to be set up between SPA / PSoS/COPFS and Axon.

SPA will be a Joint Data Controller on implementation of DESC with COPFS, PSoS and SCTS. A Joint Controller Agreement (JCA) for the data will be in place prior to sharing of live, identifiable, data between SPA and the partner organisations.

Governance of the DESC Programme is set out in a MOU. The DESC MOU describes the shared vision and commitment relating to the collaborative project between Scottish Government, Crown Office and Procurator Fiscal Service, the Police Service of Scotland, the Scottish Police Authority and Scottish Courts and Tribunals Service (DESC partners) to deliver a digital evidence sharing capability (DESC) across the Criminal Justice sector in Scotland.

A DPIA is required given the scale of the project. This is the first time that data of this nature and volume will have been shared via a 3rd party private entity using a Cloud solution. As such additional risks that do not exists in the current process require to be mitigated.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

The data to be processed is Law Enforcement data and as such falls under the controls in Part 3 of the Data Protection Act 2018.

There is no new data being collected or shared, the project seeks to automate an existing manual process that has significant issues and risks including the routine loss of data.

The data will be shared between the parties to the project as required by law.

SPA is required by law to provide Forensic Services to both PSOS and COPFS. Those services include images of victims and accused, videos and images of crime scenes including fingerprint images and images of deceased persons. Video reconstructions of serious crime scenes and RTA's are also shared.

The data relating to living individuals will fall under Part 3 of the Data Protection Act 2018.

Images of deceased and crime scenes will fall under the common law duty of confidentiality.

In the current manual process SPA is regularly asked to provide copy evidence as the original evidence has been 'misplaced' by the received authority. The DESC programme seeks to eliminate this issue.

It should be noted that SPA is NOT a Schedule 7 body. SPA is a Competent Authority by virtue of its founding legislation.

The processing is deemed 'High Risk' as a previously untested method is being utilised. This involves outsourcing the management of the evidence sharing to a private entity, Axon UK, via their product 'Evidence.com'.

The product uses Microsoft Azure to store data. It is believed that there may be risks in terms of S73 of the Data Protection Act in respect of this solution – specifically the transfer of Part 3 data by either Axon of Microsoft outside of the UK. In particular, access by Microsoft or Axon staff who are outside the UK to data assets that are in the UK.

The contract that Axon have with MS states that data will only be processed in the 2 PASF assured data centres in the UK. However, Microsoft fall short of stating that Azure is Part 3 compliant. All literature states they are GDPR compliant. MS make a specific statement in their GDPR Addendum;

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for

compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers.

Microsoft also made the below statement indicating that its current offerings may not yet be compliant;

We already provide commercial and public sector customers the choice to have data stored in the EU, and many Azure cloud services can already be configured to process data in the EU as well," wrote Smith. "We have already begun engineering work so our core cloud services will both store and process in the EU all personal data of our EU commercial and public sector customers, if they so choose. This plan includes any personal data in diagnostic data and service-generated data, and personal data we use to provide technical support." In a blog post announcing the plan, Microsoft president and chief legal officer Brad Smith said the EU Data Boundary pledge would apply to data processed by its main cloud services – including Azure, Microsoft 365 and Dynamics 365 – and the engineering work needed to deliver the project would be completed by the end of 2022.

Describe the scope of the processing: what is the nature of the data and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data is primarily Law Enforcement Data and will include images of accused, victims and crime scenes from SPA. Special Category data will be processed including genetic, biometric, health and race.

In addition user data and project staff personal data will be processed. This data will be subject to UK GDPR where it is not recorded as part of an investigation.

Data will be processed in volume, daily. All data has a pre-defined weeding and retention period and those rules will be applied to the application. A large number of accused/witnesses in more serious crimes will see their data processed via this medium. All members of the public submitting video evidence will have it processed via this medium.

The processing will cover anyone reporting a crime or who is a victim of crime in Scotland where relevant evidence is being processed.

The wider database will include public and private space CCTV, body worn video, evidential calls to police control room, police interviews, photographs/videos of; victims, accused, crime scenes, documents and fingerprints. It will also process digital evidence from computers/mobile devices and digital evidence from devices such as dash cams and video doorbells submitted by the public.

Full testing will be undertaken to make sure that all rules for weeding/deletion operate according to requirements.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

SPA does not always have direct interaction with data subjects, however, at some point in the process the data subjects will have direct interaction with one of the partners. SPA does maintain a privacy notice on our website and where we have direct interaction with data subjects and collect data we have a business type card that can be provided to data subjects that defines the purpose, retention period and contact details.

The data is already used for this purpose, the law enforcement purpose. There is an expectation from the public that policing will stay in touch with the people it serves. This includes moving to digital platforms such as DESC that allow members of the public to share dash-cam, CCTV and doorbell footage easily without the abstraction of a police officer attending and seizing a device for upload.

It is unlikely that the public have a view on compliance with S73 of the DPA when their ultimate desire is to see justice done and ease of access. However, there have been a number of journalistic articles recently highlighting that the use of Hyperscale Cloud, such as Microsoft and Amazon, does not comply with the requirements of Part 3 of the Data Protection Act 2018 and as such could lead to class actions by data subjects in the future.

Vulnerable groups and children will be amongst the data subjects, however, this is not new processing – it's just the method by which it is being achieved that is new.

The processing is not 'novel' in policing in the UK, however, it is new for policing in Scotland. There are concerns that the processing may breach the tight controls that apply to International Transfers as defined in S73 of the DPA. Those concerns relate to the provider, a wholly owned US company and its sub-processor, Microsoft Azure. There are further concerns in terms of the Cloud Act and FISA.

These concerns exist given that any major crime may see a significant volume of information processed via DESC. The crime may have been committed by a national of any country. Aside from the obvious crimes such as murder, there may be financial, computer and drug trafficking crimes that would be of interest to foreign powers.

However it should be noted that only information up to OFFICIAL SENSITIVE will be processed and as such there will be instances where information is classed at a higher level and as such cannot be processed on DESC. Further discussions will be required by the partners in this respect.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you and more broadly?

The purpose is the law enforcement purpose. It's the automation of what is currently a manual process that does not fit the needs of the public and results in data losses, offenders not being identified quickly and the public being disaffected with the police/judicial system.

The automation will allow the public to engage in a way that they have never been able to before. As an example, they will be able to send mobile phone footage directly to the police. This can help the police action resources, detect offenders quickly and also identify a locus.

The current system for processing digital evidence is clunky and results in delays throughout the process. This will speed things up for the public and the police resulting in a more efficient policing and courtroom experience. It will also reduce data losses as there will be no hard copy data.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The public regularly criticise policing in Scotland for lagging behind Forces in E&W in terms of their ability to accept digital evidence such as home CCTV and dash-cam footage. However, the storage of this data involves significant cost and as such can only be realistically achieved using an external provider.

The data being processed is not new, it's the methodology that's new. As all the organisations have ethics, security and privacy practitioners representing the interests of the public, it is not felt that further consultation is required.

There has been media coverage surrounding the procurement of DESC.

The purpose of this DPIA is to highlight risks/issues that may affect data subjects. Unusually the DPIA has been authored by the DPO, not the business area - such is the concern for getting this right.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis is Public Task.

There will also be instances where consent will be sought in terms of the use and destruction of digital evidence provided by members of the public.

The processing:

is necessary for the exercise of a function conferred on a person by an enactment or rule of law **and** is necessary for reasons of substantial public interest

is necessary to protect the vital interests of an individual

is for the administration of justice

is necessary for the safeguarding of children and of individuals at risk

relates to personal data manifestly made public by the data subject

Only data currently being processed and already subject to weeding and retention rules will be processed.

The processing via DESC will achieve a far superior crime scene to court experience not just for the partner organisations, but for the public.

Policing could continue with the current, poor, service where data security incidents are a regular occurrence and we lose vital evidence as members of the public will not submit their devices to us to allow for extraction of video.

There is no room for function/scope creep from an SPA perspective. The product has limitations for SPA. At this point there has been no formal decision on what SPA will ingest, but it is likely to be confined to digital productions.

The contract specifies the security and DP requirements, including UK sovereignty and specifies that international transfers can only be made with the Controllers consent.

SPA cannot make international transfers of Law Enforcement Data to anyone other than a relevant authority. Therefore, transfers to overseas Cloud providers, Axon USA or sub-processors outside of the UK would not be legal. Axon have been made aware of this limitation.

Step 5: Identify the Risks

CLOUD Act

The CLOUD Act gives U.S. Law Enforcement Authorities and the foreign state the power to request data stored by most major Cloud providers (including Microsoft), even if it's outside the USA.

We know that Microsoft has been a strong opponent of requests for data from the U.S. Authorities and they do have the right to challenge an order.

This legislation also covers Axon. Axon have stated that they would resist any request that they felt was manifestly unfounded.

This risk does seem to have considerable mitigation – probably enough to reduce the risk below which it would require an adequacy agreement (the impact may be high but the probability will be low).

However, it may only take one high profile case to change that. The kind of case that may give rise to this type of concern may be a high profile case involving US citizens. If the US authorities felt that they were not being provided with all the information timeously would they consider using this legislation to compel Axon/Microsoft to provide data from DESC?

As Axon hold the encryption keys they would be able to decrypt and provide the data, potentially without our knowledge or consent, where compelled by US authorities to do so.

Hyperscale Cloud/Sub-Processors

The Axon Evidence solution uses Microsoft Azure. There are a number of issues where there is no clarity/ambiguity in terms of Microsoft Terms and Conditions in respect of the suitability of this service for processing Law Enforcement Data.

At least 2 magazine articles have been published stating that Microsoft Azure is not compliant for the processing being undertaken by Policing in the UK. There does not appear to have been a denial or rebuttal published by Microsoft. Indeed, there may even have been a tacit admission of weaknesses in their product when they stated in a blog post that they would make Azure GDPR compliant by the end of 2022.

In early June 2022 the Scottish Police Authority requested, via Microsoft re-seller Phoenix, that Microsoft confirm in writing that MS Azure operates in compliance with Part 3 of the Data Protection Act 2018, and in particular is compliant with the S73 requirements. The response was that 'Microsoft would consult their CELA and respond, however, it may take some time'. This response does not give the controllers the level of confidence they might have hoped for.

There appear to be issues with compliance in respect of the following areas;

1. Microsoft acts as a data processor as the provider of Azure Cloud services to Axon. Microsoft's standard data processing addendum (DPAdd) applies. The DPAdd is drafted primarily to apply to processing that is covered by the GDPR, rather than the DPA 2018. The DPAdd states '*Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer*

or Customer's industry that are not generally applicable to information technology service providers.' It is unclear what Microsoft means by this which may affect our ability to comply with Part 3 requirements, including rights of access. Furthermore, the Microsoft DP Addendum (DPAdd) refers to GDPR, the European Union and Member State law in attachment 1. The UK is not a member of the EU.

2. Details of sub-processors provided by Microsoft do not contain sufficient details about the processing carried out by each sub-processor;
   Microsoft is generally authorised to appoint sub-processors listed on its website; if it wishes to change a sub-processor it will give the controller six months' notice; the controller can object; if the controller does so, the controller's only remedy is to terminate the affected services. It's unclear what impact this may have on service delivery.

3. Both the UK GDPR and the DPA 2018 require the contract with a processor to set out the nature, scope and purposes of the processing, however, the contract between Axon and Microsoft does not contain this granular level of detail. MS relies on standard contracts thus there is no evidence that a formal "guarantee to implement technical & organisational controls that meet all processing requirements of DPA 2018 Part 3 Chapter 4" exists.

4. The position with regard to international data transfers in the Microsoft DPAdd is complicated. Whilst data is held in the UK, the DPAdd states that data may be transferred to, or processed in, the US or any other country in which Microsoft or its processors operate. There is no list of countries/transfers or adequacy mechanisms relied on for particular transfers, although SCCs are incorporated into the DPAdd. The EDPS has raised this as a risk in its investigation report, and the Schrems II judgment has had a significant impact on the risk. Microsoft still refers to Privacy Shield in the Data Transfers section of the DPAdd, but then states it does not rely on the Framework as a legal basis for transfers. It is, therefore, unclear why Privacy Shield is cited.

   Microsoft continues to advertise that Azure is 'Police Approved'. However, it should be noted that this approval was in 2017 and thus pre-dated both the DPA 2018 and Schrems II.
   Police in the UK have reached a major milestone – they can store data in the cloud (microsoft.com)

5. Microsoft products are used on the basis of agreeing to their standard terms and conditions. There are no 'customer specific' contracts. The obligations in S59 (Part 3) DPA 2018 require a contract to be in place that details the nature of processing etc.

6. There is a risk that Microsoft could process data in contravention of S73 (Part 3) of the DPA 2018 (Transfers). Their standard T's& C's specify compliance with GDPR but not Part 3 DPA 2018, which is specific or Law Enforcement processing by competent authorities.

Processor Risk

7. The terms of the contract were clear in respect of data sovereignty, however, during due diligence it became clear that Axon may not have been fully

conversant/understanding of this term as services within the solution processed data in the USA.

General SPA Risk

8. Cloud is an attractive solution given its cost, high volume throughput and storage capacity. There is a risk that this will lead to too much data being collected and data being held for longer than is necessary for the purpose.

9. As law enforcement bodies move wholesale to Cloud, this creates a risk in terms of the data all being held in the one place, particularly since the majority of policing data will be in MS Azure UK Data Centres. A large scale attack on Cloud or ISP providers could disable large swathes of the public sector, including policing, making it an attractive target for threat actors.

Step 6: Asses Risks

	Describe the source of risk and nature of potential impact on individuals.	Likelihood of Harm	Severity of Impact	Overall Risk
No	*In some cases where the impact of the risk may be catastrophic the overall risk is elevated to HIGH*	1.Remote 2.Possible 3.Probable	1. Minimal 2.Some 3. Serious	Low 1-3 Med 4-6 High 7-9
	Sub processor Risk CLOUD Act			
1	**There is a data protection risk related to the possible access by US law enforcement and secret services to very sensitive and special categories of personal data.** *Although the likelihood is low, the risk has been elevated to High from an impact perspective as the potential consequences for data subjects and the controllers is the key risk. Should this risk materialise processing may need to stop with immediate effect. As encryption is not mentioned as a mitigating measure in Part 3, this has not been applied to the risk.	Remote	Serious	High
	Hyper scale Cloud			
	In DPAdd, the obligation on Microsoft to assist controllers with complying with data subject rights requests only refers to data subject rights under the "GDPR".			
2	**There is, therefore, an increased risk that personal data cannot then be easily collected and collated by the original data controller in order to fulfil a DSAR or information rights request**.	Possible	Some	Medium
3	**There a risk that the controllers will not have sufficient control or choice over sub-processors that are used by Microsoft, as there is no way to prevent a sub-processor from being used without terminating the services.**	Possible	Some	Medium
4	**There is a risk that Microsoft could vary its DPAdd or other terms unilaterally and that this could result in Microsoft becoming a controller and determining the parameters of the processing itself. This could affect purpose limitation as it could result in data being processed for a new purpose without the controllers' knowledge.**	Remote	Some	Low
5	**There is a risk that there is no binding contract with Microsoft in terms of S59(6)(F) DPA 2018**	Probable	Serious	High
6	**There is a risk that Microsoft could process personal data outside the UK/EEA without any visibility or control over this processing for the controllers.** As encryption is not mentioned as a mitigating measure in Part 3, this has not been applied to the risk.	Probable	Serious	High

Step 6 c'td

7	Processor Risk There is a risk that Axon UK will transfer Law Enforcement Data to the USA without the knowledge or consent of the Data Controllers and in breach of the DPA 2018	Probable	Serious	High
8	General SPA Risk There is a risk that more data than necessary will be stored due to the availability/pricing of Cloud and that once committed there will be no option to roll back should risks escalate.	Probable	Some	Medium
9	There is a risk of Hyperscale Cloud providers being subject to widescale failure/attack rendering DESC inaccessible. Whilst in the early stages this may not be an issue as the legacy manual system can be implemented, through time users will lose the knowledge of the previous systems/legacy systems will have been decommissioned.	Remote	Serious	Low

Step 7: Identify Measures to Reduce Risk

Identify measures you could take to reduce/eliminate Medium/High Risks

Risk	Options to reduce/eliminate risk	Effect on risk	Residual Risk	Approved
		Eliminated Reduced Accepted	Low Medium High	Yes/No
1	Axon have already advised that they would oppose any request that they thought was manifestly unwarranted, however, the risk lies out-with the control of the supplier. Whilst we believe that both Microsoft and Axon would challenge orders they may be required to provide the information and that requirement, and the ability to tell us, may be out-with their control. Whilst it is felt unlikely that this risk will materialise the fallout would be cataclysmic. An agreement with the US/UK that they will not seek access to Law Enforcement data would remedy this matter. However this is out-with our control.	Accepted	Medium	
2	Microsoft have been asked to provide specific assurance in respect of the processing of Part 3 data (7June). Currently awaiting an answer.		Medium	
3	Review changes to sub-processors as soon as notification received to ensure that any risks or issues are picked up and flagged with Microsoft to resolve as soon as possible. However, unknown what the outcome of that may be if MS are not in agreement with our issue.		Medium	
4	Microsoft have been asked to provide specific assurance in respect of the processing of Part 3 data (7June). Currently awaiting an answer..		Low	
5	Microsoft have been asked to provide specific assurance in respect of the processing of Part 3 data (7June). Currently awaiting an answer. MS does not produce contracts specific to each business. All contracts are generic.		High	
6	The contract with Axon is clear that data sovereignty must be maintained. There are concerns that the standard contractual clauses with MS do not meet the requirements of S59 of DPA. MS asked for view on Part b3 compliance.		High	
7	Axon reminded of the data sovereignty requirements and required to provide evidence of compliance. Ongoing monitoring of processing and reporting to be undertaken.	Reduced	Medium	
8	Robust business continuity plans must be in place in Axon and SPA. Plans must be tested and regularly reviewed.	Accepted	Low	

It should be noted that the DPIA is a living document and risks may be added or removed during the lifetime of the processing/project.

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Lindsey Davie January 2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: The ICO has been consulted re the HIGH risk processing. Interim advice has been provided, but a written summary has not yet been delivered. SPA should exercise caution in respect of proceeding with the project before this written advice has been received. SPA should ensure that the relevant risks raised by Counsel are managed or mitigated to such an extent they can be accepted. The partners, including SPA, must be alert to the possibility of data leaving the UK and the measures they must take to prevent this/report it to ICO should it happen. The partners/SPA must ensure regular audits/assessment are undertaken to ensure compliance with the contract and any subsequent written instructions provided to Axon. Assurances need to be sought from Microsoft given the huge amount of data they have in the area of sovereignty, much of it conflicting.		
DPO advice accepted by: SIRO	Chris Brown January 2023	If overruled, you must explain your reasons
Comments: As SPA will have no direct participation in the DESC pilot, there is no necessity for any decisions to be made at this point in time. DPO instructed to keep a watching brief on the pilot and to report back when written advice is received from ICO.		

Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by: SPA IM Lead		The DPO should also review ongoing compliance with Data Protection Law

Appendix A – Screening Questions

We always carry out a DPIA if we plan to:

☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
☐ Process special category data or criminal offence data on a large scale.
☐ Systematically monitor a publicly accessible place on a large scale.
☐ Use new technologies.
☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
☐ Carry out profiling on a large scale.
☐ Process biometric or genetic data.
☐ Combine, compare or match data from multiple sources.
☐ Process personal data without providing a privacy notice directly to the individual.
☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider whether to do a DPIA if we plan to carry out any other:

☐ Evaluation or scoring.
☐ Automated decision-making with significant effects.
☐ Systematic monitoring.
☐ Processing of sensitive data or data of a highly personal nature.
☐ Processing on a large scale.
☐ Processing of data concerning vulnerable data subjects.
☐ Innovative technological or organisational solutions.
☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

If we decide not to carry out a DPIA, we document our reasons.

We consider carrying out a DPIA in any major project involving the use of personal data.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

SUB-PROCESSOR	PROCESSES CUSTOMER CONTENT?	PROCESSES PERSONAL DATA?	LOCATION	FUNCTION(S) PERFORMED
Microsoft Corporation (ONLY Azure Services)	Y	Y	See: Server and Data Location	Infrastructure and Platform Services
Amazon.com, Inc.	Y	Y	See: Server and Data Location	Infrastructure and Platform Services using services such as Amazon Web Services
Black Berry Limited	N	N	United States	Security Investigations using services such as Blackberry Cybersecurity (fka Cylance)
Fastly, Inc.	N	Y	United States	Web Security Monitoring using services such as Signal Sciences
Atlassian Pty Ltd	N	N	United States	Operational Monitoring, Security Investigations, & Corporate Services using services such as OpsGenie
ServiceNow, Inc.	N	Y	United States	Security Investigations
Mixpanel, Inc.	N	Y	United States	User Analytics
Alphabet Inc.	N	Y	Various	Service Support & Client Push Notifications using services such as Crashlytics, & Google Cloud Messaging
Twilio Inc.	N	Y	United States	User Authentication & SMS Communications
Qualcomm Technologies, Inc.	N	Y	United States	Geolocation Services in Devices using services such as Skyhook
Esri	N	Y	United States	Geolocation Services in Products
Apple Inc.	N	Y	Various	Client Push Notifications using services such as Apple Push Notifications
Salesforce, Inc.	N	Y	United States	Account Management, Email Communications & Corporate Services using services such as Slack
RingCentral, Inc.	N	Y	United States	Customer Service
Microsoft Corporation (Non Azure Services)	N	Y	United States	Account Management, Email Communications & Corporate Services
Flock Group, Inc.	Y	Y	United States	Vehicle Insights for ALPR

From: [redacted]
Sent: 09 December 2022 10:00
To: Davie, Lindsey [redacted]
Cc: [redacted]
Subject: ICO to partners re DESC/Cloud issues

Dear colleagues

Thank you for meeting with us at such short notice. We discussed questions on 3 interrelated topics around the DESC programme that had been raised with us – I have summarised our thinking at present below.

International transfers for the purpose of system/tech support

We understand that technical support for DESC may at times be provided by teams in a third country without a UK adequacy decision.
Our initial view is that:

- if technical support staff in a third country access personal data on DESC this would constitute an international transfer under data protection law.
- This processing would fall under Part 3 of the Data Protection Act 2018 (DPA 2018).
- These transfers would be unlikely to meet the conditions for a compliant transfer set out in s73-76 DPA 2018.

In order to avoid a potential infringement of data protection law we strongly recommend ensuring that personal data remains in the UK by seeking out UK based tech support. If 24 hours support is required and a 'follow the sun' approach is necessary to deliver that, it may be that technical questions could be answered by support teams based in third countries without these teams accessing and processing any personal data.

As discussed we are currently seeking a view on whether the processing for the purpose of tech support may fall under UK GDPR as supplemented by DPA18. However we must emphasise that at this stage we do not have a formal view. We intend to come to you in writing with a formalised view as soon as possible – which may differ from the statement above. If this is the case we will detail why.

The US CLOUD Act

We understand that your contracted processor Axon will use Microsoft as a sub processor. Microsoft is an American company and subject to requests through US CLOUD Act.
You have raised an interesting question regarding the potential transfer of personal data by Microsoft to a US law enforcement agency under a warrant granted under the CLOUD Act would constitute an international transfer under Part 3 DPA 2018. Although we do not think that it is the intention of the legislation, the drafting may lead to such a transfer being, in principle, possible.

In any event, partners involved in the DESC project must be assured they are meeting all their obligations under data protection law including those set out in S59, S64 and S66 of the DPA 2018.

Again, this comes with the caveat this is our initial view only. We intend to come to you in writing with a formalised view as soon as possible – which may differ from the statement above. If this is the case we will detail why.

Variability of the contract with Microsoft / EDPS paper

We understand that you have concerns that there is no contract in place between Axon and Microsoft and that Microsoft may vary the service provided without your agreement as a controller. We would expect Police Scotland / the Scottish Police Authority/ COPFS to take all reasonable steps to ensure compliance with s59 DPA 2018 and to mitigate and safeguard against any risks that Microsoft (as sub processor) may vary the terms of the contract without Police Scotland / SPA/ COPF's agreement.
Please keep us updated on:

- Whether you decide to progress with the pilot in January
- If you do decide to move ahead with the pilot the actions that you have taken in relation to our advice above.

Any questions do let us know.

Regards,

[redacted]

[redacted]

Information Commissioner's Office, Queen Elizabeth House, Sibbald Walk, Edinburgh EH8 8FT.

T. [redacted] **ico.org.uk twitter.com/iconews**

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

From: [redacted]
Sent: 21 July 2022 16:13
To: Davie, Lindsey [redacted]
Cc: [redacted]
Subject: RE: HyperCloud [OFFICIAL]

Hi Lindsey,

We are not aware of any approval or assurance in terms of processing in the cloud. Can the NPCC provide documentation/correspondence with ourselves?

I can advise that we are almost finalising the legal advice on the forensics processing however we need more detail re DESC/cloud processing. Can you send us the latest version of the DPIA. Given your concerns you might wish to consider submitting the DPIA to us for prior consultation under s65 DPA 2018 so we can take a look and give you a clear position.

If you'd like to have a discussion on any of the above [redacted] and I are around tomorrow afternoon. [redacted] goes on leave for two weeks from tomorrow.

Regards,
[redacted]

[redacted]

Information Commissioner's Office, Queen Elizabeth House, Sibbald Walk, Edinburgh EH8 8FT.

T. [redacted] **ico.org.uk twitter.com/iconews**

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

From: Davie, Lindsey [redacted]
Sent: 21 July 2022 10:35
To: [redacted]
Cc: [redacted]
Subject: RE: HyperCloud [OFFICIAL]

External: This email originated outside the ICO.

OFFICIAL

[redacted]

My life has been more or less consumed by this for a number of months and I think it can actually be distilled down to some fairly simplistic facts;

The major Cloud providers (AWS/MS) state clearly that they abide by data sovereignty for data at rest. But none of them make any mention/statement about data in transit or access to the data at rest from out-with the UK. I believe this to be telling. Having asked them this question I have been waiting several weeks for their lawyers to answer – so clearly it's not something that they can 100% answer without hesitation.

MS has added this statement to their Data Protection addendum, again, I find this telling;

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers.

I fully understand that it's our responsibility as the data controller to make the call – which is what I have done. However, I have been faced with the response that this 'has all been approved by NPCC/National Accreditor/SiRO in agreement with the ICO' (as in use of Cloud for Law Enforcement Processing). Hence I really need to know if the ICO has agreed that this is all OK.

Thanks

Lindsey

Lindsey Davie
Information Management Lead

Scottish Police Authority/ Ùghdarras Poilis na h-Alba
1 Pacific Quay
Glasgow
G51 1DZ

Tel / Fòn: [redacted]
Mobile [redacted]
Email / Post-d: [redacted]
Website / Làrach-lìn: **www.spa.police.uk**
Twitter: @ScotPolAuth