From: [redacted]
Sent: 06 April 2023 16:00
To: Dominique Mitchell <Dominique.Mitchell@ico.org.uk>
Cc: Jenny Brotchie <Jenny.Brotchie@ico.org.uk>; [redacted]
Subject: PSoS Response [OFFICIAL: POLICE AND PARTNERS]

External: This email originated outside the ICO.

OFFICIAL: POLICE AND PARTNERS

Dear Dominique,

I'm glad you were able to attend for the demonstration and am glad that you found it useful. I look forward to receiving your comments and advice.

In respect of the high risk items I do not think the scoring has been accurately recorded in terms of "residual risk" and I apologise for any confusion. I will take this as a learning point and seek to improve how this is depicted in future DPIAs.

In order to comply with Part 3, PSoS is clear that law enforcement data

(Content data) must be stored and processed within the UK at all times.

The DESC Contract mandates the use of UK-based data storage and processing to support this, and Axon has confirmed this in writing. In delivering this requirement, Axon has partnered with Microsoft to deliver the cloud infrastructure and storage of the DESC Solution. Microsoft's data centres are located in the UK and are assured to national policing standards set by the Home Office.

PSoS as Lead Data Controller has undertaken due-diligence in respect of compliance with S59, S64 and S66 of the DPA18.

Axon provided PSoS with the following information:

- Details of its contract with MicroSoft which states that data will only be processed in the 2 PASF assured data centres in the UK
- Sub-processor agreements
- assurance that all sub-processors engaged are subject to the Terms and Conditions as per the contract
- assurance that data is encrypted at rest and in transit and that data stored in the Cloud would be encrypted by the supplier prior to moving it into Microsoft data storage
- Any use of the US Cloud Act to access data requires the supplier to decrypt the data, and the supplier confirmed that such a request would be legally challenged by the vendor and the client informed of the request

Under the US CLOUD Act issue, DESC data could, in theory, be obtained via US orders by warrant, subpoena or court order. Although technically possible, it would seem ***unlikely*** that US authorities would compel Axon or Microsoft to disclose data (constituting an international transfer Under Part 3 DPA 18) held within the DESC Solution given the data it contains (subject of an investigation and prosecution taking place under Scottish jurisdiction). This is unlikely to fit well within the scope of the CLOUD Act or Bilateral Agreement and PSoS do not think that it is the intention of the legislation.

The CLOUD Act is also more specific about what persons it covers. The Act and Bilateral Agreements between two nation states are intended only to be used to target citizens or residents of the country seeking the order. It is therefore unlikely that it extends that it could not compel the release of data held about DESC partner's staff and end users, who are unlikely to fit the criteria of a US person or resident. However there is no known case law to date to illustrate this position.

DESC Programme's exposure to this would be limited and potentially remote. The majority of data would be held about UK persons and persons resident in the UK (and more specifically, Scotland) and PSoS considers the risk of exposure to a US-based order to be low.

At the point of pilot, Axon had provided a list of sub-processors with only Twilio and Microsoft being relevant at point of pilot. Mitigations were in place to ensure that Twilio SMS was not utilised during pilot.

This did occur on 3 instances within the first week of pilot and the notification system which formed part of the mitigations alerted PSoS immediately (previously highlighted to ICO) and further controls were deployed which yielded no recurrence. A further control has been implemented in that the capability has been blocked in its entirety and as a result this risk has been effectively removed.

Mitigations considered for pilot were that Microsoft only processes data only in the 2 PASF assured data centres in the UK and data in transit is encrypted. Further diligence is now being undertaken with regards the specific sub-processor engagement to be in line with the full Terms and Conditions as per the contract.

PSoS recognises the risks described but considers the use of a global cloud provider is the only real and practical solution. This is informed by current understanding around the risk and likelihood of our data being exposed in such ways and the need to operate modern and secure environment for the collection and management of law enforcement content across disparate partners.

The DPIA that existed prior to pilot identified high risks but suitable mitigations as outlined were in place and the DPIA was being updated as regularly as possible through consultation with partners, legal practitioners, data protection and security representatives and regular consultation with ICO for guidance and advice. Consideration was given to making a request under Section 65 DPA 2018 however given;

a) the mitigations that were in place or planned in the coming days
b) the ongoing and detailed engagement with ICO

it was not viewed that a more formal consultation was not required prior to pilot.

I hope this provides further clarity.

I'm finishing up today for annual leave and won't be back in office until the 17th. I suspect that your office will also be closed for the Easter weekend however, if you require any further clarification prior to the 17th then please contact [redacted] in the first instance.

Kindest Regards

[redacted]
Data Protection Officer

Governance, Audit & Assurance
Police Scotland Headquarters
Tulliallan Castle
Kincardine
FK10 4BE

DataProtection@scotland.police.uk

Website: www.scotland.police.uk
Twitter: @policescotland
Facebook: www.facebook.com/policescotland

Dear [redacted]

Thank you for hosting us in Dundee and organising the viewing of DESC in action, it was really useful to see it first hand. We are currently drafting our final comments and advice based on the DPIA and the visit, and hope to provide you with that as soon as we can.

However, we note that in the DPIA there seems to be two high risks that have not been reduced but have been 'accepted' and we wanted to seek clarity on these. In our meeting of 19 January 2023 it was our understanding there were no unmitigatable high risks outstanding and therefore the processing could go ahead, and the DPIA wouldn't be submitted to us under s65 DPA 2018 but rather it would be provided to us informally. The two risks that we are referring to are as follows:

- Processing Law Enforcement Data using a Contractor and SubProcessors which operate under the jurisdiction of the US Cloud Act
- There is a risk that subprocessors engaged by the Supplier are not subject to the Terms & Conditions in Services Contract Reference 388514

As you will know if you have carried out a DPIA that identifies a high risk, and you cannot take any measures to **reduce** this risk, you need to formally consult with us under Section 65 DPA 2018. You cannot go ahead with the processing until you have done so.

Can you clarify whether both of these risks been assessed correctly? For example: it appears that you have assessed that the risk relating to the Cloud Act has a low probability but a high potential impact - is the overall risk rating correct? If yes, they have both been assessed correctly, are you able to explain why the DPIA wasn't submitted to us under s65 DPA 2018?

Regards,
Dominique

Dominique Mitchell (she/her)
Senior Policy Officer – Scotland

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

T. 0330 313 1715 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

Data Protection Impact Assessment:
Digital Evidence Sharing Capability (DESC) – Overarching DPIA

Law Enforcement Processing (content data)
UK GDPR Processing (non content data)

Control Sheet

URN (to be completed by Information Assurance)	22-389
Date Approved	
Version Number	V1.0
Document Status	In progress
Author	PSoS Information Manager (Assurance) on behalf of DESC Data Protection Working Group
Senior Responsible Owner (Project)	Andrew Hendry, PSoS Chief Digital and Information Officer on behalf of DESC
Transformation Project	Yes ☒ No ☐
Is this project a pilot?	Yes ☒ No ☐
Date on which the proposed processing is to start (if known)	24 January 2023

Revision History

Version	Date	Summary of Changes
V0.01	12/10/2022	Draft provided to DESC DPWG members
V0.02	28/10/2022	Draft provided to DESC DPWG members
V0.03	23/12/2022	Draft provided to DESC DPWG members
V0.04	17/01/2023	DESC Senior Project Manager reviewed and commented and draft provided to DESC DPWG members

Part 1 – Determining whether the proposed processing of personal data for law enforcement purposes is likely to result in a high risk to the rights and freedoms of the data subject.

Once completed, this part will be considered to decide whether the proposed processing is high risk.

Part 1, Section 1 – General

1.1.1 Does the project involve the processing of personal data?	
☒ Yes ☐ No – Please provide a summary of the project below and submit this DPIA to Information Assurance without completing any further answers.	
Click here to enter text	
1.1.2 Who is the Lead / Manager / Senior Responsible Owner for the project?	
Name	Andrew Hendry (SRO)
Designation	Chief Digital and Information Officer, Police Scotland
Contact details	[redacted]
1.1.3 State who has responsibilities for the personal data. (Refer to Note 1 of the Part 1 Guidance Notes)	
Strategic Information Asset Owner	
Name **Designation** **Contact Details**	Scottish Government Scottish Government acts as the Contracting Authority Scottish Police Authority (SPA Police Service of Scotland (PSoS) Steve Johnson ACC Criminal Justice [redacted] Police Scotland also acts as Lead Controller and Delivery Lead Crown Office and Procurator Fiscal Service (COPFS) Keith Dargie Head of Business Services [redacted] Scottish Courts and Tribunals Service (SCTS) David Fraser Executive Director of Operations
Tactical Asset Owner	
Name	Supt. Damian Armstrong
Designation	Supterintendent, DESC Programme
Contact details	[redacted]

1.1.4 Provide a summary of the project.

Digital Evidence Sharing Capability (DESC) is a project funded by the Scottish Government (SG) for collaboration between Criminal Justice partners, namely the Police Service of Scotland (PSoS), Scottish Police Authority (SPA), Crown Office and Procurator Fiscal Service (COPFS) and the Scottish Courts and Tribunals Service (SCTS).

The SG Justice Digital Strategy pledged to modernise criminal and civil law and the justice system through digital transformation. DESC is a key component of that transformation. The DESC Programme is a technical software deployment of implementation services and operational services and also a package of work to enable operational and legislative change for the collection, editing and sharing of digital evidence at every stage of a criminal case and prosecution across the justice sector, delivering a digital pathway from 'crime scene to court room'. It will deliver an end-to-end service for the collection, management and sharing of digital evidence for all Criminal Justice partners, however in this initial phase, this will be limited to PSoS, SPA, COPFS and SCTS.

Digital evidence may include public and private space CCTV, body worn video, evidential calls to police control room, police interviews, photographs, documents, digital evidence from computers / mobile devices and digital evidence from devices such as dash cams and video doorbells.

DESC will:

- provide the capability to collect and securely share digital evidence between Criminal Justice partners,
- 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, generating variant files, sharing evidence and the retention and disposal of content.

DESC will replace existing processes for the collection, sharing and management of digital evidence.

This large-scale and complex programme is transformational in its ambition; it will radically modernise the parts of the justice system it impacts. However, while DESC is significant in relation to the benefits it will deliver in itself, its value lies in its potential as a platform for further transformation. DESC lays the foundation for a truly modern criminal justice system which places the needs of Victims, Witnesses, and other users of the justice system at its heart.

The DESC solution consists of two main technologies; Axon Capture mobile device app and Evidence.com. which is a secure website. Axon is the provider of the SaaS (Software as a solution) portal through which data is accepted and transferred to the Cloud. Axon Capture will be deployed on Officers' mobile devices. There are three 'instances' of DESC, for PSoS/SPA, COPFS and SCTS, all on the same platform.

Future integrations are planned with PSoS DESC and its 'Unifi' Productions, CRIME and CASE systems, which are used to support criminal investigations before reporting to COPFS. These integrations will improve usability and reduce human error. Data will transfer between systems, examples of which include name of the Officer seizing, date/time seized, unique production number and retention category (how long we are legally required to hold data). Integrations are focused on reducing manual data input and will be subject to further DPIA assessment as they are planned.

In operational terms, a Police Officer will send a member of the public an email link to the DESC solution to upload digital evidence to DESC about a crime or incident that they have been a Victim of, or Witness to. The email link will include the STORM reference number and a short invite from the Officer. DESC is not a public portal and without the link, members of the public will not be able to submit any evidence to it, nor will they be able to use the link more than once to submit evidence. The link will take the member of the public to Evidence.com, the Cloud platform, where they can securely upload their evidence and complete Schedule 8 Certification. This certifies data as a true copy for the

Scottish Criminal Justice process. Once submitted, the evidence and certification is encrypted and transferred into DESC, with a notification sent to the requester. The Police Officer who sent the link will also receive a notification by email to confirm digital evidence has been submitted.

Police Officers and staff and SPA forensic staff (beyond Stage 1 Delivery Pilot) will also be able to upload digital evidence, including that seized or obtained under warrant, to DESC. Secure standalone workstations controlled by Police Scotland's Digital Division will be deployed in Police Stations across Police Scotland.The workstation will allow media to be accessed and evidence uploaded onto DESC. The DVD/USB etc. will be stored securely as evidence. Where an Officer needs to collect the evidence in circumstances when neither an email invite can be used, or media available from the public, a PSoS USB will be issued by their local Business Support Unit (BSU). Further assessment of these arrangements will be part of the project.

Once on DESC, digital evidence will be triaged and accepted by the requesting officer or an enquiry officer in circumstances where the investigation has been re-allocated. Police Officers will use the evidence to investigate the crime or incident and triage this, which may include converting the format, prior to sharing that to the COPFS instance of DESC. All digital material will be checked for threats, and should any threat be identified, the material will be placed into digital quarantine for assessment until it is deemed safe to release the file.

All material will be given a lead agency reference number by PSoS, which is the Crime Reference Number (CR number). Police Officers will also, during Stage 1 Delivery Pilot, create and record Productions reference number using a link to the 'Unifi' Productions system. When a suspect is identified, a Standard Prosecution Report (SPR) will be prepared and submitted for quality assurance to the Police Case Management /Assessment Units who will transfer the SPR to COPFS which will contain a link to the digital evidence within DESC when future integrations are in place. At Delivery 1 Pilot, COPFS will access DESC and search for the digital evidence using the PF Reference Number.

PSoS has the ability to edit multimedia prior to onward sharing to COPFS. Where this occurs, the original footage will remain intact within the PSoS DESC instance, should it be required, with a 'child' file created for the edited version. If required the staff member will certify this as a true copy of the original and complete any necessary certification within the solution This complies with disclosure duties under section 12 of the Criminal Justice and Licensing (Scotland) Act 2010.

The relevant evidence will be copied by PSoS into the COPFS instance of DESC. It will be allocated the relevant COPFS reference number. PSoS will notify COPFS within the SPR or Ancillary report that evidence is held in DESC. In the longer term the link to the evidence will enable prosecutors to easily find the evidence and consider this for prosecution purposes and determine the next actions pertaining to potential criminal proceedings. COPFS staff will be able to access, edit, redact, transfer, delete, disclosure and present evidence from DESC based on role-based need.

When a case decision is made for criminal proceedings, COPFS staff with appropriate authority will if required, be able to edit the material and create a new piece of evidence within the COPFS instance of DESC only, with a 'child file created for the edited version. If required the staff member will certify this as a true copy of the original and complete any necessary certification within the solution.

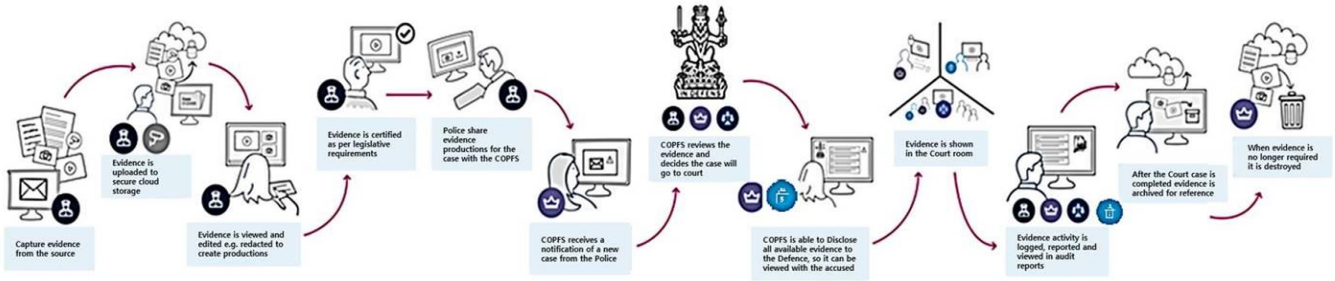
Where specific technical editing is requested by COPFS, PSOS Technical Support Unit (TSU) will undertake this editing within the PSoS/SPA instance of DESC. TSU has access to the original piece of evidence and will create new evidence with appropriate certification. TSU will then share with COPFS as a new piece of evidence. COPFS may in the future, take on more of the responsibility for technical editing, using DESC.

COPFS will share the evidence with the Defence in line with existing disclosure processes and rules. The COPFS staff will utilise a secure defence user account and select this to share the evidence with the defence agent who has provided a letter of engagement for a case. Defence agents must be registered with COPFS and have been allocated DESC access. Defence account details are held within a secure COPFS Azure directory on premise in the UK and synced to allow the Defence to

access their evidence and download this if necessary. This link will only be available for a set period of time, the default being 90 days, although this is configurable by COPFS.

The Prosecutor will be able to play evidence directly from DESC in court or will have the ability to download the material and present evidence in court.

In court, SCTS will provide the equipment and facilitate the viewing of the digital evidence from DESC.



Appendix 1(a) to this DPIA is a PowerPoint presentation that shows, at a high level the operational flow of evidence and the projected benefits of DESC.

Appendix 1(b) to this DPIA shows the process from an Officer's perspective

The foregoing information explains the overall aim of the project. DESC will be delivered in stages and this DPIA updated ahead of each stage go-live.

- Delivery 1 supports the end-to-end process from evidence ingestion to court, focusing on all new multimedia evidence to test the system and facilitate early case resolution. Processing is limited to SPA, PSoS and COPFS.

- Delivery 2 and Delivery 3 will enhance and build upon Delivery 1 including system integrations, Solemn case types, ingestion of existing and emerging evidence types and other considerations such as the case backlog conversion.

- The proposed delivery rollout at 24/01/2023 included in Appendix 1(a). This is a Delivery 1 Pilot and is initially limited to the Dundee City area. It will involve only PSoS and COPFS processing data on DESC.

- The Delivery 1 Pilot is scheduled to last for 6 months.

Part 1, Section 2 – The Purpose of the Processing

1.2.1 What is the reason you want to process the data? If in Q1.1.4 you have covered in full the reason you want to process the data, then please copy and paste the relevant sections here.
Tto facilitate the collection, management, editing and sharing of digital evidence at every stage of a criminal case and prosecution across the justice sector, delivering a digital pathway from 'crime scene to court room'
1.2.2 What is the intended outcome for the individuals whose data you propose to process?

- Improved justice for Victims, Accused and Witnesses through more effective investigation and preparation of digital evidence;
- More secure handling of personal and sensitive data relating to Victims, Witnesses, Suspects and Accused;
- Improved disclosure processes as digital evidence will be readily available in a viewable format for Criminal Justice partners promoting early case resolution which benefits the Victims, Witnesses and Accused.
- Less invasive evidence collection from personal artefacts.

1.2.3 What are the expected benefits for Partners?

Full details of the benefits are listed in the DESC Full Business Case, in summary these include:

- Increased Police Officer productivity through new ability to upload evidence from their mobile device and save directly into DESC where it can be linked to crime/case.
- Police Officers, SPA & COPFS staff can be self-sufficient and can clip and bookmark evidence themselves as required without using technical support units, freeing those staff from the task.
- Reduction in the number of requests from COPFS to Police Officers requesting additional evidence and edits to evidence to prepare them for court.
- Digital evidence can be provided more easily in a court playable format.
- Reduction in criminal justice/court time delays waiting for format conversion of digital evidence.
- Reduction in time spent by staff physically transporting evidence from A to B and the associated administration and management of same.
- Digital certification of evidence can be made available via a highly trustworthy solution.
- Reduction in the number of cases reaching court due to early pleas resulting in less Police Officer time spent having to attend trials.
- Streamlined preparation and presentation in court. Digital media will be in a viewable format from the ingest point and will be accessible from a secure COPFS computer regardless of location. This will allow prosecutors to focus on other areas of case preparation and presentation
- Reduction in time Officers spend attending court regarding technical issues around CCTV evidence and certification.
- Aids compliance with security regulations, standards and guidelines.
- Reduced risk for loss of unencrypted evidence.
- Auditable access and use, in line with the requirements of the DPA18 s62.
- Forensic and cybercrime can transfer, track and manage forensic productions without the need for re-keying therefore allowing evidence to be collated through one solution to be passed to COPFS.
- Single Interface – Integration with the Defence Agent Service will allow visibility of all evidence through a single interface regardless of where the data is being stored in COPFS.

DESC Programme holds a Programme Benefits Register which as a partnership, the Programme will monitor, measure and review throughout Pilot.

1.2.4 What are the expected benefits for society as a whole?

The SG Justice Digital Strategy has pledged to modernise criminal and civil law and the justice system through digital transformation. The 'status quo' is no longer an option for the future of digital evidence sharing. This is because the technology and processes currently used in the justice system in Scotland to capture, assess, store and transfer digital evidence cannot keep pace with the growth in volume and value of digital evidence. Current processes are increasingly labour intensive and with increased volume, less secure and more open to security risks if captured, assessed, stored, edited and transferred on a USB or DVD. The public expects, in a digitally enabled society, to be able to easily, safely and confidentially submit evidence related to crimes and incidents and for it to move seamlessly through the criminal justice process. Partners are working collaboratively, understating that there are intrinsic interdependencies and responsibilities in the criminal justice process which mean that all partners must revise their technologyand operational practices for benefits to be derived. Processing the data in a digital format is a key enabler for wider reform across the whole Criminal Justice sector in the future.

DESC is closely aligned with the vision and principles of the Christie Commission, which aims include the public service working much more closely in partnership to integrate service provision and improve the outcomes they achieve for the public. It also drives us to become more efficient by reducing duplication and sharing commonly procured and developed services and technology

At present, this process is undertaken manualy across the Criminal Justice sector, using hard copy discs / USBs / hard drives, photographs and printed documents which are collected and stored as physical productions. This is recognised as an inefficient process which presents risk in terms of Information Security and personal data breaches.

Part 1, Section 3 – Nature of Processing

1.3.1 Has the Information Security (ISM) Manager been consulted: This should be done at the outset of any project –[redacted]

☒ Yes

☐ No – if not, this must be done immediately.

☐ Not applicable – state below why there is no requirement to consult the ISM.

The Information Security Managers (also known as ISOs) from SPA, PSoS, COPFS and SCTS formed an Information Security Working Group to provide advice and guidance to the DESC Project. Records of the work are held by the Security Managers and by the DESC Project. The ISOs have and continue to will review and approve the security design and assess and accredit DESC for use for policing purposes.

A DESC Security Control Sheet has been established that sets out the security requirements, controls, standards, accreditations and cyber resilience arrangements. It is an auditable evidence-based record of continued adherence to current and developing security requirements and national strategies. Due to the nature of the content, this is a controlled document to which access is limited and it is not detailed further in this DPIA. The supplier also has a copy of this document.

1.3.2 Have the asset owners of any related systems been consulted? (e.g. IT, paper, video etc.)

☒ Yes – If so, provide details.

☐ No – State below at what stage you intend to consult.

DESC Programme and Project oversees the engagement with related systems' asset owners; this includes the involvement of relevant leads within each partner organisation. Representatives of all partners attend a range of meetings to support DESC delivery in their own organisation.

1.3.3 What will the classification of the data be under the Government Security Classification (GSC)? (GSC SOP)

Official ☐ or

Official Sensitive ☒ (NB Official Sensitive **must** be accompanied by handling instructions)

Named Recipients Only ☐ Police and Partners ☐ Police Only ☐

1.3.4 Will any processing be done via an internet / cloud based system?

☒ Yes – Provide the details below.

☐ No

DESC aligns with the Scottish Government's Digital Strategy for Justice in Scotland[1]. This strategy advocates a 'cloud first' approach meaning that public cloud will be the default delivery model for user-focused services. The Digital Strategy for Justice describes a vision of a modern, user-focused justice system which uses digital technology to deliver simple, fast and effective justice. It recognises a need to use digital technology wherever possible to broaden access to justice, improve quality of service and safeguard the rights of citizens and users.

Therefore, DESC technology is made up of a suite of interactive and dependent products. Digital evidence will be stored and accessed in a Microsoft Azure Cloud based system known as 'evidence.com'.

'Axon citizen' will be used to email a unique link to 'evidence.com' to members of the public to allow them to upload their digital evidence.

A disaster recovery backup will be held on Amazon Web Services cloud based system.

1.3.5 Will any processing of personal data be done jointly with another organisation?

☒ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☐ No

[1] The Vision for Justice in Scotland - gov.scot (www.gov.scot)

Processing on DESC is separated into 2 distinct types: 'Non-Content' Data and 'Content' Data.

'Non-Content' Data means the data processed by DESC for general contract management purposes and in accordance with the UK-GDPR, comprising limited personal data to facilitate user authentication, logon, permission management, platform performance management, maintenance and auditing. Non-Content Data is processed independently by each Data Controller. There are 5 (five) independent Data Controllers, namely SG, SPA, PSoS, COPFS and SCTS. The SG is limited as a Data Controller to Non-Content data for the purposes of contract management (as the contracting authority).

'Content' Data is means the Personal Data processed by DESC by a competent authority (as defined in the Data Protection Act 2018 section 30 (1)(a) and Schedule 7 or section 30(1)(b)) for law enforcement purposes in accordance with Part 3 of the Data Protection Act 2018 ("law enforcement processing"). Content Data is processed jointly by 4 (four) Data Controllers and clarification of the data processed jointly is contained in Appendix 2. Where partners process jointly, PSoS is the agreed Lead Controller. A Joint Controller Agreement has been agreed by the partners.

SPA: DPO - [redacted]
PSoS: DPO - [redacted]
COPFS: DPO - [redacted]
SCTS: DPO - [redacted]

1.3.6 Will another organisation be processing any of the personal / sensitive data? (Refer to the definition of processor on page 6 of the Guidance Notes). If so, a contract will be required to regulate the relationship.

☒ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☐ No

Axon Public Safety UK Limited (Axon), a company incorporated under the Companies Acts (Company Number 07390059) and having its registered office at 14 Sopwith Way, Drayton Fields Industrial Estate, Daventry, Northamptonshire, England, NN11 8PB as the supplier of the DESC solution.

Axon was awarded a contract (Services Contract Reference 388514) with the Scottish Ministers acting through the Scottish Government (SG) to supply software and services for DESC.

Axon engages a number of sub-processors, which is permitted under the terms of the contract and is responsible for ensuring that its contractual obligations are also undertaken by its permitted sub-processors. The list of approved sub-processors at date of pilot is contained in the Data Processing Agreement with Axon agreed by the Controllers and the Joint Controller Agreement. Thereafter, any further/new sub-processors must be proposed by Axon to Police Scotland (as DESC Delivery Lead) and SG (as Contracting Authority) in the first instance. Data Controllers will, subject to the successful completion of their due diligence, authorise (or refuse) permission for the use of the sub-processor.

The DPO for Axon is James Wood (jamwood@axon.com)

In addition to the contract, Data Processing Agreements are being completed by 4 (four) Data Controllers with Axon, namely SPA, PSoS, COPFS and SCTS prior to their processing data using DESC.

SG has reviewed the matter and considers that the contract it has with Axon meets its statutory requirements in relation to the limited processing for which it has responsibility.

1.3.7 Will the processing involve new technology?
☒ Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below. ☐ No
A 3rd party supplier (Axon) will provide a SaaS (system as a solution). Axon will provide a bespoke 'DESC' solution comprising of a Microsoft Azure Cloud-based network storage and data transfer platform known as 'Evidence.com' alongside 'Axon Citizen'. This is supported by MS Azure Cloud Services. A schema for Stage 1 Delivery pilot is attached as Appendix 1a & b
1.3.8 Will the processing be done in any novel or unexpected ways? (e.g. machine learning or artificial intelligence)
☐ Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below. ☒ No
No machine learning, artificial intelligence or automated processing will be carried out by DESC

Part 1, Section 4 – Scope of the Processing – What the processing covers

1.4.1 What categories of data subject are involved? (Please select all applicable)

☒ Victims
☒ Witnesses
☒ Suspect
☒ Accused
☒ Person convicted on an offence
☒ Children or vulnerable individuals – provide details below
☒ Other – provide details below

- Members of the public, public sector or business operators in the submission and collection of data to be used in criminal investigations and prosecutions. This will include Victims, Witnesses, Suspects and Accused.

- Third parties who provide supporting information or services, including expert Witnesses, forensic specialists, doctors, social workers, and other health and social care professionals;

- Police Officers and Staff working in criminal justice organisations, including but not limited to Prosecutors; Criminal Defence Solicitors and the Judiciary

Evidence Data will not be processed on DESC either from or about children under the age of criminal responsibility who are Suspected of, or identified as causing harm (ACRA Nominals) for the purposes of reporting to SCRA. However where evidence data has been submitted by a Victim or Witness, subsequent investigations may identify that the individual is a child under the age of criminal responsibility.

Digital evidence provided by members of the public / organisations (Victims, Witnesses, Suspects, Accused) may also contain personal data relating to individuals (including children and vulnerable individuals) that have no connection with a case, but who's data is captured as part of a wider recording, e.g. dash cam footage, CCTV. The data processing carried out by the partners will include mitigations to reduce the impact on these individuals that have no involvement in cases, for example by ''trimming' the length of a submitted CCTV clip to show only the section material to the case which will then be shared by partners. The original submission will however be retained to demonstrate transparency and fairness in the criminal justice process and in line with obligations from COPFS and the Lord Advocate.

1.4.2 What is the source of the personal data? (Please select all applicable)

☒ Victims
☒ Witnesses
☒ Suspect
☒ Accused
☐ Person convicted on an offence
☒ Children or vulnerable individuals – provide details below
☒ Other (e.g. data already held in other Police Scotland systems, partner agencies etc.) - provide details below

Personal data will be gathered directly from Victims, Witnesses, Suspects and Accused who may be individuals or organisations. This may include children or vulnerable individuals that are Victims, Witnesses, Suspects, Accused.

Personal data may also be requested from individuals or organisations that have captured it using technologies such as vehicle dash cameras, CCTV or doorbell cameras but are not a Victim, Witness, Accused or Suspect (e.g. PSoS identify that private CCTV may have captured relevant information and approach the company to seek a copy)

Personal data held on partners' criminal justice systems, on public space CCTV and directly relevant to a case may be shared / processed on DESC

1.4.3 List all categories of personal data to be processed. This should also include the types of information if appropriate, e.g. videos, pictures, audio files.

The following data will be processed in relation to the investigation and prosecution of crimes.

The types of Personal Data and Sensitive Personal Data will include but may not be limited to:

Documents and multimedia (including video, audio and images) containing genetic and biometric data, imagery and audio of persons, names, address, correspondence address, date of birth, date of death, telephone number, email address, Hospital Record Number (or other NHS identifiers), accessibility requirements/preferences, nationality, residency details and related information, immigration status, details of medical conditions and medical history, details of functional abilities and impairments, details of existing or previous care and living arrangements, school details (child only), medical records, and equalities data (sex/gender/race etc.) concerning an individual's sex life or sexual orientation, revealing racial or ethnic origin including immigration status, political opinions, religious or philosophical beliefs or trade union membership and alleged criminal conduct

The following types of data will be processed in relation to:

Third parties who may be asked to provide supporting information (e.g. Professional and Expert Witnesses), subject to the solution design, including:

• Name, address, profession, phone number, email address

Staff working in criminal justice organisations (including, but not limited to: Police Officers; Prosecutors; Criminal Defence Solicitors; and the Judiciary):

• Name, location, staff number, job role, phone number, email address
Electronic communications metadata: call and SMS logs -CDRs, MSISDN, MAC addresses, IP addresses, browsing data, location data, device information, click/UI events, application build number, session duration and accesses.

Inferred information; information inferred based on collected information related to users' location, browsing and consumption habits or general behaviour.

1.4.4 Does this project involve processing sensitive data? If so, tick all categories of sensitive data to be processed.

☒ Race	☐ Trade Union membership
☒ Ethnic origin	☐ Genetic data
☒ Political opinions	☒ Biometric data
☒ Sex Life	☒ Sexual orientation
☒ Religion	☒ Health
☒ Philosophical beliefs	☒ Criminal conviction data
	☐ None

1.4.5 Will the personal / special category / criminal conviction data be shared with anyone?

☒ Yes – provide details below

☐ No

- This data is currently shared between the criminal justice partners; SPA and PSoS to COPFS and COPFS to SCTS. DESC will provide a new platform to facilitate the sharing.
- As part of the criminal justice process, certain data, by law, must be shared with other parties such as defence agents.
- As part of the criminal justice processes, certain data is played in court and therefore will be available to the public who are in attendance.
- Whilst SG is a Data Controller and contracting authority, it will not have access to 'Content' Data on DESC.

1.4.6 Does the proposed processing involve the collection of data not previously collected by Partners?

☐ Yes – provide details below

☒ No

The data has always been processed as part of the criminal justice process, but in a different manner, i.e. manual processes to capture, record and transfer by DVD, USB or similar.

DESC will facilitate the increasing volume of data, in the form of digital evidence, submitted as part of the criminal justice process. The prevalence of personal image recording devices (CCTV, doorbell cameras, dash cameras, mobile phone cameras, etc.) continues to grow in society and DESC will enable that to be more easily ingested into and process through the end-to-end criminal justice process.

1.4.7 Will the personal / sensitive data be fully identifiable, pseudonymised or anonymised?
(Refer to Guidance Note 3 of the Part 1 Guidance Notes)

☒ Fully identifiable

☐ Pseudonymised – provide details of how this will be done, and at what stage in the process

☐ Anonymised – provide details of how this will be done, and at what stage in the process

1.4.8 Does the proposed processing involve any alignment or combining of data sets?
☐ Yes – provide details below ☒ No
Click here to enter text

1.4.9 How many individuals will be affected by the proposed processing, or what is the percentage of the population affected?
All Victims, Witnesses, Suspects and Accused that have either submitted, or are the subject of, digital evidence to the criminal justice process. Other individuals may also be captured in the digital evidence. The total number of crimes recorded across Scotland (Scottish Government recorded crime document 2021/2022, published 28/06/22) was 305,851. This figure includes crime groups 1-7. This is equivalent to 5.7% of the population based on the Scottish population (2011 Scottish census). The DESC pilot will be limited to the Dundee City area for a period of 6 months initially, therefore the number of individuals affected by it will be limited in number. For the period 2021/2022, the total recorded crime figure for Dundee City was 12,004. Not every crime or incident recorded will have associated digital evidence. Third parties who provide supporting information or services, including expert Witnesses, forensic specialists, doctors, social workers, and other health and social care professionals, Police Officers and Staff working in criminal justice organisations, including but not limited to Prosecutors; Criminal Defence Solicitors and the Judiciary will also have limited data captured whist working in their professional role directly related to a case which has relevant data processed on DESC
1.4.10 What is the geographical area involved? (e.g. one division, a number of divisions, whole of Scotland. If this is not to cover the whole of Scotland, name the areas involved)
For the DESC Delivery 1 Pilot, processing will be limited to the Dundee City area for a period of 6 months initially, therefore the processing is limited in its geography. It is proposed that a future rollout will eventually cover all of Scotland

Part 1, Section 5 – Context of the Processing – The wider picture including internal and external factors which might affect expectations or impact

1.5.1 Are there prior concerns internally over this type of proposed processing, or known security flaws?
☒ Yes – provide details below. This must be addressed in the risk assessment ☐ No

Whilst Evidence.Com is used in the Criminal Justice system in England & Wales, the use of large scale, cross-partner cloud based processing introduces areas of risk that require full assessment to ensure that appropriate security measures are in place to protect data subjects.

The use of the DESC solution introduces certain overseas processing, in particular in the USA due to the nature of the Cloud solution and identified supplier. Key concerns have been identified and each partner has independently sought external legal advice. The ICO has also been engaged and provided advice on an informal manner (i.e. not under the DPA18 s65 powers) both verbally on 07/12/22 and in summary, however a detailed written response is awaited on the following matters:

1. The impact of the US Cloud Act
   Certain Data Processors for DESC fall under the jurisdiction of the US Cloud Act, which in principle gives a legal gateway for the US Government to compel certain Data Processors to provide evidence (Content Data) to it, without the knowledge of the Data Controllers or the contracting authority. It is assessed that were this to happen, this would have an adverse impact on a data subject's rights.

   There is current and ongoing engagement between US law enforcement authorities and Scottish counterparts though regular and routine governance channels when a case arises that may result in a formal request for information or evidence to be provided. Therefore, because formal channels exist to request information and/or evidence and are currently used, it is unlikely that such an obligation will be imposed on the Data Processors in all but exceptional circumstances.

   DESC Partners have imposed obligations on Axon and by default, it's sub-procesors, to inform the Data Controllers when requests are made, but understand that in certain circumstances they may not be permitted to do so as a consequence of the US Cloud Act. Therefore, available mitigations are limited. Consequently, this risk has been considered by the DPOs and by the Senior Information Risk Owners (SIROs) of each of the Data Controllers.

2. Clarification of whether processing includes data in transit
   The Data Controllers understand that data in transit is not considered a transfer under Data Protection legislation. This has influenced the application of proportionate security measures to protect data and also reassure data subjects.

3. The impact of the main supplier (Axon) using sub-processors, in particular Microsoft, and relying on terms and conditions drafted for GDPR compliance only, whilst the processing of evidence (Content Data) on DESC is primarily governed by the DPA18. This matter has been investigated and the Data Controllers have worked with the supplier to identify and implement resolution pathways which include:
   - Processing 'Content' Data within the UK.
   - Understanding the role of all sub-processors in the DESC solution
   - Undertaking due diligence on all sub-processors to ensure contractual terms are properly reflected either with Axon or directly with the Data Controllers. Axon has supplied SCC (standard contractual clauses) for its sub-processors which have been reviewed by the Data Controllers. Whilst a resolution pathway has been identified for Sub-Processors, it is not expected to be in place for all Sub-Processors before the Delivery 1 Pilot Go-Live and therefore this is a risk to be considered by the DPOs and SIROs for each of the Data Controllers involved in that delivery phase.
4. The essential requirement for the supplier to have access to Content Data to deal with emergency situations that may jeopardise the software/platform. Axon has confirmed that technical support will be provided by a UK-based and vetted team.


Scotland DESC Go Live Support - 110123


Security Commitment 110123

It is anticipated that in most cases DESC partners will only ever use the UK support line to notify Axon of issues, however to maintain the routing capability 24/7 there could be the occasion an initial call is logged with Axon Globally for triage purposes only. Axon will only gather information on the fault for the correct allocation to the UK support engineers, all with the correct clearance to manage.

Axon cannot control what the customer says in the support call, but there should be no need to include Content Data information within these calls. Calls to Axon to discuss technical matters will be limited to the DESC Project team and in DESC partners' ICT specialists.

5. Bring Your Own Key (BYOK) is not possible within the existing Axon evidence.com solution
6. SPA is a competent authority for processing under DPA18 s30(1)(b)

The SIROs for PSoS, COPFS and SCTS have reviewed and accepted the risks prior to Deliery 1 Pilot, whilst SPA, which will not be processing data in the Delivery 1 Pilot will consider the matters further ahead of any processing it undertakes on DESC.

1.5.2 Describe any relevant advances in technology or security

N/A

1.5.3 Are there any current issues of public concern in the area of the proposed processing? If so, provide details.

☒ Yes – provide details below. This must be addressed in the risk assessment.

☐ No

The matters raised at 1.5.1 are in the public domain, particularly in special interest and professional (security, data protection etc) forums in general terms for overseas processing, not specifically in relation to DESC, however Axon has been mentioned.

Consequently it is important that the partners, as Data Controllers address these matters as failure to do so may cause public concern and/or confusion.

1.5.4 What relevant codes of practice have been considered and complied with?

Scottish Biometrics Commissioner's Code of Practice

For DESC Data Protection Working Group use only:

1. **Is the proposed processing of personal data (Content Data) for Law Enforcement purposes likely to result in a high risk to the rights and freedoms of the data subject?**

   ☒ Yes – Provide the rationale for your decision below

   ☐ No – Provide the rationale for your decision below

2. **Is the proposed processing of personal data (Non-Content data) for UK-GDPR purposes likely to result in a high risk to the rights and freedoms of the data subject?**

   ☐ Yes – Provide the rationale for your decision below

☒ No – Provide the rationale for your decision below

Rationale for decision:

1. Content Data

   This is large scale processing of sensitive personal data associated with the end-to-end criminal justice process across all of Scotland, albeit the Delivery 1 Pilot is limited in both scope and scale and a phased future rollout is planned.

   Consequently it is essential that the processing is undertaken in a secure manner that protects data subjects' rights and supports their right to justice / a fair trial by protecting the confidentiality, integrity and availability of digital evidence.

   The processing involves complex partnership and contractual arrangements and a third party supplier, imlementing new technology and consideration of data sovereignty issues.

   Consequently, the partners, as Data Controllers consider that processing of Content Data is high risk processing for which there are high risks that must be mitigated and a full DPIA is required.

2. Non-Content Data

   This is processing of limited personal data of Officers and staff for limited purposes which is in line with their operational activities and employment. Whilst it involves large numbers of individuals, it is limited to their working life only and the purpose for processing (to logon to a system to undertake a task) is the same as multiple other ICT platforms and systems used in the course of their working day.

   The Data Controllers have addressed in detail and in a DPA and other project documentation the purpose, use and governance of the Non-Content Data and have taken steps to design data protection principles into its processing.

   Consequently, the partners, as Data Controllers consider that processing of Non-Content Data is not high risk processing for which there are high risks that must be mitigated.

DPIA Part 2 – Assessment of legality, governance and risks

Name of Project: Digital Evidence Sharing Capability (DESC)

URN: PSoS 22-389

Part 2, Section 1 – Assessment of Necessity and Proportionality – The Data Protection Principles and other relevant sections of the Data Protection Act 2018 (DPA 2018) and UK-GDPR

1st Principle – Lawful and fair and transparent.

2.1.1A Is the processing based on consent?
☐ Yes ☒ No

2.1.1B Define your legal and lawful basis for processing. Please list any legislation specific to the proposed processing below
Appendix 2 contains details of the underpinning legislation or powers on which the processing is based for both Non-Content and Content Data. Each Data Controller has defined its legislative powers for the processing of data on DESC. Non-Content Data means the data processed by DESC for general contract management purposes and in accordance with the UK-GDPR, comprising limited personal data to facilitate user authentication, logon, permission management, platform performance management, maintenance and auditing. Non Content Data is processed under UK-GDPR Content Data means the Personal Data processed by DESC by a competent authority (as defined in the Data Protection Act 2018 section 30 (1)(a) and Schedule 7 or section 30(1)(b)) for law enforcement purposes in accordance with Part 3 of the Data Protection Act 2018 (“law enforcement processing”). Content Data is processed under Data Protection Act 2018 part 3 **Non-Content Data** 1. SG – UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest 2. SPA – UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely Police and Fire Reform (Scotland) Act s31 3. PSoS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely, Police and Fire Reform (Scotland) Act s17 & 20 4. COPFS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely the administration of justice 5. SCTS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely the administration of justice **Content Data** 1. SPA ▪ DPA2018 s35(2)(b) by a Competent Authority (s30(1)(b)) and s35(5) and Schedule 8 (1) ▪ Police and Fire Reform (Scotland) Act s31 which obligates the SPA to provide forensic services ▪ Criminal Procedure (Scotland) Act 1995 which places a statutory duty on SPA ro provide evidence to the Crown

2. PSoS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (1)
   - Police and Fire Reform (Scotland) Act s17 and s20 which place a statutory responsibilty on the Chief Constable for the administration of day-to-day policing and continuous improvement, to comly with lawful instructions from COPFS and which place statutory duties on Constables to make reports to the COPFS
   - Criminal Procedure (Scotland) Act 1995 which places a statutory duty on PSoS to provide evidence to the Crown
   - Criminal Justice and Licensing (Scotland) Act 2010, sections 117-120 places a statutory duty on PSoS to provide the prosecutor, after the first appearance of an accused, with details of all the information that may be relevant to the case, obtained during their investigation. Police Scotland also have an ongoing commitment to provide any further relevant information which is obtained.

3. COPFS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (1 & 2)
   - Criminal Procedure (Scotland) Act 1995 which places a statutory and common law duty to adduce evidence during trials to constitute a sufficiency of evidence
   - Criminal Justice and Licensing (Scotland) Act 2010 s121-123 which places a statutory and common law duty on the Crown to disclose evidence to the Defence
   - Statutory duty on COPFS to lodge evidence within time limits for Solemn cases (Criminal Procedure (Scotland) Act 1995 s68(2)

4. SCTS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (8)(1), (2) & (7)
   - Criminal Procedure (Scotland) Act, 1995
   - Judiciary and Court (Scotland) Act, 2008, section 61-62

2.1.2 Does the processing involve the processing of sensitive data? Tick all that applies

☒ Race	☒ Trade Union membership
☒ Ethnic origin	☒ Genetic data
☒ Political opinions	☒ Biometric data
☒ Sex Life	☒ Sexual orientation
☒ Religion	☒ Health
☒ Philosophical beliefs	☐ None – go to question 2.1.4 below

2.1.3 To process sensitive data for a law enforcement purpose at least one of the following (or another Schedule 8 condition not listed below) must be satisfied. The Schedule 8 conditions must be read in full before completing this question. Check all that apply and provide further details below as to why each applies. Schedule 8 of DPA 2018

☐ The individual has given consent to the processing

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 for the administration of justice

☐ is necessary to protect the vital interests of an individual

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

☐ relates to personal data manifestly made public by the data subject

☒ Other Schedule 8 condition – Provide details below

The Data Controllers for 'Content Data' are competent authorities for the processing of law enforcement data.

- PSoS, COPFS and SCTS are competent authorities as defined by Data Protection Act 2018 s30(1)(a) and Schedule 7.
- SPA is a competent authority as defined in the Data Protection Act 2018 s30(1)(b) and its statutory duty defined in the Police and Fire Reform (Scotland) Act s31

Appendix 2 provides a diagramatic overview of the functions conferred on the controllers by an enactment/rule of law and necessary for reasons of substantial public interest

COPFS and SCTS must process the data for the administration of justice

In certain cases, the processing will be necessary to safeguard children and/or individuals at risk by ensuring criminal cases are investigated and the criminal justice process followed.

SCTS must also process the data for judicial acts

All Data Controllers have an Appropriate Policy Document in place

2nd Principle – Specified, Explicit and Legitimate – DPA Section 36

2.1.4 Is the personal data to be used for the purpose for which it was first gathered?
☒ Yes ☐ No – State below the purpose for which it was gathered, and the new purpose
Click here to enter text

3rd Principle – Adequate, Relevant and Not excessive – DPA Section 37

2.1.5 What assessment has been made to ensure that the personal data being processed is adequate, relevant and not excessive in relation to what is necessary for the purpose for which they are gathered?
DESC is not a 'public' portal where data can be uploaded in an unsolicited manner. Data can only be submitted by a member of the public after a crime or incident has been reported and a link sent by PSoS. Where Victims and Witnesses provide their data, Officers will provide advice prior to providing a link on what data is required following engagement with the individual. This may, in some instances, involve viewing the data if the Victim or Witness agrees. Whilst Victims/Witnesses will be requested to submit only the minimum amount of relevant data, they may provide more where they believe it is necessary, or they may not have the knowledge or resources to 'trim' the data before submitting to DESC. Where Victim, Witness, Suspect or Accused data is uploaded by PSoS, it will be limited to that which the Officer/Staff member considers may be relevant for the incident under investigation. PSoS will report to COPFS on DESC only that data that it is required to do by Criminal Porcedure Scotland Act 1995 and Disclosure rules When data is subsequently considered by COPFS, the Prosecutor will assess what is necessary and proportionate in terms of the criminal law to prosecute the case. "Engagement has been undertaken between Scottish Government, COPFS and the Judiciary to consider if non-relevant, non-exculpatory data submitted by a Victim/Witness in relation to summary cases could be deleted after submission without undermining the judicial process. This an area still to be fully progressed and there is no defined timescale for a decision and engagement will continue beyond the proposed pilot go-live date."

4th Principle – Accurate and kept up to date where necessary – DPA Section 38

2.1.6 How will the accuracy of data be checked?

Content data is provided as evidence during the investigation of a crime or incident. During the course of the PSoS criminal investigation and following PSoS procedures and statutory requirements, Officers will determine if the data is relevant to and should be provided to COPFS.

At point of triage, Officers who identify that a member of the public has supplied evidence that isn't connected to the case – for example if they have mistakenly uploaded an unrelated video clip rather than the video clip rather than the one connected to the incident - can 'Decline' the digital evidence and it will be deleted from the system. An audit record will be mantained

If an Officer/Staff member identifies an error, for example evidence being associated with the wrong case number, they can amend it in the instance of DESC in which they are working. In addition, Case Management staff in PSoS have a number of business process steps to check accuracy prior the evidence being shared and that will be improved through integration.

If a mistake is identified after data has been shared, DESC Project has a created process showing how the Lead Agency Tracking Number can be updated and how errors in submissions from PSoS to COPFS are amended.


Incorrect LATN.pdf


Incorrect Evidence Shared in Bundle V2

COPFS is dependent on Police Scotland and SPA in the first instance to ensure the accuracy of the material shared to it. Any inaccuracies identified thereafter will be assessed and rectified on a case-by-case basis. If COPFS discover an error, it will relay information back to the reporting officer through pre-existing channels (Fiscals Memo or SFI) and it is the responsibility for the reporting officer to correct the error. This is the method already in place and replicates many of the PSOS and COPFS partnership processes. Automation through integration may be looked at in the future, for example notification a case is complete etc. but at this time it is manual using pre-existing business processes.

2.1.7 What process will be in place to keep it up to date where necessary?

If a mistake is identified after data has been shared, DESC Project has created process maps for the Lead Agency Tracking Number to be updated. These are included in 2.1.6

Any inaccuracies identified will be assessed and rectified on a case-by-case basis. If COPFS discover an error, it will relay information back to the reporting officer through pre-existing channels (Fiscals Memo or SFI) and it is the responsibility for the reporting officer to correct the error. This is the method already in place and replicates many of the PSOS and COPFS partnership processes. Automation through integration may be looked at in the future, for example notification a case is complete etc. but at this time it is manual using pre-existing business processes

2.1.8 There must be a functionality or procedure to distinguish between fact and opinion. How will you ensure that this is done? If this cannot be done, please explain why.

Fact - Data (digital evidence) is identified though criminal investigation. Digital evidence will be uploaded in its native format. The DESC processes are based around users ingesting digital files and not opinions

Opinion - DESC has the capability to include notes and bookmarks for clipping evidence. Entries via free text into notes will be part of DESC training.

2.1.9 How will you ensure that there will be a clear distinction between personal data relating to different categories of data subjects? (e.g. Victims, Witnesses, Accused etc.) If this cannot be done, please explain why

For Delivery 1 Pilot, Data ingested into DESC will be allocated a unique Production Reference number (provided by PSoS National Production system) and will be held within a case folder on Evidence.com, which when shared with COPFS, will cross refer with the National CASE Lead Agency Tracker Reference Number (SPR). SPA will not upload Data to DESC during Delivery 1 Pilot No status is given to a person supplying the data. PSoS will accept digital evidence pertaining to a case from any person that has been offered the link, provided the evidence or who has had digital evidence seized. All victims, witnesses, suspects and accused from whom digital evidence is held are recorded as 'citizens' on DESC and they are not attributed a status. There is no functionality to differentiate. During an investigation process, the status of a data subject who provides or is captured in digital evidence may change. For example, through the investigatory process and assessment of all available evidence, including but not limited to digital evidence, a Witness may become an Accused, or a Suspect may become a Witness. On DESC, as all data subjects from whom the ditigal evidence is obtained are recorded as 'citizens', status will not change. The status of individuals during the course of an investigation will continue to be recorded on associated systems, including but not limited to COS Unifi, Case Management.
2.1.10 What steps will be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes? DPA Section 38(4) and (5) refers
At each stage of the criminal justice process, outlined in s1.1.4, partners will assess the evidence submitted or held on DESC for relevance to the criminal justice process. Data that is not deemed relevant will not be shared by PSOS to the COPFS instrance of DESC. COPFS will not use Data that it does not deem relevant in criminal proceedings,but will make all disclosures to defence agents required by law. Access to Data on DESC is limited by role based access and used only for the case that it is submitted in relation to.

5th Principle – Not kept longer than necessary – DPA Section 39

2.1.11 How long will the personal data be retained?
DESC partners have convened a Records Management working group to define the retention period for the data, taking into account the nature of the criminal justice process, rights of appeal, impact on data subjects and the responsibilities and role of the Lord Advocate in determining the retention of evidence submitted, both relevant and non-relevant. During the period of the Delivery 1 Pilot, all data will be retained. E-mail invites to members of the public will be routed via Axon Citizen and deleted thereafter. A defect has been identified that means the data is not being systemically deleted at this time. Axon has identified a technical resolution, however the lead-in time for testing and implementation is c.8 weeks and it will not be ready at point of Delivery Stage 1 Pilot. DESC Project will continue to engage with Axon and implementation will proceed as soon as the functionality is ready to correct the defect. This will remediate all contact data held.
2.1.12 The system must be able to weed and delete a) individual records and b) bulk records. How will you ensure that this can be done? (e.g. manual intervention, automatic deletion etc.)

a) At point of ingestion, Officers will review digital submissions as part of the triage process. An Officer can elect to Accept or Decline the digital evidence provided. This allows for very obvious errors made during a submission to be deleted, e.g. the person submitting the evidence providing the wrong digital evidence by mistake.

Each partner's instance of DESC is 'stand alone'. Therefore, no partner can delete data from another partner's instance and a deletion by COPFS for example will not automatically update PSoS. If there is a need to delete data once shared from one partner to another (for example shared by PSoS to COPFS), the partners will be informed via a Subject Report which is sent via National Case under the Lead Agency Reference Number, which is the same process documented in 2.1.6 above. This means that each partner must have in place relevant processes to authorise deletion, based on the technology available.

Deletion capability is controlled by RBAC. This means not every person that has a logon to DESC and can access data will have the permissions to delete it. If digital evidence has been accepted and subsequently requires to be deleted, in PSoS, a 3-tier authorisation process will be applied.

1. Officer emails supervisor requesting deletion of defined data/digital evidence and providing a rationale.
2. Supervisory Officer reviews data/digital evidence. If supported, Supervisory Officer makes a request in writing to Inspector
3. Inspector reviews data/digital evidence. If supported, Inspector documents the rationale on DESC and deletes the data/digital evidence, this process includes the provision and application of a verification code by the authoriser. The data/digital evidence will be held queued for deletion for a period of 7 days before permanent deletion.
4. An audit trail of these actions will remain on DESC

b) During the Delivery Stage 1 Pilot, as defined in 2.1.11 above, data will not be systemically weeded. Any and all weeding/deletion required during pilot phase will be carried out using the processes and method defined in 2.1.12(a). Consequently, there is assurace that digital evidence and associated data can be deleted from DESC when required.

Beyong Delivery Stage 1 Pilot, Axon Evidence.com provides the functionality to manage retention and deletion through both automated and manual processes. Axon is contractually obliged to ensure that data is securely destroyed or deleted in line with Retention Rules and any additional requests from the Data Controllers.

DESC Project is planning to have the functionality to perform automated weeding of digital evidence and associated certification and data stored in DESC. This may involve integrations with other system(s) including but noyt limited to PSoS UNIFI Productions to automate the process.

The design of this functionality will be subject to further DPIA updates prior to being implemented.

Refer to 2.1.11 for details of Axon Citizen

2.1.13 If the data is to be retained after the retention period, e.g. for statistical purposes, how will it be anonymised?

There are no documented plans to retain DESC metadata for statistical or data science purposes beyong its retention period (based on primary operational value) at this time.

As noted in 2.1.11, the DESC Records Management Group in conjunction with the DESC Programme is defining retention periods for all DESC data including audit logs. If during that discussion a secondary value for anonymised or pseudonymised metadata is identified, further DPIA updates will be undertaken prior to implementation

2.1.14 What processes will be in place to ensure the data is securely destroyed / deleted?
DESC Stage 1 delivery will not involve the systemic deletion of personal data, however if individual Content Data is deleted during pilot, for example as a result of a data subjects rights request, or an officer declining submitted data (as detailed earlier in this DPIA), the data is placed in a deletion queue for a period of 7 days. This allows for any deletion errors to be remediated and data restored. At the end of the 7 day period the data is permanently deleted and cannot be restored. The same functionality will apply to systemic deletion in future. The technical security of the deletion process has been reviewed by ISO

6th Principle – Security / Security of processing – DPA Sections 40 and 66 – Technical or organisational measures in place to ensure protection of the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage and obligations relating to security, respectively.

2.1.16 If in Part 1 you stated that you had not consulted with the Information Security Manager (ISM) has this now been done?
☐ Yes – and advice received ☐ No – explain below why this has not yet been done ☒ Not applicable
Click here to enter text
2.1.17 On which risk register will the information be recorded? If it is already on a risk register, please state which.
For the Stage 1 Delivery Pilot, risks will be recorded on the DESC Partnership Risk and Issue Register. As Delivery progresses through the stages defined in 1.1.4 and into business-as-usual, any residual risks will be assessed and transitioned to the appropriate Data controller(s) and their risk register(s). This will be updated in future DPIA updates.
2.1.18 What processes will be in place to determine who will have access to the data / system and how is it done?
Role Based Access Control (RBAC) functionality will be used to manage and limit what individuals have access to and can do. Roles, groups and permissions are designed around partner-specific requirements. Each Data Controller has created a number of User Stories that set out how the roles, groups and permissions align to meet business and user requirements. Each User Role's permissions are depicted within process maps and spreadsheets to ensure that Roles are linked to RBAC. Any changes in Roles will be controlled by an Administation Role which is limited in numbers of individuals. For the purposes of the Delivery 1 Pilot: <u>SG</u> SG staff have responsibility for contract management, but will not have or be given logon capability to the DESC solution as it is not required for any purpose. <u>SPA/PSoS</u>

Administrative users will grant and remove access to the DESC solution via the SCoPE interface. Changes will then automatically propagate the RBAC solution into DESC. In instances where access needs to be removed immediately, administrative users will be able to disable user accounts within the DESC solution to avoid the slight delay in the full automated pipeline.

The DESC solution will be integrated with the PSoS Azure Active Directory (AD), which will be informed by the internal PSoS/SPA HR Management system known as SCoPE. Users will be assigned a role within SCoPE which will in turn determine their AD group membership. Permissions will then be based off of the AD group and propagate through to the associated user account in the DESC solution.

COPFS

COPFS staff will have access to SPRs and DESC Content Data based on a business need and role specific basis to enable them to access evidence within DESC. IT engineers within COPFS will grant and remove access to DESC solution via the on-premise Active Directory Azure access management policy. IT engineers will be able to immediately disable accounts within DESC to avoid the slight delay in the fully automated pipeline. Approved DESC users will manage and control access to evidence within DESC considered sensitive by COPFS

Axon as Data Processors

Axon has assured that it has RBAC processes in place to limit processing of content data to its UK based and vetted staff. ISO group are continuing to engage with Axon.

2.1.20 What level of security clearance (i.e. vetting level) will be required to access the system?

NPPV3

Axon has confirmed in writing that only UK-based and vetted staff will be able to process (access) Content Data for the purposes of providing technical support in authorised scenarios or in the event of catastrophic system failure where immediate action is required.

2.1.21 What data protection / security training will users, processors, external contractors etc. receive, before gaining access to the system?

All partners as Data Controllers are responsible for the delivery of adequate data protection / security training to their Officers/Staff (including contractors) prior to the use of DESC and on an ongoing basis thereafter. Partners will commit to the delivery of appropriate training through the Joint Controller Agreement (JCA)

As a Data Processor, Axon is contractually obliged (Services Contract Reference 388514, s13.6) to provide adequate data protection / security training to their staff prior to their use of DESC and on an ongoing basis thereafter. It is also the responsibility of Axon to ensure that sub-processors have completed training which is commensurate to their contractual requirements. DESC partners as Data Controllers are undertaking due diligence checks with Axon of its sub-processors to ensure that appropriate terms and conditions are in place.

PSoS as Delivery Lead will co-ordinate the monitoring of Axon compliance and partners will collaborate where it is appropriate to do so.

2.1.22 Confirm you will you have a SyOps / procedure manual / SOP etc. to detail the above?

☒ Yes – state below which of the above.

☐ No – state below, why not.

For Delivery 1 Pilot

- DESC Guidance Document (to support the training)
- Systems Operations form
- IT Handover documentation
- Videos
- ICT Helpdesk
- Floorwalkers
- PSoS Divisional champions
- PSoS Opertional Order

2.1.23 What technical controls will be put in place to protect data at rest, from compromise? Check all that apply.

☒ Encryption	☒ Role Based Access Control

2.1.24 How will information be protected in transit?

☐ Secure email	☒ Encryption
☐ Egress	☐ Other – Provide details below

Data in transit within the Police Scotland Network and Data Centres will be secured by:

GCM-AES-128 encryption

TLS 1.2 implementation with 256 bit connection, RSA 2048 bit key, Perfect Forward Secrecy

Data in transit to the cloud-hosted DESC solution will be secured by:

FIPS 140-2 validated: Axon Cryptographic Module (cert #2878)

TLS 1.2 implementation with 256 bit connection, RSA 2048 bit key, Perfect Forward Secrecy

2.1.25 Explain how loss of data at rest, will be prevented in case of a business continuity incident / disaster recovery. (e.g. Business Continuity Plans, backups and frequency, resilience, parallel systems etc.)

Axon is contracted to provide a fully resilient solution, with agreed Business Continuity Plans and Disaster Recovery plans.

In the event of a major disaster that results in a full loss of a Microsoft Azure region, Axon has created the Axon Evidence Information System Contingency Plan (ISCP). The ISCP focuses on the recovery of Axon Evidence to a secondary Microsoft Azure region. Axon is confident, that in the event of the complete destruction of a primary Microsoft Azure region, Axon Evidence can be recovered and restored in the secondary Microsoft Azure region within, at most, a 24-hour window.

Axon states that its BCP and ISCP programme is designed in alignment with and complies with NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide where applicable. Axon states it tests its contingency plans, backups, and operations on at least an annual basis, with test results stored internally within the Axon ISCP. Engagement with Axon on detailing this is ongoing.

AWS backup is expected to be similar to Microsoft Azure but this needs to be explored in greater detail.

Part 2, Section 2 – Information Sharing

2.2.1 Is any of the data being processed to be shared with third parties? (i.e. outwith the partners)

☒ Yes – state below which 3rd parties.

☐ No – go to question 2.3.1.

COPFS will share relevant Content Data with Defence Agents as required by the Criminal Procedure (Scotland) Act 1995 which places a statutory and common law duty on the Crown to disclose evidence to the Defence. This may be done on DESC with limited Defence Agents, and also using existing and separate processes.

Certain data will also be played in court as part of the trial process using DESC, at which the public may attend.

2.2.2 If the information is to be shared with third parties, are there Information Sharing Agreements (ISAs) already in place with these third parties?

☐ Yes – agreement(s) in place – Give details below

☐ Not yet – agreement(s) required

☒ No – none required. If not required, state the reason.

It is a statutory requirement for COPFS to disclose certain data to defence agents as part of the criminal justice process and to ensure a fair trial. This is not subject to ISAs but is subject to defined procedures within COPFS

COPFS must present relevant Data during a trial, in public and under the direction of the Judiciary. Consequently this is not subject to ISAs, but is subject to defined procedures within COPFS

Part 2, Section 3 – Measures Contributing to the Rights of the Data Subjects

Subject Access Requests (SARs) – DPA Section 45

2.3.1 How will you ensure that the personal data will be available for the processing of SARs?
During the Delivery 1 Pilot Phase, the DESC Project will act as a SPOC for the staff in PSoS (Information Disclosure) and COPFS (TBC) to access the data and facilitate SARs. A scalable business-as-usual solution will be included on the DESC Project Action List. A Pilot Action Log of all the requirements to be taken forward into Pilot will be finalised primarily based on the "Caveats" in the Ready with Caveat status assessment of the x-partner Go No Go Tracker which has been updated to confirm that the actions, risk mitigations, agreed controls and monitoring throughout this DPIA, the JCA and DPA must be undertaken.

Right to rectification, erasure and restriction – DPA Section 46, 47, and 48

2.3.2 How will you ensure that the personal data can be corrected, deleted or the processing restricted if required, in response to an individual's rights request?
During the Delivery 1 Pilot Phase, the DESC Project will act as a SPOC for the staff in PSoS (Information Disclosure) and COPFS (TBC) to access the data and facilitate Data Subjects Rights Requests. As defined in s2.1.6 of this DPIA, there is practical functionality designed into the DESC solution that will allow the rectification of incorrect data. DESC functionality also allows for the erasure of individual data and restriction of processing. A Pilot Action Log of all the requirements to be taken forward into Pilot will be finalised primarily based on the "Caveats" in the Ready with Caveat status assessment of the x-partner Go No Go Tracker which has been updated to confirm that the actions, risk mitigations, agreed controls and monitoring throughout this DPIA, the JCA and DPA must be undertaken.

Part 2, Section 4 – Other legal requirements

Auditable Logging – DPA Section 62

2.4.1 The system must create an auditable record (or log) each time a user does any of the following to the personal data. Please confirm or otherwise that the proposed system will do this. This is a legal requirement. **If these requirements cannot be met before the system goes live, the system will not be accredited.**
a) Collection – the log must record • what data was collected / input • the identity of the individual who updated the system with the data • the date and time the system was updated ☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of the DPIA.**

The Axon Evidence Accreditation Statement "Axon state that logs that are sent to the Security Incident Event Management) SIEM tool for monitoring are initially recorded in UTC. Audit trails, which are customer facing audit records, on the other hand, are in the time designated by the customer for their Axon Evidence profile. Therefore, before relying on an audit trail, care must be taken to ensure that the log file times have been translated appropriately."
The SIEM system is the Axon system. PS have asked for access to this but the question is unresolved.

b) Alteration – the log must record:

- the data that was altered
- the identity of the individual who altered the data
- the date and time the data was altered

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

Within DESC, Evidence Audit File Logs will be used to track all 'access' and 'edit' history for evidence files and case folders, including associated metadata. Therefore, any changes made to a file or its metadata (e.g. reassigning an evidential file, renaming evidence, redactions and deletions) will be logged in the Evidence Audit Log. This log entry will contain the date and time of the change, the user who performed the change, the type of change and the users client IP address.

c) Consultation (accessing / viewing) – the log must record

- what data was consulted
- the reason for the consultation
- the identity of the person who consulted it
- the date and time of the consultation

☐ Yes – the system will record an auditable record of all of the above

☒ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

All access to evidential data within DESC will be tracked within the Evidence Audit File Logs which will detail the date, time, user ID and client IP address for whenever a user accesses evidential data. The justification is not recorded in DESC in every instance but can either be inferred or identified from the sequence of user activity recorded in DESC, for example the viewing of evidence by a Police Officer and the immediate next action of sharing to COPFS, or the justifications captured in related case records or procedural manuals.

d) Disclosure (including transfers) – the log must record:

- the information that was disclosed
- the reason for the disclosure

- the date and time of the disclosure
- the identity of the person who made the disclosure
- the identity of the recipients of the data

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

These will be automatically recorded in the User audit system log files.

e) Combining with other data – the log must record:

- the data which was combined
- the identity of the individual who combined the data
- the date and time of the combination

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

The DESC solution requires technical integrations with the PSoS DEPP COS UNIFI solution in order to maintain a consistent set of production and crime data across the DESC and DEPP COS programmes. Evidential data will be uploaded into the DESC solution and will be linked to the associated incident using the STORM ID. Related pieces of evidential data in DESC will be collated in DESC in order for a case. Once a case is ready to be created within the DESC solution, it will be created with the Crime Record (CR) Number as the Case ID. The DESC solution will then make an API call to DEPP COS UNIFI to create a Production record within UNIFI linked with the CR Number. Once the production record within UNIFI has been created, UNIFI will return a Production Number back to the DESC solution, again via an API call. This will assure a consistent record of linked cases and productions across all integrated systems.

The creation of evidence, evidence bundles and cases will be tracked in the aforementioned Evidence Audit File Logs and the creation of Production records within UNIFI via API calls will be tracked in UNIFI audit logs.

f) Erasure / weeding – the log must record:

- the fact that a specific record was accessed
- that data was erased/weeded
- the identity of the individual who erased/weeded the record
- the date and time of the erasure/weeding

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

These will be automatically recorded in the User audit system log files.

Data transfers outwith the UK – DPA Sections 72 to 78 (Refer to Guidance Note 2 of the Part 2 Guidance Notes)

2.4.2 Will the data be held in or transferred to a country within the EU but outwith the UK?
☐ Yes – state below which country / countries below ☒ No – go to question 2.4.5
Click here to enter text
2.4.3 For what purpose is the data held in / transferred to the country / countries listed above? Include the legislation which governs the transfer of the data.
Click here to enter text
2.4.4 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Click here to enter text
2.4.5 Will the data be held in or transferred to a country outwith the UK and the EU?
☒ Yes – state below which country / countries below ☐ No – go to question 2.5.1
Non-Content data will be transferred to the USA For clarity, Content data will not be processed outwith the UK
2.4.6 For what purpose is the data held in / transferred to the country / countries listed above? Include the legislation which governs the transfer of the data.
Non-Content data will be transferred to the USA for the purposes of user access authentication to facilitate logon to DESC

2.4.7 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Non Content Data will be protected by the following: ▪ Contractual obligations on the supplier and its sub-processors. These are further defined in the Data Processing Agreements. ▪ Limitations on the retention of contact data ▪ Technical security controls agreed by the DESC ISO Gropu and documented in the Security Control Sheet For clarity, prior to Delivery 1 Pilot, the Data Controllers required the supplier to implement a closed loop support process to bring all technical support for Content Data into the UK.

Part 2, Section 5 – Other privacy legislation

2.5.1. Does the project involve the use of powers within any of the following? Check box as appropriate
☐ RIPA 2000
☐ RIP(S)A 2000
☐ IPA 2016
☒ None of the above

2.5.2 If any of the above apply, provide the relevant sections of the legislation
Whilst it is possible, in principle, for Content Data (evidence) gathered as a consequence of the use of the powers defined in 2.5.1 to be processed on DESC, for the Delivery 1 Pilot DESC will not be used as the storage or transfer mechanism between criminal justice partners and existing processes will be used. It is likely that a future assessment will be made on use of DESC for processing of evidence derived form these sources, however the sensitivity and risk associated with them will need to be taken into consideration in that assessment.

Human Rights Act 1998

2.5.3 Article 2 – Right to Life **Does the proposed process involve new or existing data processing that adversely impacts on an individual's right to life?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below
☒ No
Click here to enter text

2.5.4 Article 3 – Prohibition of torture **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be subjected to torture or inhuman or degrading treatment or punishment?** Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.5 Article 4 – Prohibition of slavery and forced labour
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be held in slavery or servitude or required to perform forced or compulsory labour. Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.6 Article 5 – Right to liberty and security
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to liberty and security? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.7 Article 6 – Right to a fair trial
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to a fair trial? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.8 Article 7 – Right to no punishment without law
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be held guilty of a criminal offence which did not constitute a criminal offence at the time was committed? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.9 Article 8 – Right to respect for private and family life

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to respect for his private and family life, his home and his correspondence? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

The Processors for DESC fall under the jurisdiction of the US Cloud Act, which in principle gives a legal gateway for evidence (Content Data) to be provided to the US Government without the knowledge of the Data Controllers of contracting authority. It is assessed that were this to happen, this would have an adverse impact on a data subject's right to respect private life, however there is engagement between law enforcement authorities though regular and routine governance channels when a case arises that may result in a request for information or evidence from DESC partners to be provided. Therefore it is assessed that it is unlikely that such an obligation will be imposed on the Data Processors.

This matter has been subject to review and external legal advice sought independently by all DESC partners. In addition, there has been engagement with and advice sought and received from ICO on the matter.

2.5.10 Article 9 – Right to freedom of thought, conscience and religion

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of thought, conscience and religion? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.11 Article 10 – Right to freedom of expression

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of expression? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.12 Article 11 – Right to freedom of assembly and association

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of peaceful assembly and to freedom of association with others? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below ☒ No
Click here to enter text
2.5.13 Article 12 – Right to marry **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to marry and found a family?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below ☒ No
Click here to enter text
2.5.14 Article 14 – Right to freedom of discrimination **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of discrimination on any grounds?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below ☒ No
Click here to enter text

Consultation Process with Relevant Stakeholders

2.6.1 Do you intend to consult others either internally (e.g. business areas, staff associations, TUs etc. other information experts) or externally on the proposed processing?

☒ Yes

☐ No – If you do not intend to consult anyone, you must **justify** why consultation is not appropriate.

2.6.2 Who do you propose to consult on the proposed processing? List both internal and external organisations / individuals.

- Scottish Government
- Scottish Biometrics Commissioner
- Information Commissioner's Office
- Scottish Police Federation
- Association of Police Superintendents
- Unison
- Criminal Justice Partners
- COPFS Policy Division
- Defence Community, including Law Society of Scotland
- PCS/FDA Union
- COPFS Cyber security

2.6.3 When do you propose to consult with the above organisations / individuals?

- Scottish Government – ongoing basis throughout DESC delivery
- Scottish Biometrics Commissioner – November 2022
- Information Commissioner's Office – September 2022 and ongoing as required
- Scottish Police Federation – ongoing basis throughout DESC delivery
- Association of Police Superintendents – ongoing basis throughout DESC delivery
- Unison – ongoing basis throughout DESC delivery
- Defence Community including Law Society of Scotland –ongoing since start of 2022. COPFS to host presentations and feedback sessions in December 2022.
- PCS/FDA Union – ongoing and specifically in December 2022

2.6.4 How do you intend to consult with the above organisations / individuals?

SG and staff associations are represented at DESC Programme and Project Boards and are engaged throughout the delivery on specific matters.

A formal presentation to the Scottish Biometrics Commissioner's Advisory Board will be provided, consultation will continue according to questions arising thereafter

ICO has been engaged informally providing progress updates throughout DESC delivery. Advice has been sought on a specific matter in September 2022, through submission of a part of a DPIA, however this is not submitted using DPA18 s65

Part 2, Section 7 – Assessment and mitigation of risks posed by the proposed processing to the rights and freedoms of data subjects (Refer to Guidance Note 3 of the Part 2 Guidance Notes)

Risk(s) identified to the rights and freedoms of the data subject	**Probability and Impact Score and Risk Level**	**Mitigations**	**Probability and Impact Score and Risk Level after mitigations**	**Result:** The risk is: • Eliminated (E) • Reduced and Acceptable (R/A) • High/Very High and Acceptable (H/A)* • High / Very High and Not Acceptable (H/NA)*	**Evaluation:** Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
There is a risk that sub-processors engaged by the Supplier are not subject to the Terms & Conditions in Services Contract Reference 388514	Probability = 5 Impact = 5	▪ Due diligence assessment between DESC and Axon to review evidence form sub-processors and where sufficient authorise in writng. ▪ Engagement with Microsoft to discuss its terms and conditions to review compliance with DPA2018	Probability = 4 Impact = 5	H/A	The Data Controllers have escalated the risk to their SIROs and this has been accepted. Due diligence work will continue during Pilot to further reduce the probability scoring and in particular in relation to Microsoft and AWS where the support wider UK national organisations may be required.

		▪ Risk reviewed by the SIROs of each Data Controller			
There is a risk of the Submission, Processing and Retention of Non-Relevant Data	Probability = 3 Impact = 3	▪ Police Officers will provide advice to Members of the Public about what to submit. ▪ Police Officers can decline evidence submitted in error ▪ Each partner will review the Evidence and share only that Data considered relevant.	Probability = 1 Impact = 2	R/A	The mitigations allow data subjects, when submitting evidence, to limit processing to relevant data. Each stage of the processing sets out to reduce the impact on data subjects of processing of non-relevant data
Processing Law Enforcement Data using a Contractor and Sub-Processors which operate under the jurisdiction of the US Cloud Act	Probability = 1 Impact = 5	▪ Regular and routine engagement with US authorities on law enforcement matters ▪ Auditing by partners to identify activity (after the fact) ▪ Ongoing strategic engagement with ICO and Home Office to highlight impact	Probability = 1 Impact = 5	H/A	Law enforcement agencies routinely work together through formal channels, therefore whilst the likliehood of this legislation being applied to DESC data is low, the impact on data subjects remains high.

		▪ Risk reviewed by the SIROs of each Data Controller			
'Twilio' software is under assessment for future use to send DESC upload links to members of the public. It cannot be switched off for the pilot phase and there is a risk Officers will use it before it is approved	Probability = 5 Impact = 5	▪ Training provided to all Officers ahead of the pilot phase. ▪ Monitoring to check training is effective during pilot phase	Probability = 1 Impact = 5	R/A	The probability of this risk occurring has been mitigated through training and monitoring. Impact remains high because Twilio is not currently approved for use.
A scalable BAU solution for facilitating Data Subjects Rights requests has not been identified	Probability = 5 Impact = 3	An acceptable solution has been agreed for Delivery 1 Pilot The DESC Project will ensure a scalable solution is agreed before further rollout	Probability = 0 Impact = 3	Eliminated	The task is a managed activity for the DESC Programme, which will limit the probability of this risk occurring. Once in place this risk will be fully eliminated.
The BAU system administration, including ongoing monitoring and management of risk mitigations has not been identified	Probability = 5 Impact = 3	The DESC Project will ensure a scalable solution is agreed and implemented before closing the Project	Probability = 1 Impact = 1	Eliminated	The risk mitigation during pilot will ensure a scalable solution is in place prior to future rollout
There is a known defect which will not be resolved prior to Pilot, resulting in contact details for Data Subjects being held in Axon	Probability = 5 Impact = 3	A defect has been raised and Axon is working on a resolution with a timeline of c. 8 weeks.	Probability = 5 Impact = 1	R/A	The resolution timeline has already commenced and once implemented will fully eliminate the risk

Citizen longer than is necessary					
There is a risk that DP by Design will not be baked into future DESC development due to resourcing issues in the Project.	Probability = 5 Impact = 5	The matter has been raised DESC Programe Board to appropriately resource the work during Pilot.	Probability = 1 Impact = 1	R/A	The impact on individuals will be minimised as Data Controllers will be required to adequately resource the work of the DESC Pilot

Once Part 2 of the DPIA is complete it must be reviewed by the DESC DPWG and the DPOs of all 5 (five) Data Controllers to ensure the legal requirements are met. Once satisfied that all legal requirements have been met, they will sign it and return it to the project.

*If following mitigations, the risk to the rights and freedoms of individuals remains high, processing cannot commence without the agreement of the Information Commissioner.

Approval of DPIA

Name: [redacted] on behalf of the DESC Data Protection Working Group

Signature: [redacted]

Date: 19/01/2023

Comments / Observations: Approved subject to ongoing management of the noted controls and mitigations and risk action plans agreed with SIROs

Senior Responsible Officer: (Before signing – See Guidance Note 4 in Part 2 of the Guidance Notes)

Name:

Signature:

Date:

Comments / Observations:

Appendix 1a DESC Overview Presentation
Appendix 1b D Div DESC 1 Page
Appendix 2 Data Jointly Controlled – Linear flow

From: Dominique Mitchell [mailto:Dominique.Mitchell@ico.org.uk]
Sent: 20 January 2023 12:16
To: [redacted]
Cc: Jenny Brotchie <Jenny.Brotchie@ico.org.uk>; Kenneth Macdonald <Kenneth.Macdonald@ico.org.uk>; G Dersley <G.Dersley@ico.org.uk>
Subject: ICO to PS re DESC [OFFICIAL]

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Dear [redacted],

Thank you for the meeting regarding DESC yesterday, we appreciate you continuing to keep us updated. Below is a summary of points from the meeting, as we have understood them, do let us know if anything is incorrect. We have also included the advice we provided yesterday on compliance with section 37 DPA 2018 which you should consider before progressing with the pilot and action as appropriate. We also had a couple of questions/points that would be helpful if you could clarify – these are set out at the end of the email.

Summary of meeting

- The DESC pilot will being on 24th January 2022 in Dundee City. This will involve the processing of personal data.
- There will be no international transfers involved in the provision of technical support. Where it is necessary for technical support to have access to personal data in DESC this will take place in the UK only. Phone calls to indicate there is a technical issue may be routed through the US/another country – phone support in countries other than the UK will not however involve access to personal data.
- Police Scotland will be providing SRO with documentation, including a DPIA. This is not provided under s65 DPA 2018, ie you have assessed that here are no residual high risks that cannot be mitigated. The documentation is being supplied for our information. We will review the documentation and, if appropriate, provide feedback.

- You stated that you are assured as the controller that you are meeting all obligations under data protection law including those set out in S59, S64 and S66 of the DPA 2018.
- You informed us on the call that members of the public can upload information from their devices into DESC. It is not an open portal, access is only gained through a link which would be provided to the individual by an investigating officer. The link allows an individual to upload evidence they believe is relevant to the crime. The officer can then either accept or decline the information that is uploaded. If the officer views the information and sees is it obviously not relevant, ie holiday photos uploaded by mistake, the officer can decline. This is then put into a deletion queue for 7 days before being deleted. If the information viewed is relevant the officer can accept and the information is ingested into DESC. If, for example, a video is uploaded that is 20 minutes long but the relevant evidence is only 2 minutes, the officer can clip the information that will then be shared with other partners as the case progresses, however the other 18 minutes is retained.
- We discussed that it was likely that members of the public would upload irrelevant and relevant personal data via the link, including their own personal data and personal data relating to others some of which could be sensitive data. There is also a risk that if most of the information is relevant that officers would accept the submission. We advised that given the retention requirements set out in the Code of Practice made under Section 164 of the Criminal Justice and Licensing (Scotland) Act 2010 there is a risk of excessive processing and infringement of the data minimisation (s37 DPA 2018) principle. **You should review your DPIA and ensure that you can mitigate this risk and that put in place measures and mitigations to comply with the data minimisation principles (s37 DPA 2018)**
- As you will be aware if you have a remaining residual high risk in your DPIA that cannot be mitigated prior consultation with the ICO is required under Section 65 DPA 2018. You cannot go ahead with the processing until you have consulted us.
- If your assessment is that this risk can be reduced significantly to allow you to proceed with the processing the risk should be carefully monitored and assessed throughout the pilot.

Questions / points to clarify

1. Our understanding is that all material (even that considered 'manifestly irrelevant') is retained for the 'life of a case'. Once the case is completed all information is kept in line with the corresponding retention period which is dependent on the type of crime – and that's all evidence collected as part of an investigation. Can you let us know what is meant by the 'life of a

case' ? Does Police Scotland weed and then destroy irrelevant material/evidence after a case has closed?

2. Does the design of DESC allow for the deletion of information once it has been accepted by the investigating officer?

Regards,
Dominique

Dominique Mitchell (she/her)
Senior Policy Officer – Scotland

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

T. 0330 313 1715 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

Data Protection Impact Assessment:
Digital Evidence Sharing Capability (DESC) – Overarching DPIA

Law Enforcement Processing (content data)
UK GDPR Processing (non content data)

Control Sheet

URN (to be completed by Information Assurance)	22-389
Date Approved	
Version Number	V1.1
Document Status	In progress
Author	PSoS Information Manager (Assurance) on behalf of DESC Data Protection Working Group
Senior Responsible Owner (Project)	Andrew Hendry, PSoS Chief Digital and Information Officer on behalf of DESC
Transformation Project	Yes ☒ No ☐
Is this project a pilot?	Yes ☒ No ☐
Date on which the proposed processing is to start (if known)	24 January 2023

Revision History

Version	Date	Summary of Changes
V0.01	12/10/2022	Draft provided to DESC DPWG members
V0.02	28/10/2022	Draft provided to DESC DPWG members
V0.03	23/12/2022	Draft provided to DESC DPWG members
V0.04	17/01/2023	DESC Senior Project Manager reviewed and commented and draft provided to DESC DPWG members
V0.05	18/01/2023	Author updates
V1.0	19/01/2023	IA approval
V1.1	19/10/2023	Updates from pilot
V1.2	01/11/2023	IA review

Part 1 – Determining whether the proposed processing of personal data for law enforcement purposes is likely to result in a high risk to the rights and freedoms of the data subject.

Once completed, this part will be considered to decide whether the proposed processing is high risk.

Part 1, Section 1 – General

1.1.1 Does the project involve the processing of personal data?	
☒ Yes ☐ No – Please provide a summary of the project below and submit this DPIA to Information Assurance without completing any further answers.	
Click here to enter text	
1.1.2 Who is the Lead / Manager / Senior Responsible Owner for the project?	
Name	Andrew Hendry (SRO)
Designation	Chief Digital and Information Officer, Police Scotland
Contact details	[redacted]
1.1.3 State who has responsibilities for the personal data. (Refer to Note 1 of the Part 1 Guidance Notes)	
Strategic Information Asset Owner	
Name **Designation** **Contact Details**	Scottish Government Scottish Government acts as the Contracting Authority Scottish Police Authority (SPA Police Service of Scotland (PSoS) Wendy Middleton ACC Criminal Justice [redacted] Police Scotland also acts as Lead Controller and Delivery Lead Crown Office and Procurator Fiscal Service (COPFS) Keith Dargie Head of Business Services [redacted] Scottish Courts and Tribunals Service (SCTS) David Fraser Executive Director of Operations
Tactical Asset Owner	
Name	Supt. Graham Binnie
Designation	Supterintendent, DESC Programme
Contact details	[redacted]

1.1.4 Provide a summary of the project.

Digital Evidence Sharing Capability (DESC) is a project funded by the Scottish Government (SG) for collaboration between Criminal Justice partners, namely the Police Service of Scotland (PSoS), Scottish Police Authority (SPA), Crown Office and Procurator Fiscal Service (COPFS) and the Scottish Courts and Tribunals Service (SCTS).

The SG Justice Digital Strategy pledged to modernise criminal and civil law and the justice system through digital transformation. DESC is a key component of that transformation. The DESC Programme is a technical software deployment of implementation services and operational services and also a package of work to enable operational and legislative change for the collection, editing and sharing of digital evidence at every stage of a criminal case and prosecution across the justice sector, delivering a digital pathway from 'crime scene to court room'. It will deliver an end-to-end service for the collection, management and sharing of digital evidence for all Criminal Justice partners, however in this initial phase, this will be limited to PSoS, SPA, COPFS and SCTS.

Digital evidence may include public and private space CCTV, body worn video, evidential calls to police control room, police interviews, photographs, documents, digital evidence from computers / mobile devices and digital evidence from devices such as dash cams and video doorbells.

DESC will:

- provide the capability to collect and securely share digital evidence between Criminal Justice partners,
- 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, generating variant files, sharing evidence and the retention and disposal of content.

DESC will replace existing processes for the collection, sharing and management of digital evidence.

This large-scale and complex programme is transformational in its ambition; it will radically modernise the parts of the justice system it impacts. However, while DESC is significant in relation to the benefits it will deliver in itself, its value lies in its potential as a platform for further transformation. DESC lays the foundation for a truly modern criminal justice system which places the needs of Victims, Witnesses, and other users of the justice system at its heart.

The DESC solution consists of two main technologies; Axon Capture mobile device app and Evidence.com. which is a secure website. Axon is the provider of the SaaS (Software as a solution) portal through which data is accepted and transferred to the Cloud. Axon Capture will be deployed on Officers' mobile devices. There are three 'instances' of DESC, for PSoS/SPA, COPFS and SCTS, all on the same platform.

Future integrations are planned with PSoS DESC and its 'Unifi' Productions, CRIME and CASE systems, which are used to support criminal investigations before reporting to COPFS. These integrations will improve usability and reduce human error. Data will transfer between systems, examples of which include name of the Officer seizing, date/time seized, unique production number and retention category (how long we are legally required to hold data). Integrations are focused on reducing manual data input and will be subject to further DPIA assessment as they are planned.

In operational terms, a Police Officer will send a member of the public an email link to the DESC solution to upload digital evidence to DESC about a crime or incident that they have been a Victim of, or Witness to. The email link will include the STORM reference number and a short invite from the Officer. DESC is not a public portal and without the link, members of the public will not be able to submit any evidence to it, nor will they be able to use the link more than once to submit evidence. The link will take the member of the public to Evidence.com, the Cloud platform, where they can securely upload their evidence and complete Schedule 8 Certification. This certifies data as a true copy for the

Scottish Criminal Justice process. Once submitted, the evidence and certification is encrypted and transferred into DESC, with a notification sent to the requester. The Police Officer who sent the link will also receive a notification by email to confirm digital evidence has been submitted.

Police Officers and staff and SPA forensic staff (beyond Stage 1 Delivery Pilot) will also be able to upload digital evidence, including that seized or obtained under warrant, to DESC. Secure standalone workstations controlled by Police Scotland's Digital Division will be deployed in Police Stations across Police Scotland.The workstation will allow media to be accessed and evidence uploaded onto DESC. The DVD/USB etc. will be stored securely as evidence. Where an Officer needs to collect the evidence in circumstances when neither an email invite can be used, or media available from the public, a PSoS USB will be issued by their local Business Support Unit (BSU). Further assessment of these arrangements will be part of the project.

Once on DESC, digital evidence will be triaged and accepted by the requesting officer or an enquiry officer in circumstances where the investigation has been re-allocated. Police Officers will use the evidence to investigate the crime or incident and triage this, which may include converting the format, prior to sharing that to the COPFS instance of DESC. All digital material will be checked for threats, and should any threat be identified, the material will be placed into digital quarantine for assessment until it is deemed safe to release the file.

All material will be given a lead agency reference number by PSoS, which is the Crime Reference Number (CR number). Police Officers will also, during Stage 1 Delivery Pilot, create and record Productions reference number using a link to the 'Unifi' Productions system. When a suspect is identified, a Standard Prosecution Report (SPR) will be prepared and submitted for quality assurance to the Police Case Management /Assessment Units who will transfer the SPR to COPFS which will contain a link to the digital evidence within DESC when future integrations are in place. At Delivery 1 Pilot, COPFS will access DESC and search for the digital evidence using the PF Reference Number.

PSoS has the ability to edit multimedia prior to onward sharing to COPFS. Where this occurs, the original footage will remain intact within the PSoS DESC instance, should it be required, with a 'child' file created for the edited version. If required the staff member will certify this as a true copy of the original and complete any necessary certification within the solution This complies with disclosure duties under section 12 of the Criminal Justice and Licensing (Scotland) Act 2010.

The relevant evidence will be copied by PSoS into the COPFS instance of DESC. It will be allocated the relevant COPFS reference number. PSoS will notify COPFS within the SPR or Ancillary report that evidence is held in DESC. In the longer term the link to the evidence will enable prosecutors to easily find the evidence and consider this for prosecution purposes and determine the next actions pertaining to potential criminal proceedings. COPFS staff will be able to access, edit, redact, transfer, delete, disclosure and present evidence from DESC based on role-based need.

When a case decision is made for criminal proceedings, COPFS staff with appropriate authority will if required, be able to edit the material and create a new piece of evidence within the COPFS instance of DESC only, with a 'child file created for the edited version. If required the staff member will certify this as a true copy of the original and complete any necessary certification within the solution.

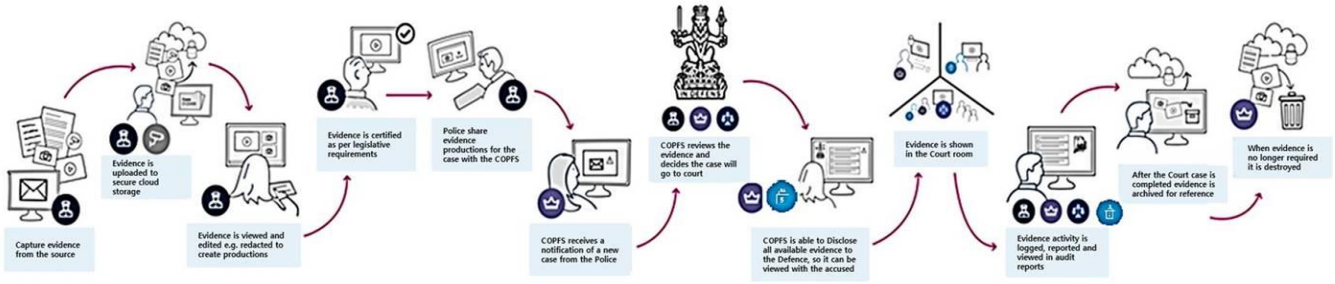
Where specific technical editing is requested by COPFS, PSOS Technical Support Unit (TSU) will undertake this editing within the PSoS/SPA instance of DESC. TSU has access to the original piece of evidence and will create new evidence with appropriate certification. TSU will then share with COPFS as a new piece of evidence. COPFS may in the future, take on more of the responsibility for technical editing, using DESC.

COPFS will share the evidence with the Defence in line with existing disclosure processes and rules. The COPFS staff will utilise a secure defence user account and select this to share the evidence with the defence agent who has provided a letter of engagement for a case. Defence agents must be registered with COPFS and have been allocated DESC access. Defence account details are held within a secure COPFS Azure directory on premise in the UK and synced to allow the Defence to

access their evidence and download this if necessary. This link will only be available for a set period of time, the default being 90 days, although this is configurable by COPFS.

The Prosecutor will be able to play evidence directly from DESC in court or will have the ability to download the material and present evidence in court.

In court, SCTS will provide the equipment and facilitate the viewing of the digital evidence from DESC.



Appendix 1(a) to this DPIA is a PowerPoint presentation that shows, at a high level the operational flow of evidence and the projected benefits of DESC.

Appendix 1(b) to this DPIA shows the process from an Officer's perspective

The foregoing information explains the overall aim of the project. DESC will be delivered in stages and this DPIA updated ahead of each stage go-live.

- Delivery 1 supports the end-to-end process from evidence ingestion to court, focusing on all new multimedia evidence to test the system and facilitate early case resolution. Processing is limited to SPA, PSoS and COPFS.

- Delivery 2 and Delivery 3 will enhance and build upon Delivery 1 including system integrations, Solemn case types, ingestion of existing and emerging evidence types and other considerations such as the case backlog conversion.

- The proposed delivery rollout at 24/01/2023 included in Appendix 1(a). This is a Delivery 1 Pilot and is initially limited to the Dundee City area. It will involve only PSoS and COPFS processing data on DESC.

- The Delivery 1 Pilot is scheduled to last for 6 months.

Police Scotland and DESC partners have been in on-going dialogue with regulatory bodies such as ICO and SBC during the planning and delivery of DESC.

A brief synopsis of the engagement with SBC and ICO is as follows:

SBC:

- 29/11/23 – Presentation delivered to Scottish Biometric Commissioners Professional Advisory Group.
- 27/04/23 – DESC representatives met with SBC which was the first of a scheduled monthly meeting going forward.

ICO:

- December 2022.
- 19/01/23 – Engagement held in advance of DESC pilot go-live.
- 22/02/23 – Quarterly cycle meeting – ICO offered apologies and advised they were working on guidance/feedback to the DESC DPIA.
- 18/04/23 – ICO invited to mock-up demonstration of DESC. Apologies offered again re guidance/feedback on DESC DPIA.

- 24/05/23 – Apologies offered again re guidance/feedback on DESC DPIA.

Through discussion with ICO mention was made of the Geo-mapping functionality which is in existence whilst using the Axon capture App. This has been reviewed and the basic data protection principles have been worked through to ensure it complies.

Part 1, Section 2 – The Purpose of the Processing

1.2.1 What is the reason you want to process the data? If in Q1.1.4 you have covered in full the reason you want to process the data, then please copy and paste the relevant sections here.

Tto facilitate the collection, management, editing and sharing of digital evidence at every stage of a criminal case and prosecution across the justice sector, delivering a digital pathway from 'crime scene to court room'

1.2.2 What is the intended outcome for the individuals whose data you propose to process?

- Improved justice for Victims, Accused and Witnesses through more effective investigation and preparation of digital evidence;
- More secure handling of personal and sensitive data relating to Victims, Witnesses, Suspects and Accused;
- Improved disclosure processes as digital evidence will be readily available in a viewable format for Criminal Justice partners promoting early case resolution which benefits the Victims, Witnesses and Accused.
- Less invasive evidence collection from personal artefacts.

1.2.3 What are the expected benefits for Partners?

Full details of the benefits are listed in the DESC Full Business Case, in summary these include:

- Increased Police Officer productivity through new ability to upload evidence from their mobile device and save directly into DESC where it can be linked to crime/case.
- Police Officers, SPA & COPFS staff can be self-sufficient and can clip and bookmark evidence themselves as required without using technical support units, freeing those staff from the task.
- Reduction in the number of requests from COPFS to Police Officers requesting additional evidence and edits to evidence to prepare them for court.
- Digital evidence can be provided more easily in a court playable format.
- Reduction in criminal justice/court time delays waiting for format conversion of digital evidence.
- Reduction in time spent by staff physically transporting evidence from A to B and the associated administration and management of same.
- Digital certification of evidence can be made available via a highly trustworthy solution.
- Reduction in the number of cases reaching court due to early pleas resulting in less Police Officer time spent having to attend trials.
- Streamlined preparation and presentation in court. Digital media will be in a viewable format from the ingest point and will be accessible from a secure COPFS computer regardless of location. This will allow prosecutors to focus on other areas of case preparation and presentation
- Reduction in time Officers spend attending court regarding technical issues around CCTV evidence and certification.
- Aids compliance with security regulations, standards and guidelines.
- Reduced risk for loss of unencrypted evidence.
- Auditable access and use, in line with the requirements of the DPA18 s62.
- Forensic and cybercrime can transfer, track and manage forensic productions without the need for re-keying therefore allowing evidence to be collated through one solution to be passed to COPFS.
- Single Interface – Integration with the Defence Agent Service will allow visibility of all evidence through a single interface regardless of where the data is being stored in COPFS.

DESC Programme holds a Programme Benefits Register which as a partnership, the Programme will monitor, measure and review throughout Pilot.

1.2.4 What are the expected benefits for society as a whole?

The SG Justice Digital Strategy has pledged to modernise criminal and civil law and the justice system through digital transformation. The ‘status quo’ is no longer an option for the future of digital evidence sharing. This is because the technology and processes currently used in the justice system in Scotland to capture, assess, store and transfer digital evidence cannot keep pace with the growth in volume and value of digital evidence. Current processes are increasingly labour intensive and with increased volume, less secure and more open to security risks if captured, assessed, stored, edited and transferred on a USB or DVD. The public expects, in a digitally enabled society, to be able to easily, safely and confidentially submit evidence related to crimes and incidents and for it to move seamlessly through the criminal justice process. Partners are working collaboratively, understating that there are intrinsic interdependencies and responsibilities in the criminal justice process which mean that all partners must revise their technologyand operational practices for benefits to be derived. Processing the data in a digital format is a key enabler for wider reform across the whole Criminal Justice sector in the future.

DESC is closely aligned with the vision and principles of the Christie Commission, which aims include the public service working much more closely in partnership to integrate service provision and improve the outcomes they achieve for the public. It also drives us to become more efficient by reducing duplication and sharing commonly procured and developed services and technology

At present, this process is undertaken manualy across the Criminal Justice sector, using hard copy discs / USBs / hard drives, photographs and printed documents which are collected and stored as physical productions. This is recognised as an inefficient process which presents risk in terms of Information Security and personal data breaches.

Part 1, Section 3 – Nature of Processing

1.3.1 Has the Information Security (ISM) Manager been consulted: This should be done at the outset of any project – iso@scotland.pnn.police.uk

☒ Yes

☐ No – if not, this must be done immediately.

☐ Not applicable – state below why there is no requirement to consult the ISM.

The Information Security Managers (also known as ISOs) from SPA, PSoS, COPFS and SCTS formed an Information Security Working Group to provide advice and guidance to the DESC Project. Records of the work are held by the Security Managers and by the DESC Project. The ISOs have and continue to will review and approve the security design and assess and accredit DESC for use for policing purposes.

A DESC Security Control Sheet has been established that sets out the security requirements, controls, standards, accreditations and cyber resilience arrangements. It is an auditable evidence-based record of continued adherence to current and developing security requirements and national strategies. Due to the nature of the content, this is a controlled document to which access is limited and it is not detailed further in this DPIA. The supplier also has a copy of this document.

1.3.2 Have the asset owners of any related systems been consulted? (e.g. IT, paper, video etc.)

☒ Yes – If so, provide details.

☐ No – State below at what stage you intend to consult.

DESC Programme and Project oversees the engagement with related systems' asset owners; this includes the involvement of relevant leads within each partner organisation. Representatives of all partners attend a range of meetings to support DESC delivery in their own organisation.

1.3.3 What will the classification of the data be under the Government Security Classification (GSC)? (GSC SOP)

Official ☐ or

Official Sensitive ☒ (NB Official Sensitive **must** be accompanied by handling instructions)

Named Recipients Only ☐ Police and Partners ☒ Police Only ☐

1.3.4 Will any processing be done via an internet / cloud based system?

☒ Yes – Provide the details below.

☐ No

DESC aligns with the Scottish Government's Digital Strategy for Justice in Scotland[1]. This strategy advocates a 'cloud first' approach meaning that public cloud will be the default delivery model for user-focused services. The Digital Strategy for Justice describes a vision of a modern, user-focused justice system which uses digital technology to deliver simple, fast and effective justice. It recognises a need to use digital technology wherever possible to broaden access to justice, improve quality of service and safeguard the rights of citizens and users.

Therefore, DESC technology is made up of a suite of interactive and dependent products. Digital evidence will be stored and accessed in a Microsoft Azure Cloud based system known as 'evidence.com'.

'Axon citizen' will be used to email a unique link to 'evidence.com' to members of the public to allow them to upload their digital evidence.

A disaster recovery backup will be held on Amazon Web Services (AWS) cloud based system.

1.3.5 Will any processing of personal data be done jointly with another organisation?

☒ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☐ No

[1] The Vision for Justice in Scotland - gov.scot (www.gov.scot)

Processing on DESC is separated into 2 distinct types: 'Non-Content' Data and 'Content' Data.

'Non-Content' Data means the data processed by DESC for general contract management purposes and in accordance with the UK-GDPR, comprising limited personal data to facilitate user authentication, logon, permission management, platform performance management, maintenance and auditing. Non-Content Data is processed independently by each Data Controller. There are 5 (five) independent Data Controllers, namely SG, SPA, PSoS, COPFS and SCTS. The SG is limited as a Data Controller to Non-Content data for the purposes of contract management (as the contracting authority).

'Content' Data is means the Personal Data processed by DESC by a competent authority (as defined in the Data Protection Act 2018 section 30 (1)(a) and Schedule 7 or section 30(1)(b)) for law enforcement purposes in accordance with Part 3 of the Data Protection Act 2018 ("law enforcement processing"). Content Data is processed jointly by 4 (four) Data Controllers and clarification of the data processed jointly is contained in Appendix 2. Where partners process jointly, PSoS is the agreed Lead Controller. A Joint Controller Agreement has been agreed by the partners.

SPA: DPO - [redacted]
PSoS: DPO - [redacted]
COPFS: DPO - [redacted]
SCTS: DPO [redacted]

Of note at this time the Axon privacy policy uses the terms 'Customer content' data and 'Customer Entity and User data' instead of content and non-content data. They define these two types of data as:

Customer data:
"Customer Data" means:
(1) "Customer Content", which means data uploaded into, ingested by, or created in Axon Cloud Services within Customer's tenant, including, without limitation, media or multimedia uploaded into Axon Cloud Services by Customer ("Evidence");

Non-Content data:
(2) "Non-Content Data", which means:
(a) "Customer Entity and User Data", which means Personal Data and non-Personal Data regarding Customer's Axon Cloud Services tenant configuration and users;

For purposes of clarity, Customer Content does not include Non-Content Data, and Non-Content Data does not include Customer Content.

This is an issue which has been identified and work is ongoing to resolve same by redrafting sub-processing agreements. However content and non-content data is as defined by partner data protection rules and not Axon.

1.3.6 Will another organisation be processing any of the personal / sensitive data? (Refer to the definition of processor on page 6 of the Guidance Notes). If so, a contract will be required to regulate the relationship.

☒ Yes – provide details of the other organisation, their Data Protection Officer (DPO) and the exact role of the other organisation in the processing of the data.

☐ No

Axon Public Safety UK Limited (Axon), a company incorporated under the Companies Acts (Company Number 07390059) and having its registered office at 14 Sopwith Way, Drayton Fields Industrial Estate, Daventry, Northamptonshire, England, NN11 8PB as the supplier of the DESC solution.

Axon was awarded a contract (Services Contract Reference 388514) with the Scottish Ministers acting through the Scottish Government (SG) to supply software and services for DESC.

Axon engages a number of sub-processors, which is permitted under the terms of the contract and is responsible for ensuring that its contractual obligations are also undertaken by its permitted sub-processors. The list of approved sub-processors at date of pilot is contained in the Data Processing Agreement with Axon agreed by the Controllers and the Joint Controller Agreement. Thereafter, any further/new sub-processors must be proposed by Axon to Police Scotland (as DESC Delivery Lead) and SG (as Contracting Authority) in the first instance. Data Controllers will, subject to the successful completion of their due diligence, authorise (or refuse) permission for the use of the sub-processor.

The DPO for Axon is James Wood (jamwood@axon.com)

In addition to the contract, Data Processing Agreements are being completed by 4 (four) Data Controllers with Axon, namely SPA, PSoS, COPFS and SCTS prior to their processing data using DESC.

SG has reviewed the matter and considers that the contract it has with Axon meets its statutory requirements in relation to the limited processing for which it has responsibility.

In the event that Police Scotland requires support from Axon (UK) with a technical problem they will share the relevant file audit log in the first instance. This file will be redacted and anonymised prior to sending. In the event that Axon (UK) require to discuss the problem with Axon (US) set guidelines are in place:

- There must be no discussion on the content itself and/or the PII therein.
- Discussion must be limited to the technical issue only.

In the event that the issue cannot be resolved authorisation will be sought from the relevant SIO and, if granted, the content data will be shared with Axon (UK) to provide further technical support. Evidence files will never be shared with Axon (US) other than in a catastrophic failure.

1.3.7 Will the processing involve new technology?

☒ Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below.

☐ No

A 3rd party supplier (Axon) will provide a SaaS (system as a solution). Axon will provide a bespoke ‘DESC’ solution comprising of a Microsoft Azure Cloud-based network storage and data transfer platform known as ‘Evidence.com’ alongside ‘Axon Citizen’. This is supported by MS Azure Cloud Services.

A schema for Stage 1 Delivery pilot is attached as Appendix 1a & b

1.3.8 Will the processing be done in any novel or unexpected ways? (e.g. machine learning or artificial intelligence)

☐	Yes – If so, give brief overview of it below. If this has been included in the summary of the project, please copy and paste the relevant sections below.
☒	No
Automation will take place between DESC, COS Unifi, National Crime and Case. The automation will be achieved by linking each separate system via a unique storm identification number or cime number. Each separate system will pull through relevant data e.g. production numbers and update each accordingly reducing the requirement to re-key the same information onto each system.	

Part 1, Section 4 – Scope of the Processing – What the processing covers

1.4.1 What categories of data subject are involved? (Please select all applicable)

☒ Victims
☒ Witnesses
☒ Suspect
☒ Accused
☒ Person convicted on an offence
☒ Children or vulnerable individuals – provide details below
☒ Other – provide details below

- Members of the public, public sector or business operators in the submission and collection of data to be used in criminal investigations and prosecutions. This will include Victims, Witnesses, Suspects and Accused.

- Third parties who provide supporting information or services, including expert Witnesses, forensic specialists, doctors, social workers, and other health and social care professionals;

- Police Officers and Staff working in criminal justice organisations, including but not limited to Prosecutors; Criminal Defence Solicitors and the Judiciary

Evidence Data will not be processed on DESC either from or about children under the age of criminal responsibility who are Suspected of, or identified as causing harm (ACRA Nominals) for the purposes of reporting to SCRA. However where evidence data has been submitted by a Victim or Witness, subsequent investigations may identify that the individual is a child under the age of criminal responsibility.

Digital evidence provided by members of the public / organisations (Victims, Witnesses, Suspects, Accused) may also contain personal data relating to individuals (including children and vulnerable individuals) that have no connection with a case, but who's data is captured as part of a wider recording, e.g. dash cam footage, CCTV. The data processing carried out by the partners will include mitigations to reduce the impact on these individuals that have no involvement in cases, for example by ''trimming' the length of a submitted CCTV clip to show only the section material to the case which will then be shared by partners. The original submission will however be retained to demonstrate transparency and fairness in the criminal justice process and in line with obligations from COPFS and the Lord Advocate.

1.4.2 What is the source of the personal data? (Please select all applicable)

☒ Victims
☒ Witnesses
☒ Suspect
☒ Accused
☐ Person convicted on an offence
☒ Children or vulnerable individuals – provide details below
☒ Other (e.g. data already held in other Police Scotland systems, partner agencies etc.) - provide details below

Personal data will be gathered directly from Victims, Witnesses, Suspects and Accused who may be individuals or organisations. This may include children or vulnerable individuals that are Victims, Witnesses, Suspects, Accused.

Personal data may also be requested from individuals or organisations that have captured it using technologies such as vehicle dash cameras, CCTV or doorbell cameras but are not a Victim, Witness, Accused or Suspect (e.g. PSoS identify that private CCTV may have captured relevant information and approach the company to seek a copy)

Personal data held on partners' criminal justice systems, on public space CCTV and directly relevant to a case may be shared / processed on DESC

1.4.3 List all categories of personal data to be processed. This should also include the types of information if appropriate, e.g. videos, pictures, audio files.

The following data will be processed in relation to the investigation and prosecution of crimes.

The types of Personal Data and Sensitive Personal Data will include but may not be limited to:

Documents and multimedia (including video, audio and images) containing genetic and biometric data, imagery and audio of persons, names, address, correspondence address, date of birth, date of death, telephone number, email address, Hospital Record Number (or other NHS identifiers), accessibility requirements/preferences, nationality, residency details and related information, immigration status, details of medical conditions and medical history, details of functional abilities and impairments, details of existing or previous care and living arrangements, school details (child only), medical records, and equalities data (sex/gender/race etc.) concerning an individual's sex life or sexual orientation, revealing racial or ethnic origin including immigration status, political opinions, religious or philosophical beliefs or trade union membership and alleged criminal conduct

The following types of data will be processed in relation to:

Third parties who may be asked to provide supporting information (e.g. Professional and Expert Witnesses), subject to the solution design, including:

• Name, address, profession, phone number, email address

Staff working in criminal justice organisations (including, but not limited to: Police Officers; Prosecutors; Criminal Defence Solicitors; and the Judiciary):

• Name, location, staff number, job role, phone number, email address
Electronic communications metadata: call and SMS logs -CDRs, MSISDN, MAC addresses, IP addresses, browsing data, location data, device information, click/UI events, application build number, session duration and accesses.

Inferred information; information inferred based on collected information related to users' location, browsing and consumption habits or general behaviour.

1.4.4 Does this project involve processing sensitive data? If so, tick all categories of sensitive data to be processed.

☒ Race	☐ Trade Union membership
☒ Ethnic origin	☐ Genetic data
☒ Political opinions	☒ Biometric data
☒ Sex Life	☒ Sexual orientation
☒ Religion	☒ Health
☒ Philosophical beliefs	☒ Criminal conviction data
	☐ None

1.4.5 Will the personal / special category / criminal conviction data be shared with anyone?

☒ Yes – provide details below

☐ No

- This data is currently shared between the criminal justice partners; SPA and PSoS to COPFS and COPFS to SCTS. DESC will provide a new platform to facilitate the sharing.
- As part of the criminal justice process, certain data, by law, must be shared with other parties such as defence agents.
- As part of the criminal justice processes, certain data is played in court and therefore will be available to the public who are in attendance.

SG is not a Data Controller and as such it will not have access to the 'Content' data on DESC. SG are currently the contracting authority however the intention is for the contract to be novated to SPA from SG. There is currently a cross partner DESC MOU which covers this aspect.

1.4.6 Does the proposed processing involve the collection of data not previously collected by Partners?

☐ Yes – provide details below

☒ No

The data has always been processed as part of the criminal justice process, but in a different manner, i.e. manual processes to capture, record and transfer by DVD, USB or similar.

DESC will facilitate the increasing volume of data, in the form of digital evidence, submitted as part of the criminal justice process. The prevalence of personal image recording devices (CCTV, doorbell cameras, dash cameras, mobile phone cameras, etc.) continues to grow in society and DESC will enable that to be more easily ingested into and process through the end-to-end criminal justice process.

1.4.7 Will the personal / sensitive data be fully identifiable, pseudonymised or anonymised? (Refer to Guidance Note 3 of the Part 1 Guidance Notes)

☒ Fully identifiable

☐ Pseudonymised – provide details of how this will be done, and at what stage in the process

☐ Anonymised – provide details of how this will be done, and at what stage in the process

1.4.8 Does the proposed processing involve any alignment or combining of data sets?
☐ Yes – provide details below ☒ No
Click here to enter text

1.4.9 How many individuals will be affected by the proposed processing, or what is the percentage of the population affected?
All Victims, Witnesses, Suspects and Accused that have either submitted, or are the subject of, digital evidence to the criminal justice process. Other individuals may also be captured in the digital evidence. The total number of crimes recorded across Scotland (Scottish Government recorded crime document 2021/2022, published 28/06/22) was 305,851. This figure includes crime groups 1-7. This is equivalent to 5.7% of the population based on the Scottish population (2011 Scottish census). The DESC pilot will be limited to the Dundee City area for a period of 6 months initially, therefore the number of individuals affected by it will be limited in number. For the period 2021/2022, the total recorded crime figure for Dundee City was 12,004. Not every crime or incident recorded will have associated digital evidence. Third parties who provide supporting information or services, including expert Witnesses, forensic specialists, doctors, social workers, and other health and social care professionals, Police Officers and Staff working in criminal justice organisations, including but not limited to Prosecutors; Criminal Defence Solicitors and the Judiciary will also have limited data captured whist working in their professional role directly related to a case which has relevant data processed on DESC
1.4.10 What is the geographical area involved? (e.g. one division, a number of divisions, whole of Scotland. If this is not to cover the whole of Scotland, name the areas involved)
For the DESC Delivery 1 Pilot, processing will be limited to the Dundee City area for a period of 6 months initially, therefore the processing is limited in its geography. It is proposed that a future rollout will eventually cover all of Scotland

Part 1, Section 5 – Context of the Processing – The wider picture including internal and external factors which might affect expectations or impact

1.5.1 Are there prior concerns internally over this type of proposed processing, or known security flaws?
☒ Yes – provide details below. This must be addressed in the risk assessment ☐ No

Whilst Evidence.Com is used in the Criminal Justice system in England & Wales, the use of large scale, cross-partner cloud based processing introduces areas of risk that require full assessment to ensure that appropriate security measures are in place to protect data subjects.

The use of the DESC solution introduces certain overseas processing, in particular in the USA due to the nature of the Cloud solution and identified supplier. Key concerns have been identified and each partner has independently sought external legal advice. The ICO has also been engaged and provided advice on an informal manner (i.e. not under the DPA18 s65 powers) both verbally on 07/12/22 and in summary, however a detailed written response is awaited on the following matters:

1. The impact of the US Cloud Act
   Certain Data Processors for DESC fall under the jurisdiction of the US Cloud Act, which in principle gives a legal gateway for the US Government to compel certain Data Processors to provide evidence (Content Data) to it, without the knowledge of the Data Controllers or the contracting authority. It is assessed that were this to happen, this would have an adverse impact on a data subject's rights.

   There is current and ongoing engagement between US law enforcement authorities and Scottish counterparts though regular and routine governance channels when a case arises that may result in a formal request for information or evidence to be provided. Therefore, because formal channels exist to request information and/or evidence and are currently used, it is unlikely that such an obligation will be imposed on the Data Processors in all but exceptional circumstances.

   DESC Partners have imposed obligations on Axon and by default, it's sub-procesors, to inform the Data Controllers when requests are made, but understand that in certain circumstances they may not be permitted to do so as a consequence of the US Cloud Act. Therefore, available mitigations are limited. Consequently, this risk has been considered by the DPOs and by the Senior Information Risk Owners (SIROs) of each of the Data Controllers.

2. Clarification of whether processing includes data in transit
   The Data Controllers understand that data in transit is not considered a transfer under Data Protection legislation. This has influenced the application of proportionate security measures to protect data and also reassure data subjects.

3. The impact of the main supplier (Axon) using sub-processors, in particular Microsoft, and relying on terms and conditions drafted for GDPR compliance only, whilst the processing of evidence (Content Data) on DESC is primarily governed by the DPA18. This matter has been investigated and the Data Controllers have worked with the supplier to identify and implement resolution pathways which include:
   - Processing 'Content' Data within the UK.
   - Understanding the role of all sub-processors in the DESC solution
   - Undertaking due diligence on all sub-processors to ensure contractual terms are properly reflected either with Axon or directly with the Data Controllers. Axon has supplied SCC (standard contractual clauses) for its sub-processors which have been reviewed by the Data Controllers. Whilst a resolution pathway has been identified for Sub-Processors, it is not expected to be in place for all Sub-Processors before the Delivery 1 Pilot Go-Live and therefore this is a risk to be considered by the DPOs and SIROs for each of the Data Controllers involved in that delivery phase.
4. The essential requirement for the supplier to have access to Content Data to deal with emergency situations that may jeopardise the software/platform. Axon has confirmed that technical support will be provided by a UK-based and vetted team.


Scotland DESC Go Live Support - 11012


Security Commitment 110123

It is anticipated that in most cases DESC partners will only ever use the UK support line to notify Axon of issues, however to maintain the routing capability 24/7 there could be the occasion an initial call is logged with Axon Globally for triage purposes only. Axon will only gather information on the fault for the correct allocation to the UK support engineers, all with the correct clearance to manage.

Axon cannot control what the customer says in the support call, but there should be no need to include Content Data information within these calls. Calls to Axon to discuss technical matters will be limited to the DESC Project team and in DESC partners' ICT specialists.

5. Bring Your Own Key (BYOK) is not possible within the existing Axon evidence.com solution
6. SPA is a competent authority for processing under DPA18 s30(1)(b)

The SIROs for PSoS, COPFS and SCTS have reviewed and accepted the risks prior to Deliery 1 Pilot, whilst SPA, which will not be processing data in the Delivery 1 Pilot will consider the matters further ahead of any processing it undertakes on DESC.

1.5.2 Describe any relevant advances in technology or security

N/A

1.5.3 Are there any current issues of public concern in the area of the proposed processing? If so, provide details.

☒ Yes – provide details below. This must be addressed in the risk assessment.

☐ No

The matters raised at 1.5.1 are in the public domain, particularly in special interest and professional (security, data protection etc) forums in general terms for overseas processing, not specifically in relation to DESC, however Axon has been mentioned.

Consequently it is important that the partners, as Data Controllers address these matters as failure to do so may cause public concern and/or confusion.

1.5.4 What relevant codes of practice have been considered and complied with?

Scottish Biometrics Commissioner's Code of Practice

For DESC Data Protection Working Group use only:

1. **Is the proposed processing of personal data (Content Data) for Law Enforcement purposes likely to result in a high risk to the rights and freedoms of the data subject?**

   ☒ Yes – Provide the rationale for your decision below

   ☐ No – Provide the rationale for your decision below

2. **Is the proposed processing of personal data (Non-Content data) for UK-GDPR purposes likely to result in a high risk to the rights and freedoms of the data subject?**

   ☐ Yes – Provide the rationale for your decision below

☒ No – Provide the rationale for your decision below

Rationale for decision:

1. Content Data

   This is large scale processing of sensitive personal data associated with the end-to-end criminal justice process across all of Scotland, albeit the Delivery 1 Pilot is limited in both scope and scale and a phased future rollout is planned.

   Consequently it is essential that the processing is undertaken in a secure manner that protects data subjects' rights and supports their right to justice / a fair trial by protecting the confidentiality, integrity and availability of digital evidence.

   The processing involves complex partnership and contractual arrangements and a third party supplier, imlementing new technology and consideration of data sovereignty issues.

   Consequently, the partners, as Data Controllers consider that processing of Content Data is high risk processing for which there are high risks that must be mitigated and a full DPIA is required.

2. Non-Content Data

   This is processing of limited personal data of Officers and staff for limited purposes which is in line with their operational activities and employment. Whilst it involves large numbers of individuals, it is limited to their working life only and the purpose for processing (to logon to a system to undertake a task) is the same as multiple other ICT platforms and systems used in the course of their working day.

   The Data Controllers have addressed in detail and in a DPA and other project documentation the purpose, use and governance of the Non-Content Data and have taken steps to design data protection principles into its processing.

   Consequently, the partners, as Data Controllers consider that processing of Non-Content Data is not high risk processing for which there are high risks that must be mitigated.

DPIA Part 2 – Assessment of legality, governance and risks

Name of Project: Digital Evidence Sharing Capability (DESC)

URN: PSoS 22-389

Part 2, Section 1 – Assessment of Necessity and Proportionality – The Data Protection Principles and other relevant sections of the Data Protection Act 2018 (DPA 2018) and UK-GDPR

1st Principle – Lawful and fair and transparent.

2.1.1A Is the processing based on consent?
☐ Yes ☒ No

2.1.1B Define your legal and lawful basis for processing. Please list any legislation specific to the proposed processing below
Appendix 2 contains details of the underpinning legislation or powers on which the processing is based for both Non-Content and Content Data. Each Data Controller has defined its legislative powers for the processing of data on DESC. Non-Content Data means the data processed by DESC for general contract management purposes and in accordance with the UK-GDPR, comprising limited personal data to facilitate user authentication, logon, permission management, platform performance management, maintenance and auditing. Non Content Data is processed under UK-GDPR Content Data means the Personal Data processed by DESC by a competent authority (as defined in the Data Protection Act 2018 section 30 (1)(a) and Schedule 7 or section 30(1)(b)) for law enforcement purposes in accordance with Part 3 of the Data Protection Act 2018 (“law enforcement processing”). Content Data is processed under Data Protection Act 2018 part 3 **Non-Content Data** 1. SG – UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest 2. SPA – UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely Police and Fire Reform (Scotland) Act s31 3. PSoS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely, Police and Fire Reform (Scotland) Act s17 & 20 4. COPFS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely the administration of justice 5. SCTS - UK-GDPR Article 6(1)(e) Processing is Necessary for the Performance of a Task carried out in the Public Interest, namely the administration of justice **Content Data** 1. SPA ▪ DPA2018 s35(2)(b) by a Competent Authority (s30(1)(b)) and s35(5) and Schedule 8 (1) ▪ Police and Fire Reform (Scotland) Act s31 which obligates the SPA to provide forensic services ▪ Criminal Procedure (Scotland) Act 1995 which places a statutory duty on SPA ro provide evidence to the Crown

2. PSoS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (1)
   - Police and Fire Reform (Scotland) Act s17 and s20 which place a statutory responsibilty on the Chief Constable for the administration of day-to-day policing and continuous improvement, to comly with lawful instructions from COPFS and which place statutory duties on Constables to make reports to the COPFS
   - Criminal Procedure (Scotland) Act 1995 which places a statutory duty on PSoS to provide evidence to the Crown
   - Criminal Justice and Licensing (Scotland) Act 2010, sections 117-120 places a statutory duty on PSoS to provide the prosecutor, after the first appearance of an accused, with details of all the information that may be relevant to the case, obtained during their investigation. Police Scotland also have an ongoing commitment to provide any further relevant information which is obtained.

3. COPFS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (1 & 2)
   - Criminal Procedure (Scotland) Act 1995 which places a statutory and common law duty to adduce evidence during trials to constitute a sufficiency of evidence
   - Criminal Justice and Licensing (Scotland) Act 2010 s121-123 which places a statutory and common law duty on the Crown to disclose evidence to the Defence
   - Statutory duty on COPFS to lodge evidence within time limits for Solemn cases (Criminal Procedure (Scotland) Act 1995 s68(2)

4. SCTS
   - DPA2018 s35(2)(b) by a Competent Authority (Schedule 7) and s35(5) and Schedule 8 (8)(1), (2) & (7)
   - Criminal Procedure (Scotland) Act, 1995
   - Judiciary and Court (Scotland) Act, 2008, section 61-62

2.1.2 Does the processing involve the processing of sensitive data? Tick all that applies

☒ Race	☒ Trade Union membership
☒ Ethnic origin	☒ Genetic data
☒ Political opinions	☒ Biometric data
☒ Sex Life	☒ Sexual orientation
☒ Religion	☒ Health
☒ Philosophical beliefs	☐ None – go to question 2.1.4 below

2.1.3 To process sensitive data for a law enforcement purpose at least one of the following (or another Schedule 8 condition not listed below) must be satisfied. The Schedule 8 conditions must be read in full before completing this question. Check all that apply and provide further details below as to why each applies. Schedule 8 of DPA 2018

☐ The individual has given consent to the processing

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 for the administration of justice

☐ is necessary to protect the vital interests of an individual

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

☐ relates to personal data manifestly made public by the data subject

☒ Other Schedule 8 condition – Provide details below

The Data Controllers for 'Content Data' are competent authorities for the processing of law enforcement data.

- PSoS, COPFS and SCTS are competent authorities as defined by Data Protection Act 2018 s30(1)(a) and Schedule 7.
- SPA is a competent authority as defined in the Data Protection Act 2018 s30(1)(b) and its statutory duty defined in the Police and Fire Reform (Scotland) Act s31

Appendix 2 provides a diagramatic overview of the functions conferred on the controllers by an enactment/rule of law and necessary for reasons of substantial public interest

COPFS and SCTS must process the data for the administration of justice

In certain cases, the processing will be necessary to safeguard children and/or individuals at risk by ensuring criminal cases are investigated and the criminal justice process followed.

SCTS must also process the data for judicial acts

All Data Controllers have an Appropriate Policy Document in place

2nd Principle – Specified, Explicit and Legitimate – DPA Section 36

2.1.4 Is the personal data to be used for the purpose for which it was first gathered?
☒ Yes ☐ No – State below the purpose for which it was gathered, and the new purpose
Click here to enter text

3rd Principle – Adequate, Relevant and Not excessive – DPA Section 37

2.1.5 What assessment has been made to ensure that the personal data being processed is adequate, relevant and not excessive in relation to what is necessary for the purpose for which they are gathered?
DESC is not a 'public' portal where data can be uploaded in an unsolicited manner. Data can only be submitted by a member of the public after a crime or incident has been reported and a link sent by PSoS. Where Victims and Witnesses provide their data, Officers will provide advice prior to providing a link on what data is required following engagement with the individual. This may, in some instances, involve viewing the data if the Victim or Witness agrees. Whilst Victims/Witnesses will be requested to submit only the minimum amount of relevant data, they may provide more where they believe it is necessary, or they may not have the knowledge or resources to 'trim' the data before submitting to DESC. Where Victim, Witness, Suspect or Accused data is uploaded by PSoS, it will be limited to that which the Officer/Staff member considers may be relevant for the incident under investigation. PSoS will report to COPFS on DESC only that data that it is required to do by Criminal Porcedure Scotland Act 1995 and Disclosure rules When data is subsequently considered by COPFS, the Prosecutor will assess what is necessary and proportionate in terms of the criminal law to prosecute the case. "Engagement has been undertaken between Scottish Government, COPFS and the Judiciary to consider if non-relevant, non-exculpatory data submitted by a Victim/Witness in relation to summary cases could be deleted after submission without undermining the judicial process. This an area still to be fully progressed and there is no defined timescale for a decision and engagement will continue beyond the proposed pilot go-live date."

4th Principle – Accurate and kept up to date where necessary – DPA Section 38

2.1.6 How will the accuracy of data be checked?

Content data is provided as evidence during the investigation of a crime or incident. During the course of the PSoS criminal investigation and following PSoS procedures and statutory requirements, Officers will determine if the data is relevant to and should be provided to COPFS.

At point of triage, Officers who identify that a member of the public has supplied evidence that isn't connected to the case – for example if they have mistakenly uploaded an unrelated video clip rather than the video clip rather than the one connected to the incident - can 'Decline' the digital evidence and it will be deleted from the system. An audit record will be mantained

If an Officer/Staff member identifies an error, for example evidence being associated with the wrong case number, they can amend it in the instance of DESC in which they are working. In addition, Case Management staff in PSoS have a number of business process steps to check accuracy prior the evidence being shared and that will be improved through integration.

If a mistake is identified after data has been shared, DESC Project has a created process showing how the Lead Agency Tracking Number can be updated and how errors in submissions from PSoS to COPFS are amended.


Incorrect LATN.pdf


Incorrect Evidence Shared in Bundle V2

COPFS is dependent on Police Scotland and SPA in the first instance to ensure the accuracy of the material shared to it. Any inaccuracies identified thereafter will be assessed and rectified on a case-by-case basis. If COPFS discover an error, it will relay information back to the reporting officer through pre-existing channels (Fiscals Memo or SFI) and it is the responsibility for the reporting officer to correct the error. This is the method already in place and replicates many of the PSOS and COPFS partnership processes. Automation through integration may be looked at in the future, for example notification a case is complete etc. but at this time it is manual using pre-existing business processes.

2.1.7 What process will be in place to keep it up to date where necessary?

If a mistake is identified after data has been shared, DESC Project has created process maps for the Lead Agency Tracking Number to be updated. These are included in 2.1.6

Any inaccuracies identified will be assessed and rectified on a case-by-case basis. If COPFS discover an error, it will relay information back to the reporting officer through pre-existing channels (Fiscals Memo or SFI) and it is the responsibility for the reporting officer to correct the error. This is the method already in place and replicates many of the PSOS and COPFS partnership processes. Automation through integration may be looked at in the future, for example notification a case is complete etc. but at this time it is manual using pre-existing business processes

2.1.8 There must be a functionality or procedure to distinguish between fact and opinion. How will you ensure that this is done? If this cannot be done, please explain why.

Fact - Data (digital evidence) is identified though criminal investigation. Digital evidence will be uploaded in its native format. The DESC processes are based around users ingesting digital files and not opinions

Opinion - DESC has the capability to include notes and bookmarks for clipping evidence. Entries via free text into notes will be part of DESC training.

2.1.9 How will you ensure that there will be a clear distinction between personal data relating to different categories of data subjects? (e.g. Victims, Witnesses, Accused etc.) If this cannot be done, please explain why

For Delivery 1 Pilot, Data ingested into DESC will be allocated a unique Production Reference number (provided by PSoS National Production system) and will be held within a case folder on Evidence.com, which when shared with COPFS, will cross refer with the National CASE Lead Agency Tracker Reference Number (SPR). SPA will not upload Data to DESC during Delivery 1 Pilot No status is given to a person supplying the data. PSoS will accept digital evidence pertaining to a case from any person that has been offered the link, provided the evidence or who has had digital evidence seized. All victims, witnesses, suspects and accused from whom digital evidence is held are recorded as 'citizens' on DESC and they are not attributed a status. There is no functionality to differentiate. During an investigation process, the status of a data subject who provides or is captured in digital evidence may change. For example, through the investigatory process and assessment of all available evidence, including but not limited to digital evidence, a Witness may become an Accused, or a Suspect may become a Witness. On DESC, as all data subjects from whom the ditigal evidence is obtained are recorded as 'citizens', status will not change. The status of individuals during the course of an investigation will continue to be recorded on associated systems, including but not limited to COS Unifi, Case Management.
2.1.10 What steps will be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes? DPA Section 38(4) and (5) refers
At each stage of the criminal justice process, outlined in s1.1.4, partners will assess the evidence submitted or held on DESC for relevance to the criminal justice process. Data that is not deemed relevant will not be shared by PSOS to the COPFS instrance of DESC. COPFS will not use Data that it does not deem relevant in criminal proceedings,but will make all disclosures to defence agents required by law. Access to Data on DESC is limited by role based access and used only for the case that it is submitted in relation to.

5th Principle – Not kept longer than necessary – DPA Section 39

2.1.11 How long will the personal data be retained?
DESC partners have convened a Records Management working group to define the retention period for the data, taking into account the nature of the criminal justice process, rights of appeal, impact on data subjects and the responsibilities and role of the Lord Advocate in determining the retention of evidence submitted, both relevant and non-relevant. During the period of the Delivery 1 Pilot, all data will be retained. E-mail invites to members of the public will be routed via Axon Citizen and deleted thereafter. A defect has been identified that means the data is not being systemically deleted at this time. Axon has identified a technical resolution, however the lead-in time for testing and implementation is c.8 weeks and it will not be ready at point of Delivery Stage 1 Pilot. DESC Project will continue to engage with Axon and implementation will proceed as soon as the functionality is ready to correct the defect. This will remediate all contact data held.
2.1.12 The system must be able to weed and delete a) individual records and b) bulk records. How will you ensure that this can be done? (e.g. manual intervention, automatic deletion etc.)

a) At point of ingestion, Officers will review digital submissions as part of the triage process. An Officer can elect to Accept or Decline the digital evidence provided. This allows for very obvious errors made during a submission to be deleted, e.g. the person submitting the evidence providing the wrong digital evidence by mistake.

Each partner's instance of DESC is 'stand alone'. Therefore, no partner can delete data from another partner's instance and a deletion by COPFS for example will not automatically update PSoS. If there is a need to delete data once shared from one partner to another (for example shared by PSoS to COPFS), the partners will be informed via a Subject Report which is sent via National Case under the Lead Agency Reference Number, which is the same process documented in 2.1.6 above. This means that each partner must have in place relevant processes to authorise deletion, based on the technology available.

Deletion capability is controlled by RBAC. This means not every person that has a logon to DESC and can access data will have the permissions to delete it. If digital evidence has been accepted and subsequently requires to be deleted, in PSoS, a 3-tier authorisation process will be applied.

1. Officer emails supervisor requesting deletion of defined data/digital evidence and providing a rationale.
2. Supervisory Officer reviews data/digital evidence. If supported, Supervisory Officer makes a request in writing to Inspector
3. Inspector reviews data/digital evidence. If supported, Inspector documents the rationale on DESC and deletes the data/digital evidence, this process includes the provision and application of a verification code by the authoriser. The data/digital evidence will be held queued for deletion for a period of 7 days before permanent deletion.
4. An audit trail of these actions will remain on DESC

b) During the Delivery Stage 1 Pilot, as defined in 2.1.11 above, data will not be systemically weeded. Any and all weeding/deletion required during pilot phase will be carried out using the processes and method defined in 2.1.12(a). Consequently, there is assurace that digital evidence and associated data can be deleted from DESC when required.

Beyong Delivery Stage 1 Pilot, Axon Evidence.com provides the functionality to manage retention and deletion through both automated and manual processes. Axon is contractually obliged to ensure that data is securely destroyed or deleted in line with Retention Rules and any additional requests from the Data Controllers.

DESC Project is planning to have the functionality to perform automated weeding of digital evidence and associated certification and data stored in DESC. This may involve integrations with other system(s) including but noyt limited to PSoS UNIFI Productions to automate the process.

The design of this functionality will be subject to further DPIA updates prior to being implemented.

Refer to 2.1.11 for details of Axon Citizen

2.1.13 If the data is to be retained after the retention period, e.g. for statistical purposes, how will it be anonymised?

There are no documented plans to retain DESC metadata for statistical or data science purposes beyong its retention period (based on primary operational value) at this time.

As noted in 2.1.11, the DESC Records Management Group in conjunction with the DESC Programme is defining retention periods for all DESC data including audit logs. If during that discussion a secondary value for anonymised or pseudonymised metadata is identified, further DPIA updates will be undertaken prior to implementation

2.1.14 What processes will be in place to ensure the data is securely destroyed / deleted?
DESC Stage 1 delivery will not involve the systemic deletion of personal data, however if individual Content Data is deleted during pilot, for example as a result of a data subjects rights request, or an officer declining submitted data (as detailed earlier in this DPIA), the data is placed in a deletion queue for a period of 7 days. This allows for any deletion errors to be remediated and data restored. At the end of the 7 day period the data is permanently deleted and cannot be restored. The same functionality will apply to systemic deletion in future. The technical security of the deletion process has been reviewed by ISO

6th Principle – Security / Security of processing – DPA Sections 40 and 66 – Technical or organisational measures in place to ensure protection of the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage and obligations relating to security, respectively.

2.1.16 If in Part 1 you stated that you had not consulted with the Information Security Manager (ISM) has this now been done?
☐ Yes – and advice received ☐ No – explain below why this has not yet been done ☒ Not applicable
Click here to enter text
2.1.17 On which risk register will the information be recorded? If it is already on a risk register, please state which.
For the Stage 1 Delivery Pilot, risks will be recorded on the DESC Partnership Risk and Issue Register. As Delivery progresses through the stages defined in 1.1.4 and into business-as-usual, any residual risks will be assessed and transitioned to the appropriate Data controller(s) and their risk register(s). This will be updated in future DPIA updates.
2.1.18 What processes will be in place to determine who will have access to the data / system and how is it done?
Role Based Access Control (RBAC) functionality will be used to manage and limit what individuals have access to and can do. Roles, groups and permissions are designed around partner-specific requirements. Each Data Controller has created a number of User Stories that set out how the roles, groups and permissions align to meet business and user requirements. Each User Role's permissions are depicted within process maps and spreadsheets to ensure that Roles are linked to RBAC. Any changes in Roles will be controlled by an Administation Role which is limited in numbers of individuals. For the purposes of the Delivery 1 Pilot: <u>SG</u> SG staff have responsibility for contract management, but will not have or be given logon capability to the DESC solution as it is not required for any purpose. <u>SPA/PSoS</u>

Administrative users will grant and remove access to the DESC solution via the SCoPE interface. Changes will then automatically propagate the RBAC solution into DESC. In instances where access needs to be removed immediately, administrative users will be able to disable user accounts within the DESC solution to avoid the slight delay in the full automated pipeline.

The DESC solution will be integrated with the PSoS Azure Active Directory (AD), which will be informed by the internal PSoS/SPA HR Management system known as SCoPE. Users will be assigned a role within SCoPE which will in turn determine their AD group membership. Permissions will then be based off of the AD group and propagate through to the associated user account in the DESC solution.

COPFS

COPFS staff will have access to SPRs and DESC Content Data based on a business need and role specific basis to enable them to access evidence within DESC. IT engineers within COPFS will grant and remove access to DESC solution via the on-premise Active Directory Azure access management policy. IT engineers will be able to immediately disable accounts within DESC to avoid the slight delay in the fully automated pipeline. Approved DESC users will manage and control access to evidence within DESC considered sensitive by COPFS

Axon as Data Processors

Axon has assured that it has RBAC processes in place to limit processing of content data to its UK based and vetted staff. ISO group are continuing to engage with Axon.

2.1.20 What level of security clearance (i.e. vetting level) will be required to access the system?

NPPV3

Axon confirmed in writing that only UK-based and vetted staff will be able to process (access) Content Data for the purposes of providing technical support in authorised scenarios or in the event of catastrophic system failure where immediate action is required. Furthermore Axon (US) can access content data in the event of a catastrophic failure (with permission from Police Scotland).

2.1.21 What data protection / security training will users, processors, external contractors etc. receive, before gaining access to the system?

All partners as Data Controllers are responsible for the delivery of adequate data protection / security training to their Officers/Staff (including contractors) prior to the use of DESC and on an ongoing basis thereafter. Partners will commit to the delivery of appropriate training through the Joint Controller Agreement (JCA)

As a Data Processor, Axon is contractually obliged (Services Contract Reference 388514, s13.6) to provide adequate data protection / security training to their staff prior to their use of DESC and on an ongoing basis thereafter. It is also the responsibility of Axon to ensure that sub-processors have completed training which is commensurate to their contractual requirements. DESC partners as Data Controllers are undertaking due diligence checks with Axon of its sub-processors to ensure that appropriate terms and conditions are in place.

PSoS as Delivery Lead will co-ordinate the monitoring of Axon compliance and partners will collaborate where it is appropriate to do so.

2.1.22 Confirm you will you have a SyOps / procedure manual / SOP etc. to detail the above?

☒ Yes – state below which of the above.

☐ No – state below, why not.

For Delivery 1 Pilot

- DESC Guidance Document (to support the training)
- Systems Operations form
- IT Handover documentation
- Videos
- ICT Helpdesk
- Floorwalkers
- PSoS Divisional champions
- PSoS Opertional Order

2.1.23 What technical controls will be put in place to protect data at rest, from compromise? Check all that apply.

☒ Encryption

☒ Role Based Access Control

2.1.24 How will information be protected in transit?

☐ Secure email

☒ Encryption

☐ Egress

☐ Other – Provide details below

Data in transit within the Police Scotland Network and Data Centres will be secured by:

GCM-AES-128 encryption

TLS 1.2 implementation with 256 bit connection, RSA 2048 bit key, Perfect Forward Secrecy

Data in transit to the cloud-hosted DESC solution will be secured by:

FIPS 140-2 validated: Axon Cryptographic Module (cert #2878)

TLS 1.2 implementation with 256 bit connection, RSA 2048 bit key, Perfect Forward Secrecy

2.1.25 Explain how loss of data at rest, will be prevented in case of a business continuity incident / disaster recovery. (e.g. Business Continuity Plans, backups and frequency, resilience, parallel systems etc.)

Axon is contracted to provide a fully resilient solution, with agreed Business Continuity Plans and Disaster Recovery plans.

In the event of a major disaster that results in a full loss of a Microsoft Azure region, Axon has created the Axon Evidence Information System Contingency Plan (ISCP). The ISCP focuses on the recovery of Axon Evidence to a secondary Microsoft Azure region. Axon is confident, that in the event of the complete destruction of a primary Microsoft Azure region, Axon Evidence can be recovered and restored in the secondary Microsoft Azure region within, at most, a 24-hour window.

Axon states that its BCP and ISCP programme is designed in alignment with and complies with NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide where applicable. Axon states it tests its contingency plans, backups, and operations on at least an annual basis, with test results stored internally within the Axon ISCP. Engagement with Axon on detailing this is ongoing.

The process when a Disaster Recovery Plan (DRP) commences is as follows:

The Business Continuity Management Group, Contingency Planning Co-Director and Contingency Plan Team will appropriately involve all levels of Axon personnel to maintain normalised Axon-internal situational awareness to recovery processes.

Reconstitution -
If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities:
(1) validating successful reconstitution
(2) deactivation of the plan.
Upon completion of data restoration process, the Contingency Plan Team performs environment validation with the appropriate Axon Cloud Services (ACS) teams.

Data Validation Testing -
Data validation testing is not applicable in the scenario in scope for the ACS DRP. Original records are assumed to be unrecoverable and inaccessible for data validation testing activities.

Functional Validation Testing -
ACS teams will perform testing and validation of operations and application functionality and ongoing system monitoring by the Axon Engineering team will occur until assurance is gained over the recovery system.

Recovery Declaration -
Upon successfully completing testing and validation, the Contingency Planning Co-Director will formally declare recovery efforts complete, and that ACS is in normal operations. ACS business and technical POCs will be notified of the declaration by the Contingency Plan Coordinator. The recovery declaration statement notifies the Contingency Plan Team and executive management that the ACS has returned to normal operations.

Recovery should be fully transparent in terms of user interaction with ACS. The URL will persist and DNS records will be updated to route requests to the alternate processing centre (Azure UK West). All core functionality, including the ability to upload new evidence, will be available to JMPU.

Part 2, Section 2 – Information Sharing

2.2.1 Is any of the data being processed to be shared with third parties? (i.e. outwith the partners)

☒ Yes – state below which 3rd parties.

☐ No – go to question 2.3.1.

COPFS will share relevant Content Data with Defence Agents as required by the Criminal Procedure (Scotland) Act 1995 which places a statutory and common law duty on the Crown to disclose evidence to the Defence. This may be done on DESC with limited Defence Agents, and also using existing and separate processes.

Certain data will also be played in court as part of the trial process using DESC, at which the public may attend.

2.2.2 If the information is to be shared with third parties, are there Information Sharing Agreements (ISAs) already in place with these third parties?

☐ Yes – agreement(s) in place – Give details below

☐ Not yet – agreement(s) required

☒ No – none required. If not required, state the reason.
It is a statutory requirement for COPFS to disclose certain data to defence agents as part of the criminal justice process and to ensure a fair trial. This is not subject to ISAs but is subject to defined procedures within COPFS COPFS must present relevant Data during a trial, in public and under the direction of the Judiciary. Consequently this is not subject to ISAs, but is subject to defined procedures within COPFS

Part 2, Section 3 – Measures Contributing to the Rights of the Data Subjects

Subject Access Requests (SARs) – DPA Section 45

2.3.1 How will you ensure that the personal data will be available for the processing of SARs?
During the Delivery 1 Pilot Phase, the DESC Project will act as a SPOC for the staff in PSoS (Information Disclosure) and COPFS (TBC) to access the data and facilitate SARs. A scalable business-as-usual solution will be included on the DESC Project Action List. A Pilot Action Log of all the requirements to be taken forward into Pilot will be finalised primarily based on the "Caveats" in the Ready with Caveat status assessment of the x-partner Go No Go Tracker which has been updated to confirm that the actions, risk mitigations, agreed controls and monitoring throughout this DPIA, the JCA and DPA must be undertaken.

Right to rectification, erasure and restriction – DPA Section 46, 47, and 48

2.3.2 How will you ensure that the personal data can be corrected, deleted or the processing restricted if required, in response to an individual's rights request?
During the Delivery 1 Pilot Phase, the DESC Project will act as a SPOC for the staff in PSoS (Information Disclosure) and COPFS (TBC) to access the data and facilitate Data Subjects Rights Requests. As defined in s2.1.6 of this DPIA, there is practical functionality designed into the DESC solution that will allow the rectification of incorrect data. DESC functionality also allows for the erasure of individual data and restriction of processing. A Pilot Action Log of all the requirements to be taken forward into Pilot will be finalised primarily based on the "Caveats" in the Ready with Caveat status assessment of the x-partner Go No Go Tracker which has been updated to confirm that the actions, risk mitigations, agreed controls and monitoring throughout this DPIA, the JCA and DPA must be undertaken.

Part 2, Section 4 – Other legal requirements

Auditable Logging – DPA Section 62

2.4.1 The system must create an auditable record (or log) each time a user does any of the following to the personal data. Please confirm or otherwise that the proposed system will do this. This is a legal requirement. **If these requirements cannot be met before the system goes live, the system will not be accredited.**
a) Collection – the log must record • what data was collected / input • the identity of the individual who updated the system with the data • the date and time the system was updated ☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of the DPIA.**

The Axon Evidence Accreditation Statement "Axon state that logs that are sent to the Security Incident Event Management) SIEM tool for monitoring are initially recorded in UTC. Audit trails, which are customer facing audit records, on the other hand, are in the time designated by the customer for their Axon Evidence profile. Therefore, before relying on an audit trail, care must be taken to ensure that the log file times have been translated appropriately."
The SIEM system is the Axon system. PS have asked for access to this but the question is unresolved.

b) Alteration – the log must record:

- the data that was altered
- the identity of the individual who altered the data
- the date and time the data was altered

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

Within DESC, Evidence Audit File Logs will be used to track all 'access' and 'edit' history for evidence files and case folders, including associated metadata. Therefore, any changes made to a file or its metadata (e.g. reassigning an evidential file, renaming evidence, redactions and deletions) will be logged in the Evidence Audit Log. This log entry will contain the date and time of the change, the user who performed the change, the type of change and the users client IP address.

c) Consultation (accessing / viewing) – the log must record

- what data was consulted
- the reason for the consultation
- the identity of the person who consulted it
- the date and time of the consultation

☐ Yes – the system will record an auditable record of all of the above

☒ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

All access to evidential data within DESC will be tracked within the Evidence Audit File Logs which will detail the date, time, user ID and client IP address for whenever a user accesses evidential data. The justification is not recorded in DESC in every instance but can either be inferred or identified from the sequence of user activity recorded in DESC, for example the viewing of evidence by a Police Officer and the immediate next action of sharing to COPFS, or the justifications captured in related case records or procedural manuals.

d) Disclosure (including transfers) – the log must record:

- the information that was disclosed
- the reason for the disclosure

- the date and time of the disclosure
- the identity of the person who made the disclosure
- the identity of the recipients of the data

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

These will be automatically recorded in the User audit system log files.

e) Combining with other data – the log must record:

- the data which was combined
- the identity of the individual who combined the data
- the date and time of the combination

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

The DESC solution requires technical integrations with the PSoS DEPP COS UNIFI solution in order to maintain a consistent set of production and crime data across the DESC and DEPP COS programmes. Evidential data will be uploaded into the DESC solution and will be linked to the associated incident using the STORM ID. Related pieces of evidential data in DESC will be collated in DESC in order for a case. Once a case is ready to be created within the DESC solution, it will be created with the Crime Record (CR) Number as the Case ID. The DESC solution will then make an API call to DEPP COS UNIFI to create a Production record within UNIFI linked with the CR Number. Once the production record within UNIFI has been created, UNIFI will return a Production Number back to the DESC solution, again via an API call. This will assure a consistent record of linked cases and productions across all integrated systems.

The creation of evidence, evidence bundles and cases will be tracked in the aforementioned Evidence Audit File Logs and the creation of Production records within UNIFI via API calls will be tracked in UNIFI audit logs.

f) Erasure / weeding – the log must record:

- the fact that a specific record was accessed
- that data was erased/weeded
- the identity of the individual who erased/weeded the record
- the date and time of the erasure/weeding

☒ Yes – the system will record an auditable record of all of the above

☐ No – Explain which of the above requirements will not be met, the reason and the mitigations. **A detailed proposal of how this will be done must be included in the risk assessment at the end of this DPIA.**

These will be automatically recorded in the User audit system log files.

Data transfers outwith the UK – DPA Sections 72 to 78 (Refer to Guidance Note 2 of the Part 2 Guidance Notes)

2.4.2 Will the data be held in or transferred to a country within the EU but outwith the UK?
☐ Yes – state below which country / countries below ☒ No – go to question 2.4.5
Click here to enter text
2.4.3 For what purpose is the data held in / transferred to the country / countries listed above? Include the legislation which governs the transfer of the data.
Click here to enter text
2.4.4 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Click here to enter text
2.4.5 Will the data be held in or transferred to a country outwith the UK and the EU?
☒ Yes – state below which country / countries below ☐ No – go to question 2.5.1
Non-Content data will be transferred to the USA For clarity, Content data will not be processed outwith the UK
2.4.6 For what purpose is the data held in / transferred to the country / countries listed above? Include the legislation which governs the transfer of the data.
Non-Content data will be transferred to the USA for the purposes of user access authentication to facilitate logon to DESC

2.4.7 What processes will be in place to ensure the data is adequately protected? This should include the means used to transfer the data, who will have access etc.
Non Content Data will be protected by the following: ▪ Contractual obligations on the supplier and its sub-processors. These are further defined in the Data Processing Agreements. ▪ Limitations on the retention of contact data ▪ Technical security controls agreed by the DESC ISO Gropu and documented in the Security Control Sheet For clarity, prior to Delivery 1 Pilot, the Data Controllers required the supplier to implement a closed loop support process to bring all technical support for Content Data into the UK.

Part 2, Section 5 – Other privacy legislation

2.5.1. Does the project involve the use of powers within any of the following? Check box as appropriate
☐ RIPA 2000
☐ RIP(S)A 2000
☐ IPA 2016
☒ None of the above

2.5.2 If any of the above apply, provide the relevant sections of the legislation
Whilst it is possible, in principle, for Content Data (evidence) gathered as a consequence of the use of the powers defined in 2.5.1 to be processed on DESC, for the Delivery 1 Pilot DESC will not be used as the storage or transfer mechanism between criminal justice partners and existing processes will be used. It is likely that a future assessment will be made on use of DESC for processing of evidence derived form these sources, however the sensitivity and risk associated with them will need to be taken into consideration in that assessment.

Human Rights Act 1998

2.5.3 Article 2 – Right to Life **Does the proposed process involve new or existing data processing that adversely impacts on an individual's right to life?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below
☒ No
Click here to enter text

2.5.4 Article 3 – Prohibition of torture **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be subjected to torture or inhuman or degrading treatment or punishment?** Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.5 Article 4 – Prohibition of slavery and forced labour
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be held in slavery or servitude or required to perform forced or compulsory labour. Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.6 Article 5 – Right to liberty and security
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to liberty and security? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.7 Article 6 – Right to a fair trial
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to a fair trial? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.8 Article 7 – Right to no punishment without law
Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right not to be held guilty of a criminal offence which did not constitute a criminal offence at the time was committed? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.9 Article 8 – Right to respect for private and family life

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to respect for his private and family life, his home and his correspondence? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

The Processors for DESC fall under the jurisdiction of the US Cloud Act, which in principle gives a legal gateway for evidence (Content Data) to be provided to the US Government without the knowledge of the Data Controllers of contracting authority. It is assessed that were this to happen, this would have an adverse impact on a data subject's right to respect private life, however there is engagement between law enforcement authorities though regular and routine governance channels when a case arises that may result in a request for information or evidence from DESC partners to be provided. Therefore it is assessed that it is unlikely that such an obligation will be imposed on the Data Processors.

This matter has been subject to review and external legal advice sought independently by all DESC partners. In addition, there has been engagement with and advice sought and received from ICO on the matter.

2.5.10 Article 9 – Right to freedom of thought, conscience and religion

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of thought, conscience and religion? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.11 Article 10 – Right to freedom of expression

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of expression? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below

☒ No

Click here to enter text

2.5.12 Article 11 – Right to freedom of assembly and association

Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of peaceful assembly and to freedom of association with others? Schedule 1 of the Human Rights Act (HRA) 1998)

☐ Yes – provide details below ☒ No
Click here to enter text
2.5.13 Article 12 – Right to marry **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to marry and found a family?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below ☒ No
Click here to enter text
2.5.14 Article 14 – Right to freedom of discrimination **Does the proposed processing involve new or existing data processing that adversely impacts on an individual's right to freedom of discrimination on any grounds?** Schedule 1 of the Human Rights Act (HRA) 1998)
☐ Yes – provide details below ☒ No
Click here to enter text

Consultation Process with Relevant Stakeholders

2.6.1 Do you intend to consult others either internally (e.g. business areas, staff associations, TUs etc. other information experts) or externally on the proposed processing?

☒ Yes

☐ No – If you do not intend to consult anyone, you must **justify** why consultation is not appropriate.

2.6.2 Who do you propose to consult on the proposed processing? List both internal and external organisations / individuals.

- Scottish Government
- Scottish Biometrics Commissioner
- Information Commissioner's Office
- Scottish Police Federation
- Association of Police Superintendents
- Unison
- Criminal Justice Partners
- COPFS Policy Division
- Defence Community, including Law Society of Scotland
- PCS/FDA Union
- COPFS Cyber security

2.6.3 When do you propose to consult with the above organisations / individuals?

- Scottish Government – ongoing basis throughout DESC delivery
- Scottish Biometrics Commissioner – November 2022
- Information Commissioner's Office – September 2022 and ongoing as required
- Scottish Police Federation – ongoing basis throughout DESC delivery
- Association of Police Superintendents – ongoing basis throughout DESC delivery
- Unison – ongoing basis throughout DESC delivery
- Defence Community including Law Society of Scotland –ongoing since start of 2022. COPFS to host presentations and feedback sessions in December 2022.
- PCS/FDA Union – ongoing and specifically in December 2022

2.6.4 How do you intend to consult with the above organisations / individuals?

SG and staff associations are represented at DESC Programme and Project Boards and are engaged throughout the delivery on specific matters.

A formal presentation to the Scottish Biometrics Commissioner's Advisory Board will be provided, consultation will continue according to questions arising thereafter

ICO has been engaged informally providing progress updates throughout DESC delivery. Advice has been sought on a specific matter in September 2022, through submission of a part of a DPIA, however this is not submitted using DPA18 s65

Part 2, Section 7 – Assessment and mitigation of risks posed by the proposed processing to the rights and freedoms of data subjects (Refer to Guidance Note 3 of the Part 2 Guidance Notes)

Risk(s) identified to the rights and freedoms of the data subject	**Probability and Impact Score and Risk Level**	**Mitigations**	**Probability and Impact Score and Risk Level after mitigations**	**Result:** The risk is: • Eliminated (E) • Reduced and Acceptable (R/A) • High/Very High and Acceptable (H/A)* • High / Very High and Not Acceptable (H/NA)*	**Evaluation:** Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
There is a risk that sub-processors engaged by the Supplier are not subject to the Terms & Conditions in Services Contract Reference 388514	Probability = 5 Impact = 5	▪ Due diligence assessment between DESC and Axon to review evidence form sub-processors and where sufficient authorise in writng. ▪ Engagement with Microsoft to discuss its terms and conditions to review compliance with DPA2018	Probability = 4 Impact = 5	H/A	The Data Controllers have escalated the risk to their SIROs and this has been accepted. Due diligence work will continue during Pilot to further reduce the probability scoring and in particular in relation to Microsoft and AWS where the support wider UK national organisations may be required.

		▪ Risk reviewed by the SIROs of each Data Controller			
There is a risk of the Submission, Processing and Retention of Non-Relevant Data	Probability = 3 Impact = 3	▪ Police Officers will provide advice to Members of the Public about what to submit. ▪ Police Officers can decline evidence submitted in error ▪ Each partner will review the Evidence and share only that Data considered relevant.	Probability = 1 Impact = 2	R/A	The mitigations allow data subjects, when submitting evidence, to limit processing to relevant data. Each stage of the processing sets out to reduce the impact on data subjects of processing of non-relevant data
Processing Law Enforcement Data using a Contractor and Sub-Processors which operate under the jurisdiction of the US Cloud Act	Probability = 1 Impact = 5	▪ Regular and routine engagement with US authorities on law enforcement matters ▪ Auditing by partners to identify activity (after the fact) ▪ Ongoing strategic engagement with ICO and Home Office to highlight impact	Probability = 1 Impact = 5	H/A	Law enforcement agencies routinely work together through formal channels, therefore whilst the likliehood of this legislation being applied to DESC data is low, the impact on data subjects remains high.

		▪ Risk reviewed by the SIROs of each Data Controller			
A scalable BAU solution for facilitating Data Subjects Rights requests has not been identified	Probability = 5 Impact = 3	An acceptable solution has been agreed for Delivery 1 Pilot The DESC Project will ensure a scalable solution is agreed before further rollout	Probability = 0 Impact = 3	Eliminated	The task is a managed activity for the DESC Programme, which will limit the probability of this risk occurring. Once in place this risk will be fully eliminated.
The BAU system administration, including ongoing monitoring and management of risk mitigations has not been identified	Probability = 5 Impact = 3	The DESC Project will ensure a scalable solution is agreed and implemented before closing the Project	Probability = 1 Impact = 1	Eliminated	The risk mitigation during pilot will ensure a scalable solution is in place prior to future rollout
There is a known defect which will not be resolved prior to Pilot, resulting in contact details for Data Subjects being held in Axon Citizen longer than is necessary	Probability = 5 Impact = 3	A defect has been raised and Axon is working on a resolution with a timeline of c. 8 weeks.	Probability = 5 Impact = 1	R/A	The resolution timeline has already commenced and once implemented will fully eliminate the risk
There is a risk that DP by Design will not be baked into future DESC development due to resourcing issues in the Project.	Probability = 5 Impact = 5	The matter has been raised DESC Programe Board to appropriately resource the work during Pilot.	Probability = 1 Impact = 1	R/A	The impact on individuals will be minimised as Data Controllers will be required to adequately resource the work of the DESC Pilot

Once Part 2 of the DPIA is complete it must be reviewed by the DESC DPWG and the DPOs of all 5 (five) Data Controllers to ensure the legal requirements are met. Once satisfied that all legal requirements have been met, they will sign it and return it to the project.

*If following mitigations, the risk to the rights and freedoms of individuals remains high, processing cannot commence without the agreement of the Information Commissioner.

Approval of DPIA

Name: [redacted] on behalf of the DESC Data Protection Working Group

Signature: [redacted]

Date: 19/01/2023

Comments / Observations: Approved subject to ongoing management of the noted controls and mitigations and risk action plans agreed with SIROs

Senior Responsible Officer: (Before signing – See Guidance Note 4 in Part 2 of the Guidance Notes)

Name:

Signature:

Date:

Comments / Observations:

Appendix 1a DESC Overview Presentation
Appendix 1b D Div DESC 1 Page
Appendix 2 Data Jointly Controlled – Linear flow