SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

2 Clyde Gateway
French Street
Glasgow
G40 4EH

LETTER SENT BY EMAIL ONLY

15 July 2025

FOI Ref 2025/26-032

Request

Your request for information dated 17 June 2025 is copied below.

Given the recent passing of the Data (Use and Access Bill) in Parliament, the radical changes it introduces for Law Enforcement data processing, and the elapsed time since I last sought information on the status of the DESC programme and its legal compliance with the existing DPA 2018 Act, I wish to request information on the programme status.

This will allow the creation of a baseline to measure changes over time as a result of the new bill once Royal Assent is given; which I feel is a reasonable endeavour of significant public interest due to the nature of risks to subjects interests and cost to the public purse.
I request you apply this context into any public interest test weighted exemption you may seek to apply.

This FOISA request is part of a batch sent to all DESC participants on the same date, but I seek individual responses from each DESC participant and not collaborative ones.

The information I require is as follows:

1 - The latest in force Data Protection Impact Assessment conducted under S.64 of the DPA 2018 (the Act) by the Authority for your participation in DESC if one is held.

2 - Copies of any communication made under S.65 between the Authority and the Commissioner in respect of identified high risks to the rights and interests of an individual over the past 12 months.
This may logically include draft DPIA's and materials under preparation, or not included in the current in force DPIA.

3- Copies of any other communications between the Authority and the Commissioner over the last 12 months relating to any identified risks in relation to offshore (i.e. non-UK located, or remotely initiated) processing by any processor or sub-processor - whether or not these were communicated to the Commissioner under S.65.

4 - Copies of any communications between the Authority and Microsoft, or the Authority and Axon (both being previously identified as Authority data processors) over the past 12 months in relation to their processing of personal data covered under Part 3 of the DPA 2018 (i.e. relating to the processing of personal data processed for a Law Enforcement purpose). NB: This may logically include information relating to services outside of the DESC service itself, such as M365 or general Azure services (Microsoft), or body-worn video, etc. (Axon), that the Authority may already consume or intend to consume for Law Enforcement processing purposes.

Response

The Scottish Police Authority has considered your request under the Freedom of Information (Scotland) Act (FOISA).

In terms of parts one and two of your request, the Authority does not hold information.[1]

By means of explanation, a decision was taken in Quarter one of 2024-25 that the Authority would not have a tenant in DESC. As such the Data Protection Impact Assessment (DPIA) was retired and has not changed since previously disclosed.[2]

We can also confirm that there has been no further communications between the Authority and Axon or Microsoft in respect of DESC.

In terms of part three of your request, the Authority can confirm that information is held. Communications with the Information Commissioner in terms of S65 of the Data Protection Act 2018 are attached as is the abridged M365 Data Protection Impact Assessment (DPIA), as sent to ICO, and the full DPIA. Please note that this is the DPIA at the time of your request. Given that the Data Use and Access Bill referred to in the DPIA has now been passed and received royal assent, the DPIA will be subject to review.

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

[2] let-20230306-foi-response-2023-015-for-dl.pdf

In terms of part four of your request, the Authority's Information Management Lead has been involved in formulating questions for Microsoft regarding M365. This correspondence is attached.

Some information has been redacted from correspondence and the DPIAs where this is third-party personal data.[3] This exemption is absolute and does not require application of the public interest test. While you may have a legitimate interest in disclosure of this information, it is our view that those interests are overridden by the interests or fundamental rights and freedoms of the data subjects.

Right to Review

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

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

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

This response will be posted to our Disclosure Log after seven days.

Yours faithfully

Scottish Police Authority

[3] This is a notice in terms of Section 38(1)(b) of FOISA - Third party data. Disclosure would contravene the data protection principle in Article 5(1)(a) of the General Data Protection Regulation: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

Scottish Police Authority
Clyde Gateway
2 French Street
Dalmarnock
Glasgow
G40 4EH

By email

15 May 2025

Dear Lindsey,

DPIA – Microsoft Office 365

The following is the Information Commissioner's response to the Scottish Police Authority (SPA) Data Protection Impact Assessment (DPIA) submission of 3 April 2025 under Section 65 of the Data Protection Act 2018 (DPA18).

The DPIA relates to the implementation of Microsoft Office 365 (M365) in a cloud based environment for a high volume of the data processing carried out by SPA and Police Scotland (PSoS). It identifies residual high risks relating to an inability to determine compliance with Part 3 of DPA18, particularly Section 59, the implications of the US Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018, and a lack of safeguards for the processing of Article 10 data and data processed outside of the UK.

The DPIA was accepted for prior consultation due to the identification of residual high risks, which per the DPO advice summary, may cause harm to individuals, and the description of potential infringements of the legislation. Upon review of the DPIA, while a general description of the processing is provided, it lacks sufficient detail for the Commissioner to form an opinion on whether the intended processing would infringe the legislation, which should be articulated more clearly with respect to individuals' rights and freedoms. The DPIA or accompanying correspondence also do not contain sufficient information to determine whether Section 65(1) has been met.

Nevertheless, we provide the following recommendations for improving the deficiencies within the DPIA, and on the residual high risks identified.

For clarity, where we say **must**, this means you're required to do this by law. **Should** doesn't refer to a legal requirement. But it's what we expect you to do, unless there's a good reason not to. If you choose to take a different approach, you must be able to demonstrate this also complies with the law. **Could** refers to an option or example you could consider to help you comply with the law effectively.

The Data (Use and Access) Bill

The DPIA makes several references to The Data (Use and Access) Bill, in particular seeking to assess how compliance may be affected when the new legislation is enacted. Our advice focusses on the requirements of, and mitigations available under, the legislation as it currently stands. Guidance on compliance with the new legislation will be published once the content is finalised and the Bill receives Royal Assent.

Summary of recommendations

1. You **should** revisit your DPIA and include sufficient detail to ensure an effective assessment of the impact of the processing on the protection of personal data. In particular:
    a. Further detail **should** be provided about the general processing operation, with acronyms and concepts explained;
    b. You **should** detail more clearly the relationship between SPA and PSoS, their respective roles and responsibilities in relation to this processing;
    c. You **must** consider how you will provide for data subject rights in the M365 environment;
    d. You **should** more clearly articulate the identified risks in terms of the risks to the rights and freedoms of data subjects within your risk assessment;
    e. You **should** include within your risk assessment further explanation of the implications of the risks, the mitigations and how these are intended to work in practice, and how the severity of the harm has been decided; and

f. You **should** separate your assessment into Part 2 and Part 3 processing, to clarify when each regime applies, the implications of such, and to demonstrate compliance with each regime.

2. We recommend referring to the letters of 2 April 2024 from Emily Keaney and Jenny Brotchie for guidance on the compliance of cloud services with Part 3 of the DPA18, and the ICO's view on the CLOUD Act.
3. Your DPIA **should** include further detail regarding the security measures, assurances and functionalities of the M365 product, and your assessment of how these affect the risk posed to individuals.
4. You **must** satisfy yourself that risks have been mitigated to acceptable levels and that you are able to demonstrate compliance with the data protection legislation before you proceed with any processing of personal data.

DPIA content and structure

We recognise that the principal concerns around the processing relate to compliance with Part 3 of the DPA18, and this is where the DPIA focusses. Considering the extent of the previous correspondence between the ICO and the controllers on this matter and similar processing activities, we acknowledge it is likely the content of the DPIA does not reflect the complete assessment that may have been carried out, by either SPA or PSoS.

However, there are several areas in which the DPIA is deficient, and lacks enough detail to allow the Commissioner to assess whether the envisaged processing would infringe any part of the legislation. In addition, the absence of any supporting material to support the submission requirement under Section 65(1) DPA18 does not allow us to properly asses whether the criteria for prior consultation has been met.

We provide the following brief observations, with recommendations for improvement.

General description of processing

The description of processing should be clearer, providing further detail about which data will be processed on particular systems, under the controllership of which organisation(s). There are acronyms which are unexplained ie NEP, and concepts such as a 'service back' and 'weeding' which require further explanation.

Controllership

Further detail on the controllership arrangement, the relationship between SPA and PSoS, and their respective roles and responsibilities in relation to the processing should be provided. The DPIA does not include sufficient information to understand the interaction between SPA and PSoS, and the systems on which the data will be processed.

As a project with joint controllership, we also note the DPIA does not include any assessment that may have been conducted by PSoS, although you have provided confirmation that they have had sight of the DPIA and are aware of the submission. Both controllers must assure themselves that a comprehensive risk assessment has been carried out and documented, and that the risks of the processing have been identified and mitigated to acceptable levels.

Data subjects rights

The DPIA does not include any consideration of the rights of the data subject, or detail any possible risk to the ability to exercise these rights. You must consider how the implementation of M365 may affect individuals exercising their rights, whether the product allows for the effective exercise of rights, and how you will provide for these rights considering any process or procedure change that may be necessary.

Risk assessment

The risk assessment should more clearly articulate the risks in terms of risk to the rights and freedoms of data subjects. The identified risks focus on the compliance of the processing with the legislation, without considering the perspective of data subjects. The data to be processed is wide ranging, and the risk assessment does not include an analysis of the

different categories of data involved, or the different categories of data subject who might be affected.

The risks and implications should be further explained, along with how the mitigations identified are to work in practice. There is a lack of explanation of how the severity of harm has been assessed, particularly due to the lack of focus on how technical deficiencies could lead to harm to individuals.

Part 2 and Part 3 processing

The DPIA was submitted under Section 65 of Part 3 of the DPA18, however describes processing that will take place under both Part 2 and Part 3 of the DPA18. The DPIA lacks clarity around when each regime will apply, the implications of such, and whether the obligations and compliance under UK GDPR have been fully considered. The DPIA would benefit from a separation of the envisaged processing into Part 2 and Part 3 assessments, to ensure compliance under both regimes has been considered and can be demonstrated.

Residual high risks

The description of the high risk to data subjects is largely confined to the summary of the DPO advice, though some risk could be inferred. Each risk should be articulated in regard to the impact on individuals' rights and freedoms for an effective assessment of the risks of the processing on the protection of personal data. This notwithstanding, we provide the following advice on the high risks identified per our previous correspondence on similar matters, and to aid your compliance.

Compliance with Part 3 and Section 59

The DPIA makes a number of references to concerns over the compliance of hyperscale cloud services with Part 3 of the DPA18, with the risk assessment concluding that the use of such providers is not currently compliant with the legislation.

As advised in the letter of 2 April 2024 from Deputy Commissioner Emily Keaney, it is our view that law enforcement agencies may use cloud service providers that process data outside of the UK in accordance with

Part 3 of the DPA18, providing they have appropriate protections in place. We advise in this letter that the IDTA or the Addendum to the EU SCCs (the "Addendum") are capable of meeting the requirements of Section 75.

The first residual high risk identified highlights a concern with compliance with Section 59 in particular, regarding the use of sub-processors. The risk assessment does not specify which information Microsoft have not provided, however there is reference elsewhere in the DPIA to a refusal to provide the specific countries where your data may be processed, and to provide International Data Transfer Agreements due to confidentiality.

Your obligation as a controller is to be satisfied that there are guarantees of appropriate technical and organisational measures which meet the requirements of Part 3 and to protect the rights of the data subjects. If you cannot identify the specific sub-processors that will be used, you should assume all sub-processors listed by Microsoft will be used as part of your processing, and put appropriate mitigations and safeguards in place.

The letter dated 2 April 2024 from Emily Keaney sets out a number of questions to consider as part of your due diligence, and makes suggestions of further checks which may be proportionate, such as carrying out your own transfer risk assessment for the transfers of personal data made by a cloud service provider.

The CLOUD Act

The DPIA identifies the CLOUD Act as a risk, although it does not articulate this risk in terms of the potential impact on individuals.

Similarly to the above risk, the letter of 2 April 2024 from Jenny Brotchie sets out that we do not consider that organisations (including competent authorities operating under Part 3 Data Protection Act 2018) must stop using cloud services because of concerns over the CLOUD Act and data protection compliance. The CLOUD Act does not alter an organisation's obligations under data protection law. We recommend that you revisit the advice set out in the letter of 2 April when assessing this risk.

Lack of safeguards for Article 10 data

The DPIA identifies a concern that within Microsoft's own risk factors, they state that the M365 product was not designed to process special categories of data on a large scale. This risk is articulated as a lack of safeguards for Article 10 data and processing of data outside of the UK.

The DPIA mentions briefly some of the security measures that Microsoft have in place, such as multifactor authentication, encryption at rest and in transit, and data recovery. It does not go into detail regarding these measures, or provide any assessment of these measures.

It appears that Microsoft consider there are avenues for Article 10 data to be processed within M365. Within the same guidance where this risk factor is stated, Microsoft advise that the product can be used for this processing, and references the highly customisable nature of the product. It is not clear to what extent the functionality, security measures, and safeguards that are available within the M365 product have been explored, as these are not detailed within the DPIA. The DPIA also does not explain or interrogate any contractual commitments or assurances from Microsoft.

The DPIA does identify one mitigation of encrypting the data and holding the key. The mitigation is not explained further nor any information provided on how this would work in practice. It is stated that this mitigation poses risks of its own, however these are not detailed.

You should explore more thoroughly within your assessment the safeguards that can be put into place through customisation of the M365 product, the technical and organisational measures Microsoft have in place, any contractual commitments from Microsoft, and any other reasonable measures that can be carried out. You should detail your assessment of these measures, including further detail regarding possible encryption, and how this affects the risk level.

Risks do not need to be entirely eliminated for the processing to proceed. Your obligation as controller is to satisfy yourself that the risks have been mitigated to an acceptable level in the circumstances of the processing, considering the intended benefits and the difficulties of mitigation.

Status of our advice

It should be noted that this advice is without prejudice to any future intervention by the Commissioner in accordance with his tasks and powers, in line with his Regulatory Action Policy. It should not be considered as legal advice or endorsement of any product or processing operation.

Next steps

This concludes our advice on your DPIA as submitted. As recommended, you should revisit your DPIA, ensure sufficient detail is included and address the deficiencies as advised. We recognise that following receipt of the advice, you may consider some or all of the high risks currently identified to be able to mitigated further. Should your revised DPIA not identify any residual high risks, you will not need to submit this to the ICO for prior consultation under either Section 65 DPA18 or Article 36 UK GDPR.

Please note if in the future the ICO has grounds to suspect the controllers are not complying with data protection law, any failure to follow the recommendations set out in this letter may be taken into account as an aggravating factor in deciding whether to take enforcement action. Please see page 11 of our Regulatory Action Policy.

We are aware that your DPIA relates to an ongoing engagement with our colleagues in the Scottish Affairs office, who will be happy to keep you updated as we prepare relevant guidance under DUA and to consider any further questions you have.

The ICO has a duty to assess and report on the economic impact of its regulatory activity, and in due course we will also seek your feedback on the impact of your engagement with us via a short questionnaire.

FOI and publicity statement

Please be aware that we are a public authority subject to the laws we regulate, such as the Freedom of Information Act 2000. You may also wish to be aware of our Communicating our Regulatory and Enforcement

Activity Policy, which describes the kind of information we may publish or disclose, such as our formal regulatory outcomes, where this will assist in the promotion of good practice and deter non-compliance.

Intention to publish

We encourage controllers to publish their DPIAs as a tool to demonstrate transparency and to build trust and confidence. Please let us know whether you intend to publish your DPIA in this instance.

Yours sincerely

Catie Galgut, Senior Policy Officer, Data Protection Impact Assessments

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018, and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

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

SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Data Protection Impact Assessment – Microsoft Office 365 (M365)

Step 1: Identify the need for a DPIA

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

The project relates to the implementation of M365, delivered and managed by PSoS, to SPA.

M365 includes Email (outlook), SharePoint, OneDrive and Teams.

The processing will be high volume, high value (all SPA and PSoS staff) and will include data subject to UK GDPR and volume data subject to Part 3 DPA (Law Enforcement). It will also include special category data such as biometrics.

The move to a cloud-based environment means that SPA and Police Scotland information and user credentials will be stored on infrastructure provided by Microsoft (Microsoft 365 and associated Microsoft cloud services) and Amazon Web Services (SailPoint Identity Access Management) which may present privacy concerns.

Step 2: Describe the processing

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

ICT is a service back from Police Scotland (PSoS), thus a shared infrastructure exists. This will have the effect of joint controllership/processing. In addition, PSoS also provides a service back in areas such as fleet, estates, finance, and HR. Thus, PSoS will also be processing data as a data processor for SPA.

The data which will be processed can originate from SPA, partners, or members of the public (email). The solution will not change the personal data that is processed by SPA. The O365/NEP approach will store information using a hybrid cloud solution provided by Microsoft. Certain information will continue to be stored locally on Police Scotland's existing IT infrastructure.

Initially core apps such as Word, Excel and PowerPoint will stay on the shared drive. Linkages to the Cloud have been disabled. Where this changes the DPIA will be revised.

PSoS has undertaken consultation with their Cyber Security and Assurance (CSA) Manager, Chief Digital Information Officer, ICT Chief Operating Officer, Chief Technology Officer, Head of Service Delivery (Digital Division), Information Security Manager (ISM), and the Records Manager (RM).

SPA Information Management Lead has also been consulted in terms of the risks/issues.

The data will be OFFICIAL and OFFICIAL SENSITIVE. High risk data such as victim/offender and special category data will be processed.

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

There is no intended effect on individuals.

Benefits

The NEP is an innovative programme and solution. It will enable significant strategic changes in the working methods of PSoS and SPA, delivering more efficient and collaborative ways of working between partners.

The O365/NEP solution is intended to take advantage of the enhanced security features which modern technology working practices can provide. The NEP will also deliver new technology in connection with the three national solutions, i.e.

Productivity Services:

- Exchange Online
- M365 Apps for Enterprise
- Teams
- SharePoint Online
- OneDrive for Business
- Power Platform

Access to:

- Bookings
- Delve
- Forms
- Planner
- Sway
- To Do
- Whiteboard
- Viva Engage

Identity Access Management Solution (IAM) – SailPoint IdentityNow:

A platform providing a distributed method to request and approve access rights (i.e. the ability to sign-in to applications as well as the level of access to functionality within them or to data sources).

National Management Centre (NMC):

Delivering a nationally coordinated monitoring, response, and remediation capability in order to protect all UK Police Forces and SPA from cyber threats.

Cloud Benefits

Cloud working comes with an elevated level of scalability and resilience not typically found within on-premises hosted solutions. Microsoft is the industry leader in cloud technology offerings and is at the forefront of technological developments in the cloud space.

Provision on an automated IAM solution that will eventually replace the semi-automated process in place today.

Provision of a 24/7 fully managed cyber threat protection solution.

Scope of Processing

Categories of Data Subjects

☒ Victims

☒ Witnesses

☒ Suspect

☒ Accused

☒ Person convicted on an offence.

☒ Children or vulnerable individuals – provide details below.

☒ Police officers

☒ Police staff

☒ Other – provide details below.

The types and categories of personal data processed will depend on the content of the information input to the system by SPA and PSoS staff. As email will be included SPA has no control over what data may be sent via email to us.

The personal data which will be processed using the solution includes data relating to employees, contractors, and suppliers. It also includes information relating to live policing matters.

The solution could be used to process personal data including:

- Personal details of staff/suspects/offenders/witnesses/victims (e.g. name, address, email address, telephone number, car registration number, national insurance number, passport, driving licences).
- System usage details relating to staff usage of the system.

- Family, lifestyle, and social circumstances of staff/suspects/offenders/witnesses/victims
- Education and training details of staff.
- Employment details of staff.
- Online identifiers (e.g. internet protocol addresses, cookies identifiers) of staff.
- Financial details (e.g. bank account details) of staff/suspects/offenders.
- Criminal records, offences (including alleged offences) and criminal proceedings, outcomes, and sentences of suspects/offenders.
- Legal proceedings about suspects/offenders.
- Data on children where children are witnesses or victims.
- Special categories of personal data, including data on disabilities, health records, religious or philosophical beliefs, trade union membership, relating to staff/suspects/offenders/witnesses/victims

There is no control over what might be emailed by members of the public, but in most cases the data will fall into one of the above categories. It should be noted that the above list is not exhaustive, and that by the nature of the solution and the scope of the IT systems with which it interfaces, the categories of personal data which may be processed via the solution is very wide. In conclusion, any data processed by SPA may be in scope.

Sources of Data

Data will primarily be provided by data subjects themselves, whether that be employees, partners, or members of the public.

The relationship with individuals therefore varies depending on the processing. In some cases, the relationship will be one of employer to employee, in others it is customer to supplier and in others (i.e. investigations) it will be Police force, victim, witness, suspect or convicted criminal.

Categories of Data

As above, the categories will depend on the content input or received from 3rd parties (such as emails).

It is likely to include.

- Personal details of staff/suspects/offenders/witnesses/victims (e.g. name, address, email address, telephone number, car registration number, national insurance number, passport, driving licences).
- System usage details relating to staff usage of the system.
- Family, lifestyle, and social circumstances of staff/suspects/offenders/witnesses/victims
- Education and training details of staff.
- Employment details of staff.

- Online identifiers (e.g. internet protocol addresses, cookies identifiers) of staff.
- Financial details (e.g. bank account details) of staff
- Criminal records, offences (including alleged offences) and criminal proceedings, outcomes, and sentences of suspects/offenders.
- Legal proceedings about suspects/offenders.
- Data on children where children are witnesses or victims.
- Special categories of personal data, including data on disabilities, health records, religious or philosophical beliefs, trade union membership, relating to staff/suspects/offenders/witnesses/victims.

Will Special Category or Criminal Conviction Data be Processed?

The following data may be processed.

- Race or ethnic origin.
- Sex Life
- Religion
- Trade Union Membership
- Genetic Data
- Biometric Data
- Sexual Orientation
- Health
- Criminal Conviction

The way data is shared will not change with the implementation of the solution.

All the data to be processed is already being processed. There will be no additional processing that does not already occur.

AS SPA provides a service via Forensic Services to the whole of Scotland it is not possible to quantify the volume of data subjects.

Prior Concerns over the Processing

There are prior concerns around the use of MS Hyperscale Cloud and compliance with Part 3 of the DPA 2018. These were surfaced during the DESC project and extend to O365. There have been several media articles on the subject. Thus, it is assessed that there may be High risks to the rights and freedoms of Data Subjects.

The concerns are predominantly in-house but should any of the risks materialise then that position could quickly change to a lack of public confidence.

Step 3: Consultation Process

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

The actual data being processed will not change; it's the use of Cloud that prompts the DPIA.

Cloud processing is widely used in the public sector and is used by all Police Forces in England and Wales. There has been no indication of any public concern in this area. Thus, consultation beyond internal experts and stakeholders will not take place.

There have been discussions with MS Legal, PSoS IM and ICT, PSoS Records Manager and DPO and SPA staff and managers, including the SIRO.

Step 4: Assess Necessity and Proportionality

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

The GDPR Principles Article 5

1st Principle – Lawful, fair and transparent

A lawful basis has been identified for all processing. Where required an appropriate policy document is in place. Privacy Notices are available on SPA's Internet page.

Data Subject requests are processed within the statutory provisions/timescales. Information is available to data subjects via the SPA Internet page.

2nd Principle – Specific, explicit, and legitimate purpose

The data to be processed/shared originates, in the main, from SPA or Police Scotland. The solution will not change the scope/purpose of current processing, nor will it be used for a different purpose.

The requirements of the UK GDPR and DPA 2018 will be met. Article 6 of the DPA will be met. Where Special Category Data is processed the requirements in Article 6, 9 and Schedule 1 of the DPA will be met.

3rd Principle – Adequate, relevant, limited to what is necessary.

There will be no change to the purpose of the processing. Existing controls will remain in place, including data audits/weeding/training, to ensure this principle is met.

4th Principle – Accurate and kept up to date where necessary.

The existing controls in this area will be maintained and, through time, enhanced through better data insight and sharing of identity information to allow the effective use of IAM through the IdentifyNow platform. This will ensure changes are pushed out to any relevant connected systems.

5th Principle – Not kept longer than necessary.

Data audits will continue to be undertaken. The Data Governance Project in SPA has looked at all non-application data, such as email and SharePoint and a strategy is now in place for the management and ongoing weeding of those sources.

Within the design blueprint for the **Productivity Services (1)** solution it details a baseline retention policy for the following elements.

- Exchange Online
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 groups
- Exchange public folders
- Microsoft Teams (Chats and Channel Messages)

Discussion will take place with PSoS records management prior to the implementation of weeding in the elements noted under the Productivity Services solution.

It is understood that the guiding principles will come from the Police Scotland data retention SOP, and the NEP guidelines. However, neither of those apply to SPA who have a separate Records Retention SOP. Thus, PSoS will need to consult with SPA prior to implementing weeding and retention.

6th Principle – Appropriate Security

Data sharing will only take place where there is a legitimate or lawful purpose. A LIA and/or Data Sharing agreement will be in place for al relevant sharing.

SailPoint IdentityNow has a full RBAC system. As part of the implementation Multi Factor Authentication (MFA) will be configured between the M365 tenant and the existing Azure AD tenant.

Any changes to permissions have to be requested via SPA IM.

Appropriate SOPs/SyOPs are agreed.

The data will reside on the MS infrastructure and as such MS also has responsibility to ensure compliance with this principle in terms of our data. This will include encryption at rest and in transit, data recovery and notification of any incidents involving our data.

SailPoint will be used for business continuity and DR as well as back-ups, which will be UK based.

Data may be transferred or processed outside the UK in the form of Microsoft's processing, particularly for their support model that uses a 'follow the sun' model. MS has disclosed volume sub-processors outside the UK but will not confirm what processors may be used for our processing. Furthermore, CLOUD Act and FISA 702 could result in our data being processed in the USA without our knowledge. Data GEO should be configured to UK.

Step 5: Identify any Risks

Record the detail of any risks, providing as much information as possible.

1. There is a risk that PSoS will implement weeding/retention or other controls without consulting SPA.

2. There is a risk that once deployed PSoS will fail to keep SPA advised of ongoing matters, including risks and issues.

3. There is currently a risk with the use of Hyperscale Cloud providers for processing Law Enforcement data. Such use does not currently comply with Part 3 of the DPA.

    - Compliance with S59
    - Transfer of data to processors in high-risk countries
    - Cloud Act
    - FISA S702

    Microsoft has declined to share with SPA the specific countries where our data may be processed. They have instead pointed to their list of sub-processors. Out-with Europe none of those have adequacy for Law Enforcement data and Some have no adequacy and may be deemed as 'hostile' countries.

    Microsoft will not confirm if our data will be processed in any of those countries, which includes China. They have also declined, due to confidentiality, to provide SPA with the assurances it needs for those transfers, including International Data Transfer Assessments.

    Microsoft does not believe that the controls in Part 3 of the DPA apply to them.

    The Cloud Act remains a threat to SPA data given the powers that it confers For the USA to order Microsoft, via a court order, to provide them with our data. The CLOUD Act also allows for a gagging order so that Microsoft cannot disclose requests to us.

    Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorises intelligence collection on foreign intelligence targets located overseas. This could include access to data processed in Microsoft Cloud.
    Europeans, forget the US Cloud Act… worry about FISA instead (!)

Microsoft makes the following statement in respect of the risk factor for processing on a large scale of special categories of data in Office 365: "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or of personal data relating to criminal convictions and offenses".*

Office 365 is not designed to process special categories of personal data on a large scale.

When asked to explain the reason for this narrative, the Microsoft position was that the controls required for Part 3 data are not inherent in the product and it would be for the customer to ensure the required controls were implemented.

4. There is a risk that the Data Use & Access Bill (DUAB) will be deemed to have sanctioned anti-competitive measures by changing the UK Data Protection Legislation primarily to accommodate Hyperscale Cloud providers. If the Bill (or Act) were to be struck down, then the position would revert to non-compliant processing. It would be hard to argue otherwise given that the Bill specifically changes the elements of concern highlighted by SPA during DESC.

5. There is a risk that, by using MS Cloud before the DUAB received royal assent that SPA/PSoS will be seen to be giving Microsoft 'special' treatment.

   Microsoft have declined to provide the information that we need to assess compliance with S59 of the DPA. They also have sub-processors in hostile nations including China. If any other company had declined to tell us who processes what data of ours and where and further declined to provide the evidence of IDTA's or SCC's we would, in all likelihood, not progress with a tender bid.

   An example of this would be the DESC project. Axon was required to provide the data of all sub-processors and show us IDTA's and SCC's. SPA was vindicated in this requirement when it became clear they had not undertaken an IDTA and some of their SCC's were unsigned or pre-dated the 2018 legislation. Thus, it could be argued that Axon was treated differently from Microsoft, who may be seen to be receiving preferential treatment.

6. There is a risk that, after DUAB receives Royal Assent, Microsoft may not agree to sign up to the Code of Conduct required by the legislation. The Code of Conduct will be based on S59 requirements. Given that Microsoft currently believe that the requirements in S59 are for us to comply with and not them, they may decline to sign a Code of Conduct in this respect.

UK law enforcement data adequacy at risk | Computer Weekly
Reassessing UK law enforcement data adequacy | Computer Weekly

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Remote 2. Unlikely 3. Possible 4. Likely 5. Certain	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low: 1-6 Med: 7-12 High: 13-18 Extreme: 19-25		Eliminated Reduced Accepted		Yes No
1	There is a risk that PSoS will implement weeding/retention or other controls in O365 without consulting SPA or fail to advise of relevant issues.	3	3	9 Medium	Ensure ongoing dialogue with PSoS IA and ISO to ensure that SPA is sighted on any material changes/decisions in terms of the deployment, use and functionality of O365	Reduced	Low	
2	Office 365 does not offer back up for data (not to be confused with Geo redundancy).	5	4	20 Extremely High	PSoS will need to deliver back up (and any additional services required) in time for go live	Eliminated	N/A	
	There is currently a risk with the use of Hyperscale Cloud providers for processing Law Enforcement data. Such use does not currently comply with Part 3 of the DPA.							
3(a)	Microsoft will not provide the information necessary for SPA to be able to determine compliance with Part 3 and in particular S59 and the use of sub-processors.	5	3	15 High	No mitigation, although signing the proposed Code of Conduct may be a future mitigation.	No change	High	

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Remote 2. Unlikely 3. Possible 4. Likely 5. Certain	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low: 1-6 Med: 7-12 High: 13-18 Extreme: 19-25		Eliminated Reduced Accepted		Yes No
3(b)	Microsoft will not confirm if our data will be processed in any 'hostile' countries or countries without adequacy, which includes China. They have also declined, due to confidentiality, to provide SPA with the assurances it needs for those transfers, including International Data Transfer Assessments.	5	3	15 High	Microsoft support engineers requiring access to user data must first submit a lockbox data request. This can only be approved by M365 administrators. Whilst this reduces the probability, the impact may still be significant. The GEO for 365 should also be set to UK.	Reduced	Medium	
3(c)	Microsoft does not believe that the controls in Part 3 of the DPA apply to them. Failing to comply with the controls means they may be deemed to be acting as a Controller.	3	3	9 Medium	No mitigation, although signing the proposed Code of Conduct may be a future mitigation.	No change	Medium	
3(d)	The CLOUD Act remains a threat given the ability for the USA to require MS to provide them with our data in response to a Court Order. The Order could include a gagging clause meaning we would be unsighted and unable to challenge.	3	5	15 High	There is evidence that Microsoft will challenge requests where appropriate and will always act in the customers interests. However, they will be unable to consult with or advise us where a gagging order has been issued. The risk remains High	No change	High	

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Remote 2. Unlikely 3. Possible 4. Likely 5. Certain	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low: 1-6 Med: 7-12 High: 13-18 Extreme: 19-25		Eliminated Reduced Accepted		Yes No
					due to the implications should the threat materialise.			
3(e)	Section 702 of FISA is a risk given the more covert aspect of requests in this area. Current tensions between the UK/Europe and the USA give rise to concerns about the use of FISA	3	3	9 Medium	A mitigation would be to encrypt our data and hold the key, however, this comes with its own risks.	No Change	Medium	No
3(f)	Microsoft states in their own risk factors that O365 is not designed for processing the data that will be ingested by SPA. Specifically, the lack of safeguards for Article 10 data & processing of data outside the UK	5	4	20 Extremely High	A mitigation would be to encrypt our data and hold the key, however, this comes with its own risks.	No Change	Extremely High	No
4	There is a risk that the DUAB will be challenged when enacted. If this were to materialise and the Bill/Legislation struck down, then we would revert back to the 'Part 3 Non-compliant' risk.	3	4	12 Medium	No mitigation	No change	Medium	

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Remote 2. Unlikely 3. Possible 4. Likely 5. Certain	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low: 1-6 Med: 7-12 High: 13-18 Extreme: 19-25		Eliminated Reduced Accepted		Yes No
5	If the DUAB does not receive Royal Assent before O365 is deployed, then the processing would not be legal (given that DUAB makes changes to Part 3 specifically for this purpose).	4	3	12 Medium	Delay deployment until DUAB has received Royal Assent	Eliminated	Medium	No
6	DUAB will only resolve the risk if MS agrees to sign up to the Code of Conduct. If MS declines to do this, which is a possibility given their view that Part 3 does not apply to them, then the processing will remain non-compliant.	3	4	12 Medium	If Microsoft agrees to the Code of Conduct this risk may be eliminated.		Medium	

Step 7: Sign off and Record Outcomes		
Name of system/Project: MS Office 365	**Date:** 2 April 2025	**Agreed actions** • Submit DPIA to ICO under S65 DPA • Seek view from ICO around Code of Conduct importance. • Advise PSoS that we have reservations about the legality, but understand the need for progress, leaving them to make the final decision. • Ensure a programme of education in SPA to reduce the risk by training staff about what they should and should not be using the MS applications for
Remediation approved by:		
Residual risks approved by:		The IM Lead is not seeking agreement at this stage. These may be reviewed after submission to ICO.
DPO advice provided by: [redacted], IM Lead		DPO must advise on compliance, Step 6 measures and whether processing can proceed. The evidence tends to suggest that the risks, whilst valid (or the legislation would not be changing), have not materialised in any of the deployments of O365 in numerous public sector organisations processing High Value data. As PSoS processes significantly more data than SPA and has greater risk, the final decision may be left to PSoS, whilst highlighting our view that we need to keep one eye on the ball as things could change quickly.

Summary of DPO advice:

SPA must never lose sight of the most serious risk, loss of life. Any decisions must be balanced between the need for progression and the protection of data subjects. Information being processed by SPA could result in serious risks for data subjects. Accordingly, all decisions must be taken with this in mind. That is not to say we cannot accept risk…simply that the benefit must outweigh the risk and the probability of the risk must be within appetite.

Many of the risks in O365 will be eliminated or reduced if the Data Use & Access Bill (DUAB) passes and MS agree to a Code of Conduct. There are reasons to proceed, primarily as NEP/PDS and NPCC are pushing forward with developing sharing using O365. Criticism could be levied if we fail to keep up with this approach…cautiously. It may also be the case that loss of life occurs due to our failure to keep up to date with systems allowing us to manage and share data more effectively.

SPA is a late adopter of Office 365. The reason for that is the due diligence that we have undertaken. We are aware of the risks and issues, and, in my opinion, we are in a better position than most organisations using O365 in that we have poured through MS documentation to better understand the product and undertaken consultation with both Microsoft and ICO to understand the landscape and risks/benefits. We are not simply looking to deploy the product because other Forces have done it.

The risk has, to an extent, to be balanced with the benefits. Whilst there are a number of technical legislative risks, the Home Office, ICO and Policing have been using MS Cloud for some years now without issue. That does not mean its legal, however, it serves as an indication of the probability of any of the risks seriously impacting the business or data subjects and informs the risk appetite. The benefits to data subjects of a more agile IT environment in policing **may** outweigh many of the risks. However, that does not mean that we should go live and cease work on the compliance.

SPA IM will need to keep abreast of any developments in law or MS T's and C's that may adversely affect the deployment of the product. Some of the concerns come from the current political climate. SPA IM will need to ensure that they keep up to date with any changes to US legislation or findings in the European Court of Human Rights that warrant a review of the processing/DPIA.

It is, therefore, the view of the IM Lead that the DPIA be submitted to ICO under S65 DPA asking for a quick turnaround. The ICO should also be asked their view should MS not sign a Code of Conduct as specified in DUAB.

DPO advice accepted or overruled by SIRO (name):		If overruled, explanation must be provided:

Comments:		
Referred to ICO:		ICO Response:
Comments:		

Appendix A – Screening Questions

We always carry out a DPIA if we plan to:

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

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

☐ Evaluation or scoring.
☐ Automated decision-making with significant effects.

☐ Systematic monitoring.
☐ Processing of sensitive data or data of a highly personal nature.
☐ Processing on a large scale.
☐ Processing of data concerning vulnerable data subjects.
☐ Innovative technological or organisational solutions.
☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

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

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

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

SCOTTISH POLICE AUTHORITY
ÙGHDARRAS POILIS NA H-ALBA

Data Protection Impact Assessment:
Microsoft Office 365 (O365) Project

GDPR and Part 3 Processing

(To manually check the boxes double **right click** on the tick box and select checked or unchecked)

Date Approved	TBC
Version Number	V2.0
Document Status	Final
Author	Police Scotland (PSoS) Digital Division [redacted], Scottish Police Authority (SPA)
Date on which the proposed processing is to start (if known)	06/25

Revision History

Version	Date	Summary of Changes
V0.1	12/12/2024	Initial Draft
V0.2	19/03/2025	Updates
V1.0	25/03/2025	Light touch version for SIRO/ICO
V1.1	09/06/2025	Full version for SIRO

Part 1 – Determining whether the proposed processing of personal data for GDPR/DPA 2018 purposes is likely to result in a high risk to the rights and freedoms of the data subject.

The SPA DPIA guidance must be read before answering the questions.

Once completed, this part must be submitted to SPA Information Management to decide whether the proposed processing is high risk.

Part 1, Section 1 – General

1.1. Does the project involve the processing of personal data? (Refer to the definition of personal data in the Guidance Notes).
☒ Yes ☐ No – Please provide a summary of the project below and submit this DPIA to Information Management at SPAIM@spa.police.uk without completing any further answers.
The processing will involve personal data falling within Part 2 and Part 3 of the UK Data Protection legislation.

1.2 Who is the Lead for the project?	
Name	[redacted]
Designation	Head of Service Delivery, ICT
Contact Details	[redacted]@scotland.police.uk

1.3 Who is the Information Asset Owner	
Name	[redacted]
Designation	Chief Digital Information Officer
Contact Details	ChiefDigitalInformationOfficer@scotland.police.uk

1.4 Who is the SIRO	
Name	[redacted]
Designation	Depute CEO
Contact	[redacted]@spa.police.uk

1.5 Provide a summary of the project.

PSoS/SPA relationship

PSoS provides IT (Information Technology) as a 'service back', meaning they provide SPA with IT services, including a shared network infrastructure. SPA has no IT staff. Thus, the procurement, deployment and ongoing management of IT services is the responsibility of PSoS.

SPA and PSoS are separate legal entities and data controllers. Both are Competent Authorities as per the DPA 2018. PSoS by way of Schedule 7 and SPA by way of the Police and Fire (Reform) Scotland Act 2012.

SPA provides forensic services, including crime scene analysis, fingerprints, and DNA to PSoS, the Crown Office and Procurators Fiscals (COPFs), the Scottish Fire Service (SFS) and the Police Independent Review Commissioner (PIRC).

Police Scotland cannot enter into contracts, all contracts are in the SPA's name.

Whilst most processing will be based on the same legislative requirements, the Data Protection Act (Part 3), introduces differences in S73(4) in terms of the application of the law surrounding transfers as SPA is not a Schedule 7 body as mentioned in S73(4)(b).

SPA is not a Police Force and as such has no direct involvement with this project. However, as a data controller using the service by way of our reliance on PSoS for IT services, SPA has to assess the implications and risks for use of the product, particularly since Part 3 of the DPA 2018 introduces differences in law between Police Forces and SPA.

The detail in this DPIA, with the exception of risk, has been provided by PSoS.

Purpose of Project

To provide the Scottish Police Authority (SPA) with a modern, cloud-enabled, and standardised collaborative platform for productivity and identity tools which will enable enhanced access to information and systems in a secure manner.

Key outcomes:

- Provide a secure platform and national standards that enable new digital ways of working and better collaboration.
- Improved mobility through a reduction in staff time spent travelling for meetings/briefings.
- Improved access to systems and information, both internal and external.
- Improved internal and external collaboration and communication across Policing and the Public Sector.
- Alignment to a national cyber security service, monitoring UK policing systems, providing a 24/7 service monitoring for threats, attacks, and irregular user

activity, and effectively sharing Police threat intelligence.
- Providing a national process, standards, and mechanism for managing PSoS and SPA user IDs, reducing the barriers in information sharing with other Forces and streamlining the joiner/mover/leaver processes.

Project Approach:
At the Full Business Case (FBC) stage the approved delivery option for the O365 project was adoption of the approach documented by the National Enabling Programmes (NEP).

NEP Background:
UK Police Forces rely on Microsoft productivity tools, and on-premises IT infrastructure to conduct their day-to-day tasks (up to Government Security Classifications (GSC) 'Official' security classification, including 'Official' information which is sensitive and must be managed accordingly). Each Police Force implements their IT solutions differently as they function as independent organisations where the procurement of IT is concerned. This has led to a disparate IT estate deployed across UK policing making assurance across the board complicated.

O365/NEP solution:
The National Police Chiefs Council (NPCC) set a United Kingdom (UK) Policing Vision 2025 to have all 48 Police Forces in the UK digitally enabled and cloud ready. To enable this vision, the National Police Technology Council (NPTC), with sponsorship from the National Police Chiefs Council (NPCC) and the Association of Police and Crime Commissioners (APCC), secured initial funding from the Police Transformation Fund (PTF) to establish three national solutions as part of the NEP initiative:

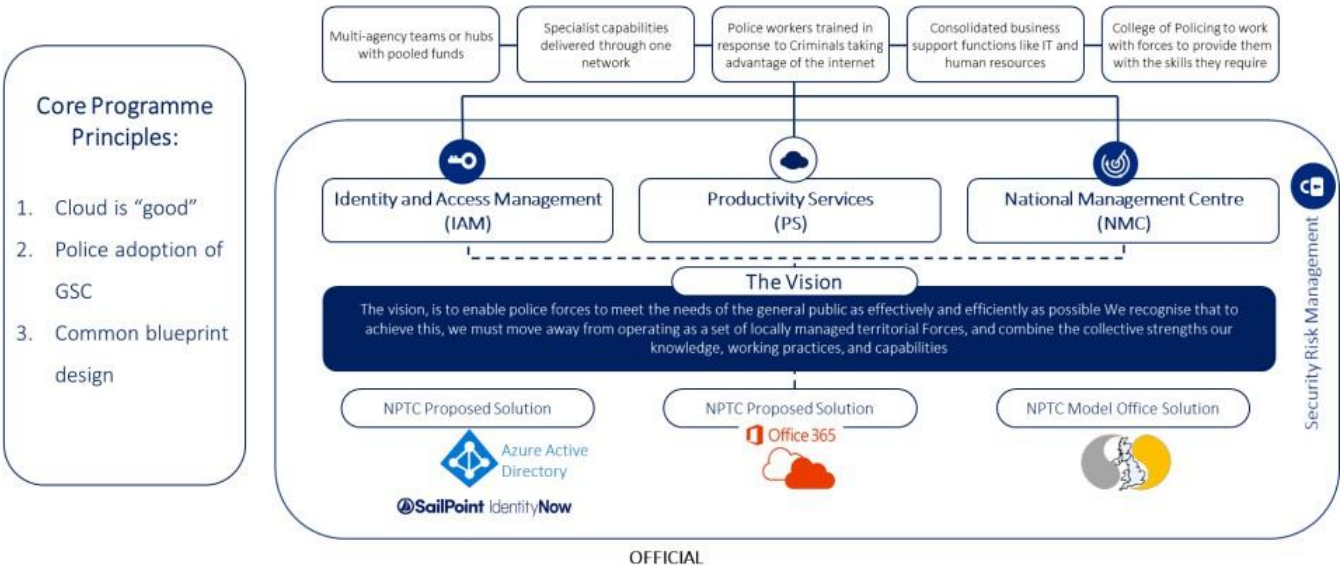
1. **Productivity Services** – To establish a national and standardised technology platform that compliments the Public Contact vision from the Digital Policing Portfolio and delivers productivity benefits such as: collaborative production for documents; spreadsheets and presentations.
2. An **Identity Access Management** (IAM) platform - To enable user access to local, regional, and national information, network and applications including cloud services in an efficient and effective manner.
3. A **National Management Centre** (NMC) - To deliver a nationally coordinated monitoring, response, and remediation capability to protect all UK Police Forces from cyber threats.

The three national solutions were major programmes of work and received both top-down support from the NPCC, APCC and the Home Office, and bottom-up support from the policing technology leadership community in recognition of the need for technology to enable significant strategic changes in the working methods of UK Police Forces.

One of the goals of the programme was to remove existing obstacles to efficient information sharing and cross-force communication to deliver a more efficient and collaborative way of working between Police Forces and their partners.

NEP Solution

Microsoft technologies were chosen for the NEP, due to their potential to meet programme compliance needs. SailPoint IdentityNow will be used for identity governance.



The NEP is not mandated to make UK Police Forces compliant with data protection legislation. The intent of the programme was to provide robust security around all information in the system with privacy built in to both the assessment of risk and application of necessary and proportionate controls (including an assessment of the security standards of third-party cloud service providers such as Amazon and Microsoft).

The O365/NEP solution is designed to mitigate the risks of cloud migration and operation, and to provide management of risks at the national level. To support this a collection of Low-level Designs (LLD) were produced and accredited at a national level. These have been noted on the next page and form the guiding principles for delivery of the products noted in this DPIA.

Vol	Title	Key Contents
1	Introduction	• Context, target audience, approach • Design overview (components)
2	Identity and Access Management	• Azure Identity and Access Management (IAM) components including Active Directory (AD), AD Connect, Conditional Access, Azure AD B2B, Privileged Identity Management, AD Identity Protection, IdentityNow (SailPoint)
3	**Core Productivity Services**	• **Exchange Online, Network requirements for Microsoft 365, Microsoft 365 Apps for enterprise, Microsoft 365 Admin Center, Security and Compliance**
4	Collaboration Services	• Microsoft Teams, SharePoint Online, OneDrive for Business, Sharing Controls, Yammer, Microsoft 365 Usage Analytics, Stream, Microsoft 365 Groups, Power Platform, Planner, Delve
5	Mobility	• Microsoft Endpoint Manager Intune - mobile device and application management
6	Flow Diagrams	• Data flows for authentication, email and collaboration services
7	Business Processes	• IAM operational business processes and process diagrams
8	Identity Governance	• IAM identity governance processes and process diagrams
9	Security Model	• Security Model background, methodology and controls
10	Windows 10 – Technical Design	• Windows 10 Traditional Management - solution overview, design principles, requirements, architecture and components. SCCM and VPN configuration
11	Windows 10 – Modern Management	• Windows 10 Modern Management with Intune solution overview, design principles, requirements, architecture and components.
12	Build Configuration Template	• Pro forma document for the capture and elaboration of Force-specific implementation details

Products in Scope:
The project will seek to deliver the following components through the implementation of Microsoft cloud services deployed in a hybrid configuration, (the use of the productivity tools will be subject to acceptable use cases and internal approval). The term *"Hybrid"* within this DPIA means that the project will put in place new infrastructure that will run alongside existing infrastructure in place today. This provides the business more flexibility and allows the project to introduce new technology with minimum impact to the business or staff.

Core Productivity Services – Design Volume 3 (NEP National Solution 1)

Component(s)	Description
Exchange Online	Hybrid infrastructure and software for the delivery of Email, Calendar & Tasks to any enabled device or via a web client
O365 App's for Enterprise	Latest version of tools including Word, Excel, PowerPoint, Publisher, Access to support core productivity tasks such as document creation, editing and sharing

Exchange Online:
This design for Exchange Online is a hybrid solution, which will support the routing of all email including PSN-P for legacy mail domains such as PNN, via the internet, enabling the transition to police.uk.
During the decommission of the Government Convergence Framework (GCF) a set of technologies underpinning the Police National Network (PNN) ensuring secure (i.e. encrypted) communication between police forces and criminal justice partners existed, PSoS Digital Division adopted a solution leveraged off the back of the NEP documented approach, i.e.

"The end state for a force's implementation must be an Exchange Hybrid configuration with Exchange Online in the cloud and latest Exchange hybrid infrastructure on-premises".

The following innovative technology was introduced during the project:

- Exchange Hybrid Infrastructure
- Exchange Online (including Exchange Online Protection)
- Microsoft Defender for Office 365

The GCF exit work was carried out by the PSoS Digital Division systems team and outside the remit of the O365 Project. Standalone PSoS DPIA (URN 21-0300 – UK GDPR processing and URN 21-0304 – Law Enforcement processing) were raised by the systems team to cover the exchange work. SPA had no role in this work.

O365 Apps for Enterprise:
At the time of writing this DPIA O365 Apps for Enterprise has been deployed across all business areas. This replaced Office 2013 that went out of Microsoft support in April 2024.

Collaboration Productivity Services – Design Volume 4 (NEP National Solution 1)

Component(s)	Description
Teams	Teams is the collaboration and communication platform at the centre of Microsoft 365, (O365)
SharePoint Online	SharePoint Online is Microsoft 365's main document storage service.
One Drive for Business	OneDrive for Business provide users with cloud storage of their own work-related files.
Power Platform	The Power Platform is a suite of services aimed to deliver innovative business solutions, across one seamlessly integrated platform, in Microsoft 365.
Additional Services	• Bookings • Delve • Forms • Planner • Sway • To Do

	• Whiteboard • Viva Engage

Teams:

Microsoft Teams is an online communication and collaboration platform that brings together chat, video conferencing, file storage, including shared files, and application integration. It is part of Microsoft 365. Microsoft Teams is used as a successor of Skype for Business. Teams was rolled out across SPA early due to the need for staff to work from home during the Covid-19 pandemic. Teams was replaced by Webex in April 2023 but remains in place to facilitate collaboration with partners who do not support the use of Webex. Rules to ensure the appropriate rights and freedoms for data subjects in terms of the use of Webex and Teams are in development, in particular with respect to the recording of meetings. A privacy notice has also been developed and can be found on the SPA website.

SharePoint Online and OneDrive for Business:

These two storage services allow employees to store and share files with each other more easily from the Office software, and from Teams in particular. OneDrive is the basic application to store files. SharePoint works as an interface on top of OneDrive to allow file storage, and additional options such as the creation of wikis and forms. If a Teams call is recorded, it is automatically stored in the organisation's OneDrive.

To make use of the services employees must have an Office 365 work account and be assigned a license. Licenses are registered in Azure Active Directory, (AAD). This is Microsoft's online cloud identity service. Office 365 uses the AAD to give people access to Microsoft's cloud services, such as Teams, SharePoint Online, OneDrive for Business and Exchange Online.

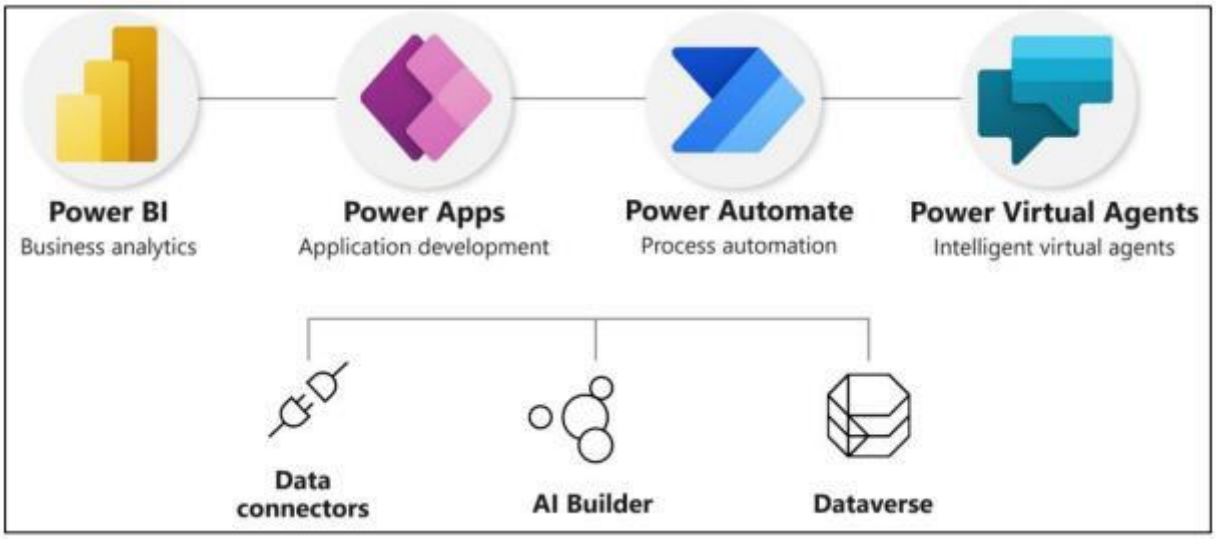
Although the NEP recommendation is to migrate all SharePoint On-premises files to SharePoint Online, they recognise that some forces may wish to maintain their content on-premises. This will be the case for SPA whilst we review the current data for compliance. The project will therefore adopt a hybrid implementation.

With SharePoint Server hybrid, productivity services in SharePoint Online can be integrated with SharePoint on-premises to provide unified functionality and access to data. This will allow a gradual move of on-premises SharePoint server services to Microsoft 365; SharePoint Server hybrid will provide a staged migration path by extending on-premises workloads to SharePoint Online.

SharePoint Online is fully auditable providing audit log reports to view the data in the audit logs for a site collection. Administrators have the ability to sort, filter, and analyse this data to determine who has done what with sites, lists, libraries, content types, list items, and library files in the site collection. For example, you can determine who deleted which content.

SPA does not permit the use of SharePoint for Part 3 processing and has provided guidance to staff in terms of the use of SharePoint for processing Part 2 personal data. Most of the personal data will be staff comms as SPA uses SharePoint as an Intranet site.

Power Platform:
The Power Platform is a suite of services aimed to deliver innovative business solutions, across one seamlessly integrated platform, in Microsoft 365. Power Platform provides a low code interface for force users to quickly create custom apps, while simultaneously providing robust tools for pro developers. The Power Platform is made up of four services:



Under the NEP Memorandum of Understanding (MOU) there are no Power BI features included. Extract below lifted from the designs:

"Under the MOU Licensing, the 'Power Apps for Microsoft 365' license is available for all force users. If enabled, this license provides forces with a limited set of features in the Power Apps, Power Automate and Power Virtual Agent services. These are basic features with more advanced features needing additional licensing. There are no Power BI features included under the MOU licensing.

Any further requirement over and above the basic settings/features enabled by the project will need to follow the current process for requesting new applications, i.e. IT Connect request detailing the use case and justification.

Additional Services:

- **Bookings -** Allows the scheduling and managing of appointments with external people, without the need to authenticate. Bookings include a web-based booking calendar, based in an Exchange online mailbox, and integrates with Outlook to optimise a user's calendar and give external parties the flexibility to book an appointment slot.

- **Delve:** A content discovery tool across Microsoft 365, highlighting documents others are working on in locations you have access to, like Teams and SharePoint Online. It provides an interface for users to manage their Microsoft 365 profile.

- **Forms:** Provides staff with the ability to create web-based surveys, quizzes, and polls for distribution internally or externally.

- **Planner:** A task management tool, utilising Kanban boards, to organise and allocate work. It uses content-rich task cards with files, checklists, labels, and other features to allow users to collaborate in Planner and Microsoft Teams.

- **Sway:** A web-based presentation app, that allows users to express ideas using an interactive canvas. Sway's design engine allows users to easily produce professional, interactive, and visually appealing designs from images, text, documents, videos, maps, and other web-based sources.

- **To Do:** A personal task management app that empowers users to track and focus on the things they need to get done.

- **Whiteboard:** A free-form, digital canvas which provides users with a shared digital whiteboard where people can work and come together. Whiteboard enables teams to collaborate in real time, with pen, touch, or keyboard devices.

- **Viva Engage (Formerly known as Yammer):** An enterprise grade social networking tool designed to improve how knowledge and information is shared across forces. It can connect users within the SPA and externally to create a collaborative platform built on Microsoft 365 collaboration and security & compliance features.

Apps will not be automatically deployed; staff will need to make a request. SPA IM staff approve requests and as such have oversight of the use. User guides will be reviewed/developed for all applications to ensure staff comply with Data Protection requirements when processing personal data on any apps.

Identity Access Management – Design Volume 3 (NEP National Solution 2):
The solution chosen by the NEP for the Identity and Access Management (IAM) solution was IdentityNow which is a cloud-based Identity-as-a-Service (IdaaS) solution provided by SailPoint. It is an identity and access governance system that connects to authoritative sources and target applications via virtual appliances that are installed within Police Scotland's infrastructure.

SailPoint IdentityNow was completed in November 2023 and now forms an integral part in the governance of access to multiple applications and other services in use throughout PSoS/SPA and to external national Policing applications through the National Identity Access Management, (NIAM) platform managed by the UK Home Office.

National Management Centre (NMC) – (NEP National Solution 3):
Providing protective monitoring and assistance to police forces in all aspects of cyber security. The use of the NMC and its alignment to the Police Scotland Digital Strategy for procurement of cyber security services was approved by the PS Chief Digital and Information Officer on 21/09/2022.

The NMC service contains seven elements:

Service	Description
Performance Monitoring	The NMC's Protective Monitoring capability will provide 24/7 proactive detection, triage and notification of potential cyber incidents based on security event data from the Police Scotland security platform.
Cyber Incident Response	The NMC will provide a 24/7 Cyber–Incident Response service to Police Scotland.
Cyber Threat Intelligence	Delivery of tailored and contextualised Cyber Threat Intelligence analysis and reporting, ongoing collection, analysis and reporting of threat intelligence based on prioritised intelligence requirements.
Malware Analysis Service	The NMC Malware Analysis Service (MAS) portal supports the submission, automation, and analysis of malware samples as part of the overall NMC MAS. The MAS combines process and technology to support clients in the investigation, analysis, and handling of malware related security incidents.
Vulnerability Assessment	Identifying new vulnerabilities as they are released by vendors and communicate to forces in near-real time, with context and guidance around patching and updating.
Penetration Testing Support	The Penetration Testing Support service will offer guidance throughout the lifecycle of a Police Scotland managed Penetration Test.
Customer Interface	The NMC will assign a member of their cyber liaison team to be a named and consistent point of contact for Police Scotland from the point that service commences.

As previously referenced the 3 national solutions the NEP has been built on consists of:

1. **Productivity Services**
2. **Identity Access Management**
3. **National Management Centre**.

Due to the size and scope of the project there could be further DPIA requirements identified as the work matures.

Delivery Approach

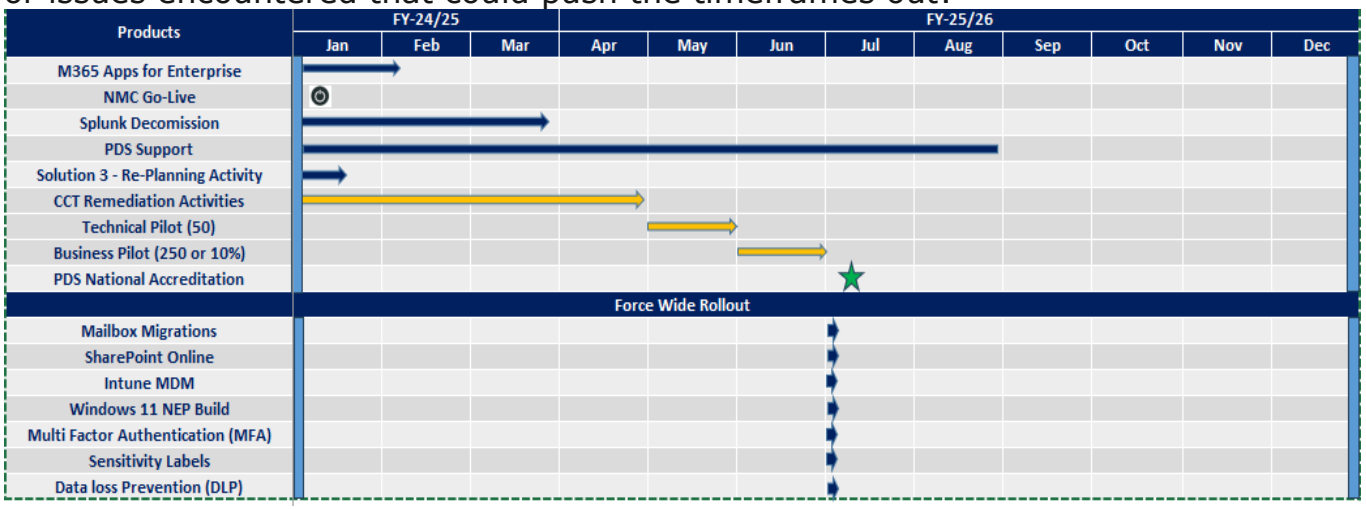
The project will closely follow the approach detailed by the NEP for solution 1. This begins with the execution of the Configuration Check Tool (CCT) against the PSoS/SPA Microsoft O365 Tenant. *"A Microsoft 365 tenant is a dedicated instance of the services of Microsoft 365 and organization data stored within a specific default location; in this case it is withing the UK. Each Microsoft 365 tenant is distinct, unique, and separate from all other Microsoft 365 tenants".*

The output from this exercise is the creation of a gap analysis report detailing the PDS/NEP design position, the PSoS/SPA position, and next steps, i.e. remediation of the gaps.

The report highlighted 233 gaps between the PDS/NEP approach and the PSoS Tenant setup. The project needs to evidence that the remediation work to bring the project into alignment with the PDS/NEP blueprint designs has been carried out. This work is expected to run through until the end of April 2025. If all the High category design decisions have been remediated, then the project will conduct a technical pilot. This will provide the users with full access to the cloud elements of Solution 1. If successful the project will progress to a 250, or 10% of the workforce business pilot. Again, if successful further checks will be conducted between PDS/NEP and the project to determine that compliance to the design blueprints has been maintained throughout the pilot phases. If the project is still in compliance and no deviations have been raised throughout the work, Police Scotland will gain acknowledgement that it follows the nationally accredited design blueprints and in line with every other force in the UK. At this stage the onus on rolling across PSoS/SPA sits with the project.

It needs to be noted that the above does not replace or negate the need to conduct our own governance for any new solution. Throughout the remediation work the project is currently and will continue to have discussions with the internal governance bodies and where applicable abide to and gain the necessary approvals to allow it to proceed with the pilot work and eventual full rollout.

The image below provides an overview of the work in flight. As with all projects the dates have been set on the understanding that there are no major strategy changes or issues encountered that could push the timeframes out:



Why the NEP and Microsoft Services

In general, UK Police Forces rely on Microsoft productivity tools and on-premises IT infrastructure to conduct their day-to-day tasks (up to Official-Sensitive security classification). Each Police Force implements their IT solutions differently as they act as independent organisations where the procurement of IT is concerned. This has led to a disparate IT estate deployed across UK policing. One of the effects of this is that security of the Police IT estate is extremely difficult to implement and assure as a whole. This impact on system and information security also affects the protection of the privacy of Police Officers, Police employees, victims of crime, witnesses, suspects in investigations, convicted offenders, public and any other parties involved in Police work.

The increase in threats to Police from cyber-related actors and the awareness of the general public of their privacy rights can, and should, be improved.

The National Police Chiefs Council (NPCC) set a UK Policing Vision 2025 of having all 48 Police Forces in the UK digitally enabled and cloud ready. To enable this vision, the National Police Technology Council (NPTC), with sponsorship from the NPCC and the Association of Police and Crime Commissioners (APCC), secured initial funding from the Police Transformation Fund (PTF) to establish three national solutions as part of the National Enabling Programme initiative. The solutions have been noted early in this DPIA. They received both top-down support from the NPCC, APCC and the Home Office, and bottom-up support from the policing technology leadership community in recognition of the need for technology to enable significant strategic changes in the working methods of the UK Police Force. This has removed existing obstacles to efficient information sharing and cross-force communication and delivered more efficient and collaborative ways of working between Police Forces and their partners.

Similarly, for the use of the Microsoft online services, i.e. no other supplier can/could offer a combined license package or services that SPA, via PSoS, have been adopting for a number of years.

Microsoft acts as a data processor on behalf SPA in respect of the processing of personal data within the O365 tools that form part of the NEP solution. There is a central Memorandum of Understanding (MOU) in place between Microsoft and Police Digital Service (PDS) which agrees to common pricing and discounts. This means that Microsoft's Online Service Terms and Data Processing Addendum apply directly between each force as controller and Microsoft as processor. On their own PSoS/SPA would not have been able to secure these discounts.

By not using Microsoft SPA would not be following the NEP approach resulting in major deviation to the programme and problems for the PSoS adoption given our shared IT infrastructure. The possibility of finding other suppliers who could offer a similar service is remote meaning setting up and tendering for multiple suppliers at one off costs. The ongoing management of multiple contracts would be time consuming and increase the risk of a potential loss of service.

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.
The data which will be processed via the solution originates primarily from SPA, our partners and the communities we serve. In general terms, the solution will not change the nature or scope of the personal data which SPA routinely collect or process today, it simply provides an improved, consistent, and more secure solution which can be used to store and access personal data. The data is being processed to fulfil SPA's obligations in terms of the Police and Fire Reform (Scotland) Act 2012.
1.2.2 What is the intended outcome for the individuals whose data you propose to process?
There will be no change in outcome for data subjects. The data which will be processed via the O365/NEP solution originates mainly from SPA and criminal justice partners. In general terms, the O365/NEP solution does not change the nature or scope of the personal data which we routinely collect or process today, it simply provides an improved, consistent, and more secure cloud-based solution which we can use to store and access the data.
1.2.3 What are the expected benefits for the business?

The introduction of Teams during Covid provided SPA with the ability to operate a successful home working model that later turned into the normal way of work for office-based staff. It provided a high number of benefits in terms of operating expenses, infrastructure running costs, staff health and wellbeing, travel expenses, and increased productivity.

The deployment of the O365/NEP solution across SPA will deliver productivity benefits whilst improving the overall Cyber Security maturity. The development of the cyber risk management position of the organisation is assessed against the National Institute of Standards for Technology's (NIST's) Cybersecurity Framework, providing a baseline. A re-assessment is undertaken once the project has completed delivery where an overall improvement can be demonstrated from the integration of the NEP blueprint design set.

PSoS advises that inclusion of the integrated security elements (including the NMC, IAM solution and Security Model) will significantly improve the security of SPA information and therefore the ability to protect the privacy of data subjects in accordance with the requirements of the Data Protection legislation.

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

A solution like SailPoint IdentityNow is aimed at ensuring improved Information Security processes are introduced with appropriate governance. By ensuring data, much of which is sensitive in nature, is appropriately protected and that only those that have a need to know have access should help protect the rights and freedoms of data subjects and improve public confidence in the SPA.

Productivity Services – to establish a national and standardised technology platform that complements the Public Contact vision from the Digital Policing Portfolio and delivers productivity benefits such as: collaborative production of documents, spreadsheets, and presentations (amongst other examples); and the storage and management of these files, email and file-sharing. A key aim is to remove barriers to operational efficiency and to enable joint working, as well as digital engagement with the public (i.e., enabling public interaction with SPA through digital means).

The National Management Centre will deliver a nationally coordinated monitoring, response and remediation capability that will protect Police data from Cyber Threats and potential loss of any public data held.

Part 1, Section 3 – Nature of processing

1.3.1 Has the SPA Information Management Lead been consulted: This should be done at the outset of any project – SPAIM@spa.police.uk

☒ Yes

☐ No

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

The IM Lead was contacted at point of risk assessment.

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

☒ Yes – If so, provide details.

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

The assets sit within PSoS Digital Division.

PSoS advise that the project adheres to all the governance meetings and holds a monthly Steering group meeting inviting staff from PSoS information assurance representing UK GDPR and Law Enforcement, Project Assurance, Cyber Security Assurance, Digital Division groups/Senior Management, Records Management, and others.

Consultation has been undertaken with the PSoS Cyber Security and Assurance (CSA) Manager, Chief Digital Information Officer, ICT Chief Operating Officer, Chief Technology Officer, Head of Service Delivery (Digital Division), Information Security Manager (ISM), and the Records Manager (RM).

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

OFFICIAL

OFFICIAL
SENSITIVE

POLICE ONLY

POLICE & PARTNERS

1.3.4 Will any processing be done via an internet / Cloud-based system?
☒ Yes – Provide the details below. ☐ No
The O365/NEP approach will store information using a hybrid cloud solution provided by Microsoft. Certain information will continue to be stored locally on SPA's existing IT infrastructure. Exchange and SharePoint online will be implemented through a hybrid approach. See below example on the use of a hybrid approach for Exchange: *"A hybrid deployment offers organizations the ability to extend the feature-rich experience and administrative control they have with their existing on-premises Microsoft Exchange organization to the cloud; Hybrid deployments provide the seamless look and feel of a single Exchange organization between an on-premises Exchange organization and Exchange Online in Microsoft Office 365. In addition, a hybrid deployment can serve as an intermediate step to moving completely to an Exchange Online organization".*

1.3.5 Will SPA be processing the personal data jointly with another organisation? (Refer to the definition of controller in Appendix 1 of the Guidance Notes). If so, documentation 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
PSoS and SPA will be joint controllers given that PSoS delivers ICT to SPA. SPA and PSoS have a Data Sharing Agreement in place.
1.3.6 Will another organisation be processing any of the personal data on behalf of SPA? (Refer to the definition of processor in Appendix 1 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

The move to a cloud-based environment means that SPA information and user credentials will be stored on infrastructure provided by Microsoft (Microsoft 365 and associated Microsoft cloud services) and Amazon Web Services (SailPoint Identity Access Management) which may present privacy concerns.

SailPoint Contract (IAM Solution)

14042023 - Scottish Police Authority - HT

NEP/Police Digital Service (PDS) Contract (between the Police Digital Service (PDS) and the Scottish Police Authority (SPA).

Co-operation Agreement in relatio

Microsoft Contract

The Microsoft 365 product suite and contracts are procured directly with Phoenix Software Ltd and cover a three-year term. Microsoft's Worldwide Data Processing Addendum applies (and is incorporated into Microsoft's standard Online Service Terms). And can be viewed view the link below.

SPA have asked for the amendment to the DPAdd that was made for DESC use of Azure, given that the Microsoft DPAdd does not refer to UK GDPR or DPA 2018.

Licensing Documents (microsoft.com)

1.3.7 Will the processing involve new technology? (i.e. technology that is new to SPA.)

☒ 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

The NEP is an innovative programme and solution. It will enable significant strategic changes in the working methods of SPA and will remove existing obstacles to efficient information sharing and communication, delivering more efficient and collaborative ways of working between SPA and their partners in policing.

The O365/NEP solution is intended to take advantage of the enhanced security features which modern technology working practices can provide. The NEP will also deliver new technology in connection with the three national solutions, i.e.:

Productivity Services:

- Exchange Online
- O365 Apps for Enterprise
- Teams
- SharePoint Online
- OneDrive for Business
- Power Platform

Access to:

- Bookings
- Delve
- Forms
- Planner
- Sway
- To Do
- Whiteboard
- Viva Engage

Identity Access Management Solution (IAM) – SailPoint IdentityNow:

A platform providing a distributed method to request and approve access rights (i.e. the ability to sign-in to applications as well as the level of access to functionality within them or to data sources).

National Management Centre (NMC):

Delivering a nationally coordinated monitoring, response, and remediation capability in order to protect all UK Police Forces from cyber threats.

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

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
- ☒ Police officers
- ☒ Police/SPA staff
- ☒ Other – provide details below

The types and categories of personal data processed will depend on the content of the information input into the system by SPA and the communications received from partners and the public.

The personal data which will be processed using the solution includes data relating to police officers, employees, contractors, and suppliers. It also includes information relating to live police investigations. By way of example, information which is contained within emails which are stored in the Azure cloud hosting environment, and information relating to service requests (e.g., when individuals make an individual rights request under the UK GDPR) will be processed utilising the solution.

The solution could be used to process personal data including:

- Personal details of staff/suspects/offenders/witnesses/victims (e.g. name, address, email address, telephone number, car registration number, national insurance number, passport, driving licenses).
- System usage details relating to staff usage of the system.
- Family, lifestyle, and social circumstances of staff/suspects/offenders/witnesses/victims
- Education and training details of staff.
- Employment details of staff.
- Online identifiers (e.g. internet protocol addresses, cookies identifiers) of staff.
- Financial details (e.g. bank account details) of staff/suspects/offenders.
- Criminal records, offences (including alleged offences) and criminal proceedings, outcomes, and sentences of suspects/offenders.
- Legal proceedings about suspects/offenders.
- Data on children where children are witnesses or victims.
- Special categories of personal data, including data on disabilities, health records, religious or philosophical beliefs, trade union membership, relating to staff/suspects/offenders/witnesses/victims.

It is important to stress that the above list is not exhaustive, and that by the nature of the solution and the scope of the IT systems with which it interfaces, the

categories of personal data which may be processed via the solution is very wide.

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
☒ Police officers
☒ Police/SPA staff
☒ Other (e.g. data already held in other SPA systems, partner agencies etc.) - provide details below

The personal data which will be processed using the solution includes data relating to police officers, employees, contractors, suppliers and the public. It may also include information relating to the prevention/detection of crime. By way of example information which is contained within emails which are stored in the Azure cloud hosting environment will include general correspondence, complaints, individual rights requests, requests from lawyers etc.

The relationship with individuals therefore varies depending on the processing in question. In some cases, the relationship will be one of employer to employee, in others it is customer to supplier and in others it will be SPA to criminal justice partners and members of the public.

The products used to provide the solution will only hold unstructured data sets, rather than structured information held in databases. Unstructured data refers to individual, isolates pieces of data that cannot be joined together, such as data within emails. It is not the intention of the solution to replace core policing systems functionality.

Staff are instructed to save information that needs to be retained into the appropriate system or network drive to ensure organisational rules are applied. Audits of mailboxes are undertaken to ensure compliance.

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 types and categories of personal data processed by the solution will depend on the content of the information input into the applications by users.

The solution could be used to process personal data including:

- Personal details of staff/suspects/offenders/witnesses/victims (e.g. name, address, email address, telephone number, car registration number, national insurance number, passport, driving licenses (to identify themselves for

information rights requests)).

- System usage details relating to staff usage of the system.
- Family, lifestyle, and social circumstances of staff/suspects/offenders/witnesses/victims
- Education and training details of staff.
- Employment details of staff.
- Online identifiers (e.g. internet protocol addresses, cookies identifiers) of staff.
- Financial details (e.g. bank account details) of staff.
- Criminal records, offences (including alleged offences) and criminal proceedings, outcomes, and sentences of suspects/offenders (primarily from subject request)
- Legal proceedings about suspects/offenders/staff (such as comms from Crown Office)
- Special categories of personal data, including data on disabilities, health records, religious or philosophical beliefs, trade union membership, relating to staff/suspects/offenders/witnesses/victims.

SPA has no control over the content of inbound mail and the public/lawyers will often email us with information meant for PSoS. These emails are deleted after the data subjects are provided with a contact for PSoS.

1.4.4 Does this project involve processing special category or criminal conviction data? If so, tick all categories of special category data to be processed. (Refer to the definition of criminal conviction and special category data in Appendix 1 of the Guidance Notes)

☒ 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

The solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to process personal data. As an example, SPA often receives requests for a copy of data subjects' fingerprints. The offer of postage/egress mail is made but many data subjects request the data to be emailed via webmail.

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

☐ Yes – provide details below

☒ No

The solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to process personal data.

1.4.7 Will the personal / special category / criminal conviction data be fully identifiable, pseudonymised or anonymised?

☒ 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

Microsoft Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default. Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. However, it is not possible to define all data used within the services or solutions put in place by the project. As previously stated, the data which will be processed via the solution originates mainly from SPA/PSoS and key Partners. In general terms, the solution will not change the nature or scope of the personal data which we routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access personal data.

Data may be provided to research programmes/Government in a pseudonymised/anonymous format. The practices used throughout SPA regarding data handling will not change because of this project.

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 SPA staff. Individuals whose personal information is processed by SPA on the O365 platform. It is not possible to quantify volume for external parties.

1.4.10 What is the geographical area involved?

Whole of Scotland and any location where a partner or data subject is based.

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 ☐ No
SPA has concerns re the legality of the MS Cloud processing. ICO has previously provided advice to SPA in terms of the processing of Part 3 data in MS Azure. SPA was able to progress with the processing as services where data sovereignty could not be guaranteed were turned off and MS provided an addition to their DPAdd for the processor. However, Microsoft advises that O365 operates in a completely different manner and there is currently no way to guarantee data sovereignty.
1.5.2 Describe any relevant advances in technology or security
Cloud working comes with an elevated level of scalability and resilience not typically found within on-premises hosted solutions. Microsoft is the industry leader in cloud technology offerings and is at the forefront of technological developments in the cloud space. Provision on an automated IAM solution that will eventually replace the semi-automated process in place today. Provision of a 24/7 fully managed cyber threat protection solution.
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
There has been significant coverage of the 'Hyperscale' Cloud issue and data sovereignty in the media and in online chat groups.
1.5.4 What relevant policy or procedure has been considered?
Records Retention SOP. Data Protection SOP. Information Sharing SOP. Information Security SOP.

This form should now be sent to SPAIM@spa.police.uk mailbox to assess the content/risks.

Data Protection Impact Assessment

Part 2 – Assessment of legality, governance and risks

Name of Project: Microsoft Office 365 (O365) Project

Part 2, Section 1 – Assessment of Necessity and Proportionality – The General Data Protection Regulation and relevant sections of the Data Protection Act 2018 (DPA 2018)

The Data Protection Principles

1st Principle – Lawful, fair and transparent

This principle is covered by sections 2 and 3.

2nd Principle – Specific, explicit and legitimate purpose

2.1.1 Does the proposed processing involve the collection of data not previously collected by PSoS?
☐ Yes – State below the purpose(s) for which you are collecting the data. (If you answered this question in Part 1 Q 1.4.6, please copy and paste the response below). ☒ No
The solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access the personal data.
2.1.2 Are you processing the data for a different purpose than that for which it was collected?
☐ Yes – Provide details below of the original purpose and the new purpose, and an assessment of whether the two purposes are compatible. ☒ No
The solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access the personal data.

3rd Principle – Adequate, relevant, limited to what is necessary

2.1.3 What assessment has been made to ensure that the data to be processed is adequate, relevant and limited to what is necessary for the purpose for which they are processed?
The solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access the personal data. The following will still apply. **Information used for a policing purpose:** The Code of Practice on the Management of Police Information ("MOPI") sets out at 2.2.2 that the police purposes are defined as: protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice; and any duty or responsibility of the police arising from common or statute law. Any such information used for a policing purpose will be processed in accordance with Part 3 of the DPA 2018. **Information used for a non-policing purpose:** Information used for any purpose other than a policing purpose will be deemed to be used for a non-policing purpose. This includes, without limitation, processing of employee data by employer data controllers. Any information used for a non-policing purpose will be processed in accordance with the UK GDPR and the DPA 2018 and under any relevant statutory powers relating to that information and the purpose for which it is being processed. Personal data will be processed in compliance with the relevant conditions set out at Article 6 and 9 (if appropriate) of the UK GDPR and in Schedule 1 (as appropriate) of the DPA 2018.

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

2.1.4 How will the accuracy of the data be checked?

In general terms, the solution will not change the nature or scope of how the accuracy of the personal data which SPA routinely collect, process, or share with others today is maintained, it simply provides an improved, consistent, and more secure solution which can be used to store and access that personal data. Data entered by SPA can be checked and corrected if found to be inaccurate. This won't be the case for data such as chats, voicemail and call history which will be an accurate record of events.

IdentityNow: With regards to the accuracy of staff identities used for access to the new solutions, technology, or existing solutions/application in place throughout SPA, this will be derived from HR systems in place today and will remain so after delivery of the project. See detail below lifted from the SailPoint IdentityNow DPIA:

"During initial implementation identity information will be exported from the SCoPE HR system in Comma Separated Values (CSV) format to allow a bulk ingestion of data. Thereafter, the SCoPE system will utilise the IdentityNow REST API to push changes made within the HR system to the IAM platform. In all instances, the data is sourced and maintained within the HR platform and its accuracy is, therefore, governed by that system and the processes and procedures currently in place.

Under the NEP framework all identity information is refreshed from the source HR system with a minimum frequency of once per day. It is intention of the Police Scotland implementation to keep identity information up to date in as near real time as possible. This will be achieved by the SCoPE HR system invoking the REST API within IdentityNow to push changes to identity information as they occur.

Within IdentityNow all identity data is obtained from an authoritative source (that being the SCoPE HR system) and then kept synchronised thereafter. The accuracy of the data is, therefore, governed by that authoritative source"

2.1.5 How will inaccurate data be corrected?

The solution will not change the nature or scope of how the accuracy of the personal data which SPA routinely collect, process, or share with others today is maintained, it simply provides an improved, consistent, and more secure solution which can be used to store and access that personal data.

Data entered by SPA can be checked and corrected if found to be inaccurate through the existing processes in place for all source systems.

2.1.6 How will it be kept up to date where necessary?

The solution will not change the way that data is kept up to date. Data will still require to be processed in accordance with the SPA Records Retention SOP. Each area of the solution will have its own rules including storage/retention/use. Audits will be conducted to ensure the applications are compliant.

5th Principle – Not kept longer than necessary

2.1.7 How long will the personal data be retained?

Data is retained by Microsoft for the duration of our use of the service. As a customer SPA will, at all times during the term of the subscription, have the ability to access, extract, and delete data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion.

Within the design blueprint for the **Productivity Services (1)** solution it details a baseline retention policy for the following elements:

- Exchange Online
- SharePoint Online sites
- OneDrive accounts
- Microsoft 365 groups
- Exchange public folders
- Microsoft Teams (Chats and Channel Messages)

However, this is not mandated and can be superseded by the policies/SOPs in place today within SPA, see below.

"The NEP baseline retention configuration is NOT designed to offer forces any kind of compliance in relation to GDPR, MOPI or other regulations. Its primary purpose is to provide a configuration that prevents data being maliciously or accidentally deleted. Forces are responsible for meeting their information governance and compliance obligations".

Discussion have commenced with Records Management prior to the implementation of the elements noted under the Productivity Services solution. During the reviews/discussion the guiding principles will come from the SPA Record Retention SOP, and the NEP guidelines.

With regards to the **Identity Access Management (2)** solution (SailPoint IdentityNow):

"SailPoint IdentityNow data will be retained for the duration of employment for police officers and police staff + 90 days after the date they leave. For contract/agency staff it is the duration of their contract with Police Scotland + 90 days on the date their contract terminates"

With regards to the **National Management Centre (3)** solution the NMC stipulate that all data contained within the Sentinel instance is retained for a minimum of 365 days for compliance purposes.

2.1.8 Is the personal data already covered by the existing Record Retention SOP?

☒ Yes – Provide the section / paragraph from the Record Retention SOP below

☐ No – The Records Manager within IA must be consulted as soon as possible

A full review of the SOP is currently underway and where required additional guidance will be added.

2.1.9 The system must be able to weed and delete a) individual records and b) bulk records. How will you ensure this can be done? e.g. manual intervention, automatic deletion etc.

SailPoint IdentityNow:

The intent of an IAM solution is to automate, to the greatest extent possible, the Joiners, Movers, and Leavers processes. Changes in the authoritative system (i.e., SCoPE HR) such as a retiral will invoke those Leaver processes to remove the account from linked sources (e.g. Active Directory). IdentityNow also supports the capability to manually manage identity records through the web-based management portal so records can be deleted via manual methods if required.

Bulk removal of records is supported by the IdentityNow platform and is triggered through changes in the authoritative source (i.e. SCoPE HR). The automated leavers process (triggered when an employee is marked as having left the organisation) is then invoked to remove the account from connected sources (e.g. Active Directory, Azure Active Directory, etc.). This is the exact same process as for individual deletions. For Active Directory it should be noted that Police Scotland's retention period, shared by SPA, is 90 days before an account flagged for removal is fully removed from the system.

Automated retention and disposal are enabled through the O365 Compliance Centre. Further work will be conducted with the Records Management Officer when it comes to the retention policies for Outlook, SharePoint online and OneDrive for business, currently retentions policies are in place for Teams and OneDrive for business.

SPA commenced a data governance programme in 2023 to try and get staff to weed data from Outlook. Our policies are very clear that Outlook is not a storage application and emails should either be deleted or moved to the on prem drive if required. However, we are encountering problems with staff complying with this instruction. It is our intention to reduce the size of email boxes going forward to prevent its use for storage.

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

There is no intention or need to keep the data beyond the retention periods. Any data kept for stats is anonymised.

2.1.11 What process will be in place to ensure the data is securely destroyed/deleted?

With regards to data stored on Microsoft technology this is detailed within the Microsoft Products and Services Data Processing Addendum, Licensing Documents (microsoft.com).

"At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.
Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such data."

SailPoint IdentityNow is hosted on Amazon Web Services (AWS), a cloud hosting provider. All data management is handled through the IdentityNow web portal and is governed by SailPoint processes. Amazon processes ensure that when data is deleted it is inaccessible and provide the following guidance (https://aws.amazon.com/compliance/data-center/data-layer/) on physical media decommissioning.

Microsoft, SailPoint and Amazon hold ISO 27001 accreditation governance around secure data destruction.

6th Principle – Security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

2.1.12 Recording Project Risk

The project risk register resides on the Project Portfolio Management Anywhere (PPMA) solution within PSoS. PPMA is a portfolio management tool introduced by the Project Management Office (PMO). Reports are generated from the solution to inform senior staff. The risks will be managed within this tool during the lifetime of the project. At the end of the project any residual risks will be assessed and either closed or transferred over to the appropriate business function.

SPA does not have a separate risk register for this project.

2.1.13 What processes will be in place to determine who will have access to the data / system?

SailPoint IdentityNow operates with a full Role Based Access Control (RBAC) system that allows the granular control of access to nominated members of staff. As part of the implementation federated authentication will be configured between the IdentityNow tenant and Police Scotland's existing Azure AD tenant (which includes SPA). Access to IdentityNow and the provision of roles will be to user accounts that originate from the on-premises Active Directory environment.

Microsoft technology: As part of the implementation Multi Factor Authentication, (MFA) will be configured between the O365 tenant and Police Scotland's existing Azure AD tenant.

2.1.14 How will access to the system be granted and removed?

Account creation providing access to the solution elements will be managed by the Joiners, Movers, Leavers (JML) process controlled by the Identity Access Management (IAM) solution provided by SailPoint IdentityNow, i.e.

- "Joiners" processes typically involve the creation of a new user account just prior to that employee beginning their first day of work and ensures that they have access to the key systems that their role requires.
- "Movers" processes cover the various changes in access rights that an employee goes through as they change role within the organisation. For instance, an employee may change role from Payroll to Procurement so the underlying IAM system would remove their rights to Payroll but grant them all the rights they need to carry out their role in Procurement.
- "Leavers" processes ensure that, on the day an employee leaves the organisation, that their access rights are revoked. Email account is deleted after 30 days.

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

All SPA staff and contractors have been vetted to an appropriate level commensurate with their role.

Administrators will require enhanced vetting (Management Vetting (MV)). SPA does not have any administrators, but staff such as the IM Lead are MV cleared.

Microsoft state that their staff are vetted and will not permit police vetting of their employees, which contradicts the requirements of the National Police Vetting Policy.

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

It is not envisaged that there will be a demand or need for any additional data protection /security training beyond what is in place today other than how to access the new technology.

The Microsoft technology, other than the additional services noted on page 6 are in use today, i.e. Outlook, Word, Excel, PowerPoint, Project, Visio, Note Pad. Training will take place in respect of the rules for using the applications, such as no Part 3 data in SharePoint.

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

☒ Yes – state below which of the above

☐ No – state below, why not

The implementation of the NEP solutions will require SyOps and procedural manuals to be put in place. This will be achieved working in conjunction with the PSoS Cyber Security & Assurance (CSA) group.

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

☒ Encryption ☒ Role Based Access Control

2.1.19 How will information be protected in transit?

☐ Secure email ☒ Encryption

☐ Egress ☐ Other – Provide details below

Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which

Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

SPA will not be deploying additional encryption at this point.

2.1.20 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.)

As a SaaS (Software as a Service) offering business continuity and backup forms part of that service and is managed by SailPoint. The SailPoint Data Security Programme documentation (https://docs.sailpoint.com/wp-content/uploads/SailPoint-Data-Security-Program-v2022MAY04.pdf) states:

e. **Business continuity and disaster recovery (BCDR)**: SailPoint shall maintain formal BCDR plans that are regularly reviewed and updated to ensure SailPoint's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. **Data backups**: SailPoint shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

All backups are hosted in the UK, however, if an incident affects the UK the data may be moved to Dublin.

Microsoft Data Recovery Procedures

- On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered.
- Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located.
- Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data.
- Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Part 2, Section 2 – Lawfulness of processing – Articles 6, 9, and 10

2.2.1 Which Article 6 condition is being relied on to process the personal data?

☐ a) Consent of the data subject

The processing is **necessary:**

☐ b) for the performance of a contract (includes employment) – provide details below of the contract involved.

☐ c) for the compliance with a legal obligation – provide details of the relevant legislation below.

☐ d) in order to protect the vital interests of the data subject or other person

☒ e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (referred to as **public task**) – provide details of the public task below and any supporting legislation.

☐ f) for the purposes of the legitimate interests pursued by the controller or third party – provide details of the legitimate interest and whether a third part is involved.

SailPoint IdentityNow: The data being utilised is for the provision of identity management (the validation/verification that the subject represented by the identity is who they claim to be) and the provision of access rights (the ability to login to and utilise an application and the data hosted within it) that are appropriate and necessary for the person to undertake their duties and fulfil their obligations under the terms of their employment.
National Management Centre: The data being utilised is for the provision of a Cyber Threat protection solution.
Productivity Services: The data being processed relates to processing carried out in the public interest or as part of the role of SPA.

2.2.2. Does the processing involve criminal convictions etc.?

☒ Yes – Go to Q 2.2.3

☐ No – Go to Q 2.2.4

2.2.3 Will the processing of criminal convictions etc. data be carried out only in an official capacity either within or out-with SPA?

☒ Yes – provide further details of the processing below and state which Article 6 conditions applies (See conditions in Q 2.2.1)

☐ No – provide further details below and state which condition within Schedule 1 Parts 1, 2 or 3 will be met.

e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (referred to as **public task**).

The NEP solution will process a significant amount of sensitive personal data and

data relating to criminal activities and convictions. By way of example, the content of all emails passing through the system will be processed as well as team collaborative workspaces which could contain sensitive data relating to ongoing criminal investigations.

2.2.4 Does this project involve processing special category/criminal conviction data? If so, tick all categories below which apply.

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

2.2.5 If special category data is to be processed which Article 9 condition is being relied upon?

☐ a) explicit consent from the data subject

☐ b) processing relates to personal data manifestly made public by data subject

The processing is **necessary**

☐ c) to carry out obligations and exercising specific rights in relation to employment-state below the specific obligations or rights (of Police Scotland or the data subject) in connection with employment.

☐ d) to protect the vital interests of the data subject or another person and the data subject is physically or legally unable to give consent.

☐ e) for the establishment, exercise or defence of legal claims or under a court order

☒ f) for reasons of substantial public interest – see guidance notes and state below which of the condition(s) from Schedule 1 Part 2 apply

☐ g) other-provide another condition from Article 9 which is not listed above and the reason it applies.

Part 2, Section 3 – Measures contributing to the rights of the data subjects – Articles 12 to 19 and 21

2.3.1 Is the proposed processing already covered in a privacy notice?
☒ Yes ☐ No – State below whether a new privacy notice is required or whether an existing one can be amended, and if so which one.
https://www.spa.police.uk/privacy-policy/
2.3.2 Do individuals have an opportunity and / or right to decline to disclose or have their information shared?
☒ Yes ☐ No
In certain limited scenarios data subjects can object, the most common instance being the recording of video calls, where informed consent is sought.
2.3.3 How will you ensure that the personal data is available to Information Management for the processing of subject access requests?
The data which will be processed/shared via the solution originates primarily from SPA. In general terms, the solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access the personal data. The current Subject Access Request process still applies.
2.3.4 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?
The data which will be processed/shared via the solution originates primarily from SPA. In general terms, the solution will not change the nature or scope of the personal data which SPA routinely collect, process, or share with others today, it simply provides an improved, consistent, and more secure solution which can be used to store and access the personal data. The current Individual's Rights Request process still applies. SPA own and have access to all data stored on the Microsoft online services destined to be implemented through the O365 project in order that they can correct, delete, and suspend processing via the normal processes in place today. All source data used to construct identities within SailPoint IdentityNow are derived from an authoritative source rather than created within the solution itself. The processes inherent in that authoritative source (i.e. the SCoPE HR system) are utilised to ensure the rights under UK GDPR can be enacted and enforced. As a "downstream" service the IdentityNow platform receives those changes and applies them to the corresponding identities.

Part 2, Section 4 – Audit capabilities

2.4.1 Which of the following audit functionality will be included in the system? Check all that apply.
The ability to audit the following: ☒ data which has been collected ☒ data which has been altered ☒ data which has been viewed ☒ the identity of the person who has consulted (viewed) the data ☐ justification for, the date and time of the consultation (no justification) ☒ data which has been disclosed (electronically) ☒ the identity of the person who has disclosed the data ☐ the justification for, and the date and time of the disclosure ☒ the identity of the recipient(s) of the data ☒ details of data which has been combined ☒ the fact that data has been erased
2.4.2 If any of the above has not been checked, state below the reason.
O365 is an off the shelf product and does not comply with the current DPA requirements in Part 3 for Logging, however, the Data Use & Access Bill will remove the justification requirement. That said, these are not databases where people can view data they are not entitled to. For example, everyone has their own email account and other staff cannot access or view the content of that box. Where email is used to make a disclosure of data it is likely that the data will have come from a core system that has audit, although legacy systems may not have justification. SPA is currently procuring a new Core Operating system and the requirements of S62 are included in full in the requirements.

Part 2, Section 5 – Information Sharing

2.5.1 Is any of the data being processed to be shared with third parties? i.e. out-with SPA
☒ Yes – state below which 3rd parties ☐ No – go to question 2.6.1.
The solution will not change the nature or scope of the personal data which SPA routinely collects, processes, or shares with others today. NIAM is a centralised Identity Access Management platform managed by the UK Home Office and is used to control access to the various NLEDS applications. Whilst a very limited subset of personal information is shared with NIAM (e.g. email address, forename, surname, etc.) this data is used to facilitate access to those national applications. SPA will usually avoid using O365 Apps to make disclosures of Part 3 data. Egress, encrypted email, is used instead. SPA does not permit the recording of Teams calls.
2.5.2 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.
Information may be shared with 3rd parties. Where sharing occurs a Data Sharing Agreement will be in place. SPA shares on a limited basis. The Microsoft 365 product suite and contracts are procured directly through Phoenix Software Ltd acting on behalf of Microsoft as an elected Gold Partner. The contract between Phoenix Software and the SPA is attached below for reference: NFC141 Microsoft Contract_Scottish Po Microsoft's Worldwide Data Processing Addendum is also applicable (and is incorporated into Microsoft's standard Online Service Terms). This can be viewed view at the link below: Licensing Documents

Part 2, Section 6 – Data transfers outwith the UK – DPA Sections 72 to 78

2.6.1 Will the data be held in or transferred to a country without adequacy for either Part 2 or Part 3 processing?
☒ Yes – state which country / countries below ☐ No – go to question 2.6.4
SPA has the choice of where to store the data. At present this has been set to use UK South London. However, Microsoft have stated that they cannot guarantee that data will not be processed by sub-processors in other countries. The EEA has adequacy for both Part 2 and Part 3 processing. Some of the countries on the MS Sub-processor list have adequacy for Part 2, but other than the EEA, there is no adequacy for Part 3 data.
2.6.2 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.
MS advise that support from sub-processors uses a follow the sun model. They also advise that sub-processors would not be able to view content data without prior approval from MS. The transfers will be governed by Part 2 and Part 3 of the DPA and adequacy agreements are in place for some countries. It is simply not possible to separate out Part 2 and Part 3 processing as emails may contain either.
2.6.3 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.
The data will be encrypted by MS. This means MS hold the key and have the ability to decrypt the data. Data will be pseudonymised by MS, however, its unclear how they pseudonymise personal data that does not include a name.
2.6.4 Will the data be held in or transferred to a third country (i.e. outwith the EEA and the UK)?
☒ Yes – state which country / countries below ☐ No – go to question 2.7.1
MS provides a list of sub-processors here; Microsoft General - Online Services Subprocessors List (1.4.2023).pdf The list of MS sub-processors includes countries that the UK may regard as hostile, including China. MS is unable to give assurances that data will not be processed in those countries given their follow the sun support model. They have stated that IDTA's are in place, however, will not share the detail for confidentiality reasons. Thus, SPA cannot be assured that those assessments included both Part 2 and Part 3 processing.
2.6.5 For what purpose is the data held in / transferred to the country / countries listed above? Include any legislation or details of an adequacy decision which governs the transfer of the data.
See MS Online Services Sub-processors as above.
2.6.6 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.
Whitepaper

Part 2, Section 7 – Other privacy legislation

2.7.1 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
2.7.2 If any of the above apply, provide the relevant sections of the legislation
N/A

Human Rights Act 1998

2.7.3 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
SPA's processing will not affect Human Rights

2.7.4 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
2.7.5 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
2.7.6 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

2.7.7 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

2.7.8 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

2.7.9 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
It is possible that this right will be breached where content data is sent to hostile nations or nations without comparable rights.

2.7.10 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

2.7.11 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
It is possible that this right will be breached where content data is sent to hostile nations or nations without comparable rights.
2.7.12 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
2.7.13 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

2.7.14 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

Part 2, Section 8 – Consultation process with relevant stakeholders

2.8.1 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.
2.8.2 Who do you propose to consult on the proposed processing? List both internal and external organisations / individuals.
SPA Records Management Officer SPA SIRO SPA CEO PSoS SIRO Consultation is ongoing with Microsoft in connection with data sovereignty. Conversations with ICO have been ongoing for 2 years. KC's advice sought.
2.8.3 When do you propose to consult with the above organisations/individuals?
Consultations are ongoing
2.8.4 How do you intend to consult with the above organisations/individuals?
A combination of face-to-face and online meetings/workshops (e.g. MS Teams/Webex); emails; telephone calls; and formal agreements.

Part 3: Risk Assessment

Record the detail of any risks/mitigation, providing as much information as possible

1. **There is a risk that PSoS will implement weeding/retention rules or other controls without consulting SPA.**
   SPA and PSoS used to share a Record Retention SOP, however, the document was recently reviewed/updated without any consultation with SPA.

   Mitigation
   Ongoing communication with PSoS to ensure SPA has sight of all relevant policies, procedures and processes that may affect SPA processing**.**

2. **Office 365 does not offer full back up for data** (not to be confused with Geo redundancy).
   MS are clear that whilst they offer backup for specified apps for specified times data retention and integrity is the customers responsibility. Given that data will require to be backed up for longer than some of the MS enabled functionality, a solution must be in place. The solution for retrieving data is also complex via the Security and Compliance Centre. Searches for deleted files must be run on keywords using MS Content Search or eDiscovery. Data must then be exported in order to restore. Making actions such as restoring an entire mailbox problematic.

   Mitigation
   Key data to be backed up by PSoS.

3. **Microsoft is unable to supply evidence in order to comply with the requirements of S59 of the DPA 2018.**
   Section 59 states that 'the controller may only use a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to ensure that the processing will meet the requirements of THIS PART and ensure the protection of the rights and freedoms of the data subject'.

   There is no reference in Part 3 to the use of Standard Contractual Clauses to assure transfers. ICO guidance states;
   You can also transfer personal data to other recipients (who are not relevant authorities) if you meet some additional conditions and notify the ICO.
   If there is no 'adequacy decision' about the country, territory or sector for your restricted transfer, you may still make the transfer on the basis that other appropriate safeguards exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.
   Appropriate safeguards may be provided for by:
   1. a legal instrument providing appropriate safeguards which binds the intended recipient; or
   2. an assessment performed by the controller which concludes that

appropriate safeguards exist. In this case, you must inform the Information Commissioner of the categories of data transfers that take place.

You must document the transfer and provide this documentation to the Information Commissioner on request. You must record:

3. *the date and time of the transfer;*
4. *the name, and any other pertinent information about the recipient;*
5. *the justification for the transfer; and*
6. *a description of the data you transferred.*

You must ensure that any personal data you have transferred is not further transferred to another third country without your authorisation, or authorisation from another UK competent authority, and any authorisation can only be given where the transfer is necessary for any of the law enforcement purposes.

This advice reflects the requirements in Part 3 that the processing must be NECESSARY for a Law Enforcement Purpose or must be covered by an adequacy agreement and every single time a transfer is made to a country without adequacy/not for a LE purpose the ICO must be notified. However, MS will not notify SPA when it transfers data to such a country and it is, therefore, not possible to comply with this requirement.

It is also not possible for SPA to assess the safeguards of the rights and freedoms of data subjects in such countries, particularly where they may be deemed as hostile.

S59(5) – The processing by the processor must be governed by a contract in writing between the Controller and the Processor setting out the following;

a. *the subject matter and duration of the processing*
b. *the nature and purpose of the processing*
c. *the type of personal data and categories of data subjects involved*
d. *the obligations and rights of the controller and processor*

It is not possible for SPA to fulfil this requirement. There is no contract, per se with MS. Users either accept MS T's and C's, including the DPAdd or don't. As such the nature and purpose of the processing and the type and category of data subjects cannot be met in full.

The MS DPAdd refers only to GDPR. There is no mention of the Data Protection Act 2018 or UKGDPR. SPA has requested that MS provide an ancillary document, like that provided to Axon via the DESC project, that will specify that the data will fall under UKGDPR and DPA 2018. Whilst this affords some level of assurance it falls short of the S59(5)(b) and (c) requirements.

S59(6) - The contract must, in particular, provide that the processor must—

(a) act only on instructions from the controller,

(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality,

(c) assist the controller by any appropriate means to ensure compliance with the rights of the data subject under this Part,

(d)at the end of the provision of services by the processor to the controller—
(i)either delete or return to the controller (at the choice of the controller) the personal data to which the services relate, and
(ii)delete copies of the personal data unless subject to a legal obligation to store the copies,
(e)make available to the controller all information necessary to demonstrate compliance with this section, and
(f)comply with the requirements of this section for engaging sub-processors.

S59(7) The terms included in the contract in accordance with subsection (6)(a) must provide that the processor may transfer personal data to a third country or international organisation only if instructed by the controller to make the particular transfer.

SPA cannot comply with this section as MS is unable to specify what data originating from SPA will be processed outside the UK for support functions. In order to try and mitigate this risk SPA asked to see TRA/IDTA for the countries used by MS where there is no adequacy. MS declined to provide the assessments.

SPA does not issue a contract, the Controller must accept MS T's & C's, including the DPAdd. In which case there is no method whereby the data will only be transferred if instructed to do so.

Microsoft will not confirm if our data (for support purposes) will be processed in any 'hostile' countries or countries without adequacy. Countries without adequacy listed on Microsoft Sub-Processors list include;

China
Serbia
India
South Africa
UAE
Chile
Hong Kong
Brazil
Egypt
Malaysia

No region is provided for processing undertaken by AWS.

MS has declined, due to confidentiality, to provide SPA with the assurances it needs for those transfers, including International Data Transfer Agreements.

Issues for Rights and Freedoms of Individual

China

1. *Government surveillance and State access*
   Chinese law (e.g., the 2017 National Intelligence Law) can compel companies to share data with Chinese authorities upon request. This can happen without judicial oversight raising serious concerns about the lack of transparency, lack of recourse for UK data subjects and indiscriminate surveillance.

2. *Inability to exercise data subject rights*
   The rights to access any data, rectify it, erasure and objection are unlikely to be effective or enforceable in China.

3. *Lack of independent oversight*
   There is no independent data protection authority with comparable powers, this may lead to lack of accountability for data misuse or breaches.

4. *Risk of Re-identification or Misuse*
   Data transferred to China could be used for profiling, surveillance or blacklisting. It may be combined with other data sets to re-identify pseudonymised data. This would be of particular concern for sensitive data.

5. *Transparency*
   Under UK law individuals must be informed about where their data is going and why. As MS will not provide this information, transparency cannot be achieved.

6. *Sector specific concerns for SPA.*
   Transferring data to China could pose National Security Risks, risks to ongoing investigations, Human Rights concerns (such as the repression of Uyghurs and political dissidents).

   The DPC enquiry fined TikTok for failing to verify, guarantee and demonstrate that personal data of EEA users, remotely accessed by staff in China, was afforded a level of protection equivalent to that guaranteed within the EU.

Serbia

1. *Legal and Regulatory Differences*
   While Serbia has implemented data protection laws that are largely aligned with the GDPR, its framework may lack the same level of rigor and enforcement found in the UK.
   UK data subjects may not enjoy equivalent protections, such as limits on data processing or consent. Serbia's legislation does not reflect some GDPR protections regarding government access to data or remedies for data subjects.

2. *Weaker Enforcement & Remedies*
   Serbian Data Protection Authority (Povernik) is active but may lack adequate resources or authority to effectively enforce rules or investigate breaches. UK individuals might find it difficult to lodge complaints or seek redress, especially in cases involving complex processing.

3. *Data Access by Government Authorities*
   Serbian law allows state bodies to access personal data for law enforcement and national security reasons. There may be insufficient legal safeguards or transparency, making it harder for UK subjects to challenge excessive surveillance or improper use of their data.

4. *Security of Data Handling*
   There may be variability in cybersecurity standards or organisational practice across Serbian data processors or controllers. However, it expected that MS partners and sub-processors will have to meet a high standard set by Microsoft. Without seeing the SCC's/IDTA's and TRA we cannot be sure what exactly that is.

India

1. *Lack of Comprehensive Data protection Law*
   India does not currently have a GDPR equivalent framework in place. While the Digital Personal Data Protection Act 2023 has been passed, it is not yet fully implemented and is still evolving. Data subjects may not benefit from key GDPR principles like purpose limitation, data minimisation and consent requirements.

3. *Limited Oversight and Enforcement*
   India's proposed Data Protection Board is not yet operational, and its independence and enforcement powers are not clear. Data subjects may have limited or no recourse in case of data misuse, breaches or illegal processing.

4. *Government Access to Data*
   India has broad laws allowing state surveillance and access to private data e.g. Under the Information Technology Act and telecom regulations**.** This means that UK data may be accessed without adequate safeguards, judicial oversight and transparency**.**

5. *Inconsistent Security Practice*
   Security standards vary widely across organisations and sectors.

6. *Lack of Data Subject Rights*
   Under the DPDPA rights are more limited than under UK data protection legislation.

7. *Cultural & Legal Differences*
   Differences in how privacy is culturally and legally interpreted may result in different thresholds for what constitutes harm, consent or fair use.

South Africa

1. *Differences between POPIA and UK GDPR*
   South Africa's Protection of Personal Information Act (POPIA) provides a data protection framework, but it has fewer and less detailed rights. The definition of lawful processing is also broader.

2. *Weaker Enforcement and Remedies*
   South Africa's Information Regulator is relatively new and has limited resources. Enforcement may be slow.

3. *Security Breach Notification*
   While POPIA requires reasonable security measures and breach notification, security may vary widely by organisation.

4. *Government Surveillance and Access*
   South Africa permits interception and monitoring of communications for national security and law enforcement under laws like Regulation of Interception of Communications Act. Thus, UK data may be accessed by public bodies without the same safeguards or judicial oversight required in the UK.

United Arab Emirates

1. *Inadequate Legal Protection*
   UAE has limited Data Subject rights Their data protection laws (e.g., Federal Decree-Law No. 45 of 2021) are relatively new and do not guarantee the same level of rights (e.g. access, rectification, erasure, objection) as the UK GDPR.

2. *Weak Regulatory Oversight*
   While the UAE has established data protection authorities (such as under the DIFC and ADGM free zones), enforcement outside of these zones can be limited or inconsistent.UK data subjects may find it difficult to seek redress or lodge complaints if their data is misused or breached once in the UAE.

3. *Government Surveillance and Access*
   Broad State Powers: UAE authorities have broad powers to access personal data, particularly for national security or law enforcement purposes, with limited transparency or judicial oversight.
   Lack of Independent Oversight: Unlike the UK, the UAE does not have an independent body with strong oversight powers to control or review surveillance activities.

4. *Re-identification and Misuse of Data*
   Data that is believed to be anonymised under UK standards might not be treated the same way in the UAE, increasing re-identification risk.
   Secondary Use: There may be fewer legal restrictions on secondary use or onward transfers of data to third parties, including other countries.

5. *Contractual and Operational Risks*
   Standard contractual clauses or binding corporate rules may be harder to enforce or interpret in the UAE context. Data breach notification obligations and enforcement are not as mature or robust in the UAE, potentially delaying mitigation for affected individuals**.**

6. *Human Rights*
   The broader human rights environment in the UAE, including restrictions on free speech, press freedom, and political dissent, may compound risks if personal data is misused for profiling or surveillance.

Chile

1. *Lack of Adequate Legal Protections*
   Chile does not currently have data protection laws equivalent to those in the UK. This means data subjects may not have enforceable rights (e.g. to access, correct, or delete their data). There may be fewer obligations on Chilean organisations to process data fairly, transparently and for limited purposes.

2. *Limited Oversight and Enforcement*
   Chile's data protection authority (Consejo para Transparencia) has limited enforcement powers compared to the UK's ICO.
   Individuals may have less recourse if their data is misused or mishandled.

3. *Government Access and Surveillance*
   There may be a risk of disproportionate or opaque government access to personal data without sufficient safeguards or redress mechanisms for UK citizens.

4. *Security Standards*
   Organisations in Chile may not be subject to the same strict cybersecurity and data breach notification requirements as in the UK. This increases the risk of data breaches or unauthorised access.

5. *Challenges in Exercising Rights*
   UK data subjects may find it harder to exercise their data protection rights (e.g. to complain, object to processing, or seek compensation) across jurisdictions. Language, legal system differences, and lack of bilateral enforcement mechanisms may add barriers.

Hong Kong

1. *Government Surveillance and Interference*
   Since the enactment of the Hong Kong National Security Law in 2020, there are increased powers for government authorities to compel access to data. UK data subjects' information may be accessed by Hong Kong or Chinese authorities without robust legal safeguards or recourse.

2. *Weak Enforcement of Data Subject Rights*
   Issue: While Hong Kong has the Personal Data (Privacy) Ordinance

(PDPO), it lacks many of the explicit rights found in the UK GDPR. Data subjects may not be able to exercise the same level of control over their data once it's transferred.

3. *Limited Legal Redress*
   UK data subjects may have difficulty seeking compensation or legal remedies in Hong Kong if their data rights are infringed. This undermines the UK GDPR principle of effective judicial remedy.

4. *Lack of Independent Supervisory Authority*
   The Office of the Privacy Commissioner for Personal Data (PCPD) in Hong Kong has limited enforcement power compared to the UK's Information Commissioner's Office (ICO). Lower regulatory oversight may reduce accountability for data misuse or breaches.

6. *Data Security Standards*
   Hong Kong's cybersecurity laws and standards may not match UK expectations, especially regarding breach reporting and security-by-design requirements. This increases vulnerability to data breaches or unauthorised access.

Brazil

1. *Enforcement and Redress Challenges*
   UK data subjects may struggle to enforce their rights in Brazil due to jurisdictional issues, language barriers, and limited access to effective legal remedies. The Brazilian regulator (ANPD) is still relatively new (established in 2020) and may not have the same enforcement powers or maturity as the UK's ICO.

2. *Different Legal Bases and Data Subject Rights*
   Brazil's LGPD (Lei Geral de Proteção de Dados) does offer many rights similar to the UK GDPR, but differences in implementation, interpretation, and enforcement could result in weaker protection. For example, the concept of "legitimate interest" is less developed in Brazilian law, potentially affecting how data controllers justify processing.

3. *Government Access and Surveillance*
   There may be concerns around state surveillance or access to personal data by Brazilian authorities without adequate safeguards or oversight. UK GDPR requires that public authority access in third countries must be proportionate and subject to independent oversight—this may not be fully assured in Brazil.

4. *Security Risks and Data Breach Handling*
   Variations in cybersecurity standards and incident response requirements between countries can expose UK data to greater risk. While the LGPD includes breach notification rules, response times and expectations differ, possibly leading to delayed awareness of breaches affecting UK individuals.

5. *Onward Transfers*
   Data transferred to Brazil could be further transferred to other countries that offer even less protection, unless specific controls are in place. UK law requires that any onward transfer must maintain equivalent safeguards, which may not be enforced rigorously in Brazil.

Egypt

1. *Weak Enforcement Mechanisms*
   Enforcement of data protection rights in Egypt may be limited, inconsistent, or influenced by state interests. UK individuals may struggle to enforce their rights or seek redress in Egypt if their data is mishandled.

2. *Surveillance and State Access*
   Egyptian authorities have broad powers to access data for national security reasons, often without meaningful judicial oversight. This raises risks of unlawful access, particularly if the data involves political views, activism, or sensitive communications.

3. *Lack of Independent Oversight*
   Although Egypt established a data protection authority, questions remain about its independence and practical authority. Data subjects may have no effective way to challenge decisions or actions taken by Egyptian processors or controllers.

4. *Incompatibility with UK Data Subject Rights*
   UK data subjects enjoy extensive rights (access, rectification, erasure objection, etc.) under the UK GDPR. These rights may not be fully recognized or enforceable once the data is transferred to Egypt.

5. *Increased Risk of Data Breaches or Misuse*
   Differences in cybersecurity standards and practices can expose transferred data to higher risk of breaches, leaks, or unauthorised processing.

Malaysia

1. *Limited Enforcement and Redress Mechanisms*
   UK data subjects may struggle to enforce their rights or seek compensation if their data is misused in Malaysia. The Malaysian Personal Data Protection Commissioner does not have the same enforcement powers as the UK Information Commissioner's Office (ICO).

2. *Risks of Surveillance and Government Access*
   Malaysian authorities may have broad powers to access data for national security or law enforcement purposes without the same safeguards and oversight mechanisms found in the UK. There may be no equivalent to the UK's protections against disproportionate government surveillance (e.g. under the Investigatory Powers Act or judicial oversight).

3. *Incompatibility of Legal Frameworks*
   The Malaysian PDPA applies only to commercial transactions and does not apply to government bodies. This creates a significant gap in data protection coverage compared to the UK GDPR, which applies more broadly.

It should be noted that the above represent the sub-processors on the Microsoft list that do not have UK GDPR adequacy. There are a significant volume that have UK GDPR Adequacy, but not Part 3. Part 3 does not specify that the controls in Part 2 are suitable for Part 3 processing.

Possible Mitigations

Mitigation measures are limited.

Should SPA get sight of TRA's, IDTA's and SCC's and how staff in sub-processors are vetted it may give us a measure of confidence. However, this information cannot be supplied by Microsoft for reasons of confidentiality.

Appendix 2 relates to security incidents reported by Microsoft since 2022. The data shows that, despite all their controls, data can still be compromised by state actors.

4. Transfers to the above nations may not be compliant with S73/75/77 DPA 2018.

The relevant legal framework for transferring Law Enforcement data outside of the UK is Part 3 of the Data Protection Act 2018. Thus, SCC's/BCC and IDTA's are not relevant as per ICO guidance;

International data transfer agreement and guidance | ICO
International transfers | ICO

1. The sub-processors are not Relevant Authorities
2. The transfer is not necessary for a Law Enforcement Purpose
3. The countries do not have adequacy.
4. There is no way of SPA knowing when transfers are made and what data is in those transfers and as such notification of the transfers to ICO would not be possible.
5. There is no immediate threat warranting the transfer.
6. It is not possible for SPA to assess whether appropriate safeguards are in place, particularly since we cannot see the agreements in place between the processor and sub-processors.

SPA has been consulting with ICO for 2 years in respect of the use of Hyperscale Cloud providers for Law Enforcement Data.

On 2nd April 2024 advice was received from Emily Keaney, ICO, around international transfers in the DESC programme. This advice related to the use of Azure by a processor. This DPIA is for O365, which operates in a different

manner from Azure storage. Microsoft themselves state they cannot give us the guarantees around international transfers that they can for Azure, as O365 works in a very different manner.

However, considering the ICO guidance for Azure, SPA could still not meet the mitigations as suggested in the ICO correspondence. The correspondence points to mitigation in S75 of Part 3 DPA 2018. However, SPA cannot get beyond Section 73(4) of Part 3, a requirement BEFORE Section 75 can be considered.

S73*(4)*

(a) the intended recipient is a relevant authority in a third country or an international organisation that is a relevant international organisation, or
(b) in a case where the controller is a competent authority specified in any of paragraphs 5 to 17, 21, 24 to 28, 34 to 51, 54 and 56 of Schedule 7— SPA does not meet this critera
(i) the intended recipient is a person in a third country other than a relevant authority, and
(ii) the additional conditions in section 77 are met. SPA (unlike PSoS) cannot meet the requirements of S73, thus cannot proceed to S75/77.

The Data Use and Access Bill (DUAB) proposes changes to this section of the DPA 2018, specifically in relation to the issues above. If it were legal to make the transfers in the current legislation, it's unclear why DUAB seeks to change the text.

Possible Mitigations;

1. *Use of Lockbox*
   If PSoS/SPA were to use the Microsoft Lockbox functionality, then Microsoft engineers could not access our data without consent every time. However, Microsoft state that Lockbox 'does not protect against data requests from law enforcement agencies or other 3rd Parties', thus reducing the value of Lockbox as a mitigation.

2. *Customer encryption*
   SPA/PSoS could use their own encryption and manage the key. Thus, Microsoft would not be able to access data for any reason without PSoS/SPA.

   If customer encryption was utilised the performance of the products may be impacted. Furthermore, Microsoft may be unable to take immediate action to manage a threat/issue without our assistance. This delay could affect availability.

   Managing encryption keys is not without risk. This requires either a 3rd party key management company (who could access the data) or an in-house crypto custodian. Managing encryption keys itself can present the following risks;

2.1 Key Loss
If you lose your encryption keys, you lose access to your data permanently. There is no way to recover encrypted data without the correct keys. This is especially critical for:

- Backup data
- Encrypted devices
- Encrypted cloud storage

2.2 Poor Key Storage Practices
Improper storage (e.g. storing keys in plaintext, on unprotected devices, or in easily accessible locations) can lead to unauthorised access.

- Risks include theft, loss, or malware infections.
- Many breaches have occurred because keys were stored alongside the encrypted data.

2.3. Human Error
Manual management increases the chance of mistakes:

- Using weak passwords to protect keys
- Misconfiguring encryption algorithms
- Accidentally deleting or overwriting keys

2.4. Key Exposure
Without strong operational security:

- Keys can be leaked via email, chat, or unencrypted file transfers.
- Developers may accidentally commit them to code repositories (e.g., GitHub).

2.5. Insufficient Key Rotation
Failure to regularly rotate keys can expose data if a key is compromised. Manual key rotation is often forgotten or improperly done, increasing the window of vulnerability.

2.6. No Built-in Redundancy
Professional key management systems (KMS) offer automatic backups, recovery, and failover. If you're managing your own keys and something goes wrong (e.g., hardware failure), there's no safety net unless you've implemented one.

2.7. Scalability Issues
As your organisation or system grows, managing keys across multiple environments and users becomes complex and error-prone without automation and centralised management.

Summary:

Managing your own encryption keys is high risk unless you have strong

security practices and infrastructure. As PSoS deliver SPA ICT they would be responsible for the overheads with managing keys.

Self-Managed Keys

Area	Pros	Cons
Control	Full control over key generation, storage, access, and policies.	You are solely responsible for everything; no fallback.
Security	Can be extremely secure if implemented well (e.g., air-gapped HSMs).	High risk of misconfiguration, theft, or loss; requires expert knowledge.
Compliance	May be necessary for certain highly regulated environments.	Easy to fall short of regulatory standards without audit trails and automation
Availability	We decide key access rules, redundancy, and uptime strategies	Needs robust planning for disaster recovery, backup, and failover
Cost	No recurring service fees if done in-house	High upfront costs for hardware, training, and ongoing maintenance
Scalability	Customisable to specific needs	Doesn't scale easily; complex to manage across teams, regions, or applications
Integration	Can be integrated with legacy or custom systems	May lack plug-and-play integration with modern SaaS/Cloud tools

Cloud Managed Encryption Keys

Area	Pros	Cons
Control	Still retains policy and access control, though the provider manages infrastructure.	Less direct control over physical storage and key lifecycle
Security	Provider ensures physical and logical security, access logging, and compliance.	Shared responsibility model—misconfigurations (e.g., IAM roles) are still a risk
Compliance	Supports industry standards (e.g., FIPS 140-2, ISO, GDPR, HIPAA).	Trust in cloud provider is essential; not suitable for all regulatory frameworks.
Availability	Built-in redundancy, failover, and durability	Depends on provider uptime and your cloud

		service region.
Cost	Pay-as-you-go pricing; efficient at scale	Costs can add up with many keys, operations, and high usage.
Scalability	Designed to handle massive workloads and multi-region deployments.	Can lead to vendor lock-in; migration can be complex.
Integration	Native integration with cloud services, APIs, and identity tools.	Less customisable than self-managed solutions in some edge cases.

Given the experience of Microsoft in managing keys and their 24/7/365 availability, it makes sense to allow Microsoft to manage encryption to ensure no loss of availability.

However, this brings its own risks in terms of access via CLOUD Act/FISA.

5. Risk of Using a Cloud Subject to CLOUD Act

1. *Data Sovereignty Concerns*
   Microsoft has acknowledged that it cannot guarantee UK policing data stored in its Microsoft 365 platforms will remain within the UK or countries with adequacy. This is due to the inherent architecture of its hyperscale public cloud infrastructure, which involves regular international data transfers for service continuity. Such transfers may contravene the UK's Data Protection Act 2018, which mandates that law enforcement data remain under UK jurisdiction unless specific safeguards are in place. SPA is unable to avail itself of those safeguards due to the fact it cannot move beyond S73 DPA 2018.

2. *Exposure Under the U.S. CLOUD Act*
   The CLOUD Act allows U.S. law enforcement to compel U.S. based companies, like Microsoft, to provide data stored on servers globally, provided the data is under their control. This means UK law enforcement data stored in Microsoft's cloud could be subject to U.S. legal requests, potentially conflicting with UK data protection laws and raising national security concerns.

   From Microsoft website;
   In the first half of 2024, Microsoft received 166 total requests from law enforcement around the world for accounts associated with enterprise cloud customers. Of those 166 requests:
   - In 118 cases (71%), the requests were rejected, withdrawn, no data was available, or law enforcement was successfully redirected to the customer.
   - In 48 cases (29%), Microsoft was compelled to provide responsive information:
   - In 27 cases, Microsoft were required to disclose customer content.

Sixteen of such disclosures were associated with U.S. law enforcement.

Whilst there is evidence that Microsoft will challenge requests where they believe a formal path exists, pointing requestors to the Data Controller, Microsoft can be issued with a gagging order that prevents them from telling us that data has been/is to be accessed. Without knowledge of the request, we are unable to verify the accuracy of the data prior to any potential use by the US authorities.

3. *Regulatory Ambiguity*
The UK's Information Commissioner's Office (ICO) has suggested that UK police may use cloud services processing data overseas if "appropriate protections" are in place. However, the lack of clear definitions for these protections creates uncertainty and potential legal vulnerabilities for law enforcement agencies.

4. *Suspension of Accounts*
There is evidence that the current US administration is flexing its reach in terms of Microsoft Accounts for its adversaries.

The networker: Microsoft shutting down email accounts of ...

5. *Security of Data*
Given the significant amount of sensitive public sector data being processed on Microsoft worldwide, it is a focus of interest for Foreign Intelligence and criminals. The below articles provide further background.

Federal agencies' emails caught up in latest Microsoft hack, CISA says
U.S. government board calls Microsoft's security practices "inadequate"
Chinese hackers accessed US government email accounts - Microsoft – The Irish Times
Hackers Exploiting Microsoft 365 OAuth Workflows to Target Organizations

6. FISA S702

1. *Warrantless Access to Non-U.S. Data*
Under Section 702, U.S. intelligence agencies like the NSA can compel U.S.-based cloud providers, including Microsoft, to disclose data pertaining to non-U.S. persons located outside the United States. This access does not require individual warrants or probable cause, allowing for the collection of data for foreign intelligence purposes.

2. *Limited Transparency and Oversight* FISA 702
Orders are issued through a secretive court process, and providers are often prohibited from disclosing the existence or details of such orders. This lack of transparency makes it challenging for UK data subjects to ascertain whether their data has been accessed or to seek redress.

3. *Conflict with UK and EU Data Protection Laws*
The broad surveillance powers granted under FISA 702 have been found

to conflict with the General Data Protection Regulation (GDPR) principles, particularly concerning adequate protection and legal remedies for data subjects. The Court of Justice of the European Union (CJEU) has previously invalidated data transfer mechanisms like Privacy Shield due to such conflicts.

4. *Expanded Definition of Service Providers*
   Recent legislative changes have broadened the definition of "electronic communications service providers" under FISA 702, potentially encompassing a wider range of entities, including data centres and other infrastructure providers. This expansion increases the scope of entities that can be compelled to assist in surveillance activities.

7. Article 10 UK GDPR

Processing by SPA using Microsoft 365 (M365) does not inherently breach Article 10 of the UK GDPR, but it can raise legal and compliance risks depending on how it is implemented.

Article 10 governs the processing of personal data relating to criminal convictions and offences. It states:

"Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by UK law providing for appropriate safeguards for the rights and freedoms of data subjects."

In the UK, Part 3 of the Data Protection Act 2018 (DPA 2018) applies specifically to law enforcement processing.

Law Enforcement use of Microsoft 365 to process sensitive data, including criminal offence data, can be lawful if:

1. The processing is under official authority (i.e. police statutory powers).
2. Appropriate safeguards are in place under Part 3 DPA 2018.
3. Data security and confidentiality are robust and compliant with the principles in Article 5 UK GDPR (e.g. integrity and confidentiality).
4. Data is stored and processed within appropriate jurisdictions (e.g. within the UK or countries with adequate protection).
5. There are clear Data Processing Agreements (DPAs) in place with Microsoft that define responsibilities and restrict Microsoft from using the data beyond the service delivery context.

Where SPA are authorised to process such data, they can breach Article 10 if:

- Microsoft is allowed to access, process or transfer criminal offence data without proper legal basis or safeguards.
- Data is transferred to jurisdictions (like the U.S.) without sufficient safeguards or legal instruments (e.g., UK–US Data Bridge or Standard Contractual Clauses).

- Microsoft acts in a way that is not just a data processor, but also a controller, creating independent purposes for data use.

There is ongoing scrutiny around whether large U.S. Cloud providers can ever provide an adequate level of protection for sensitive law enforcement data under the UK GDPR.

Summary

Using M365 is not automatically a breach of Article 10 UK GDPR. However, it could be, if criminal offence data is not processed with the required legal controls, safeguards, and oversight.

Risk Summary

Microsoft 365 is not a database per se, so there is an argument that access to the data may not provide large scale sensitive personal data and as such the apps may not be targeted. However, SPA has undertaken a Data Governance Project encompassing the content of email boxes and SharePoint sites.

Despite clear instructions that email boxes must not be used as a filing system, staff continue to allow email boxes to grow. A cap for new staff has been implemented, but this will still allow a significant volume of data to be stored in email accounts. A large percentage of those emails will contain Part 3 data.

SPA has provided clear guidance that SharePoint must not be used for Part 3 data. However, SPA IM recently established that Forensic Services and Police Scotland have been using SharePoint since 2013 to share case data in major crimes. This was undertaken without SPA or PSoS Information Managements consent/knowledge. Whilst this data will not be moved to the Cloud based SharePoint application, there is a concern that some data may be re-added by staff. SPA IM will look at the feasibility of dip sampling the content going forward.

It is for these reasons that SPA has some concerns about the move to Cloud and 3rd party access to this data. SPA is fully aware that it is our responsibility to manage this risk.

Human Rights Legislation

In light of the sanctions imposed on the Microsoft account of the Chief Prosecutor of the International Criminal Court, followed on the 5th June by the designation of another 4 ICC judges, SPA has concerns about the protection of UK citizens and the practices being deployed by the US administration.

Whilst SPA has no risk factor in these sanctions, close monitoring will be undertaken to establish if a risk of SPA staff being sanctioned could be a possibility in the future. SPA forensics staff are sometimes cited to give evidence in the USA.

Additional Relevant Information

EDPS

The European Data Protection Supervisor (EDPS) found that the European Commission's use of Microsoft 365 infringed several data protection rules, particularly concerning the transfer of personal data outside the EU/EEA without adequate safeguards. The EDPS ordered the Commission to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and its affiliates located in countries outside the EU/EEA not covered by an adequacy decision, effective December 9, 2024.

The EDPS highlighted that the Commission's contract with Microsoft lacked specificity regarding the types of personal data collected and the explicit purposes for their collection. Public authorities should ensure that their agreements with service providers like Microsoft clearly define data categories and processing purposes to comply with data protection regulations.

Microsoft's Response to the EDPS Ruling

Microsoft has consistently maintained that it has not provided EU public sector customer data to any government. In light of the EDPS's findings, Microsoft has implemented measures to enhance data protection and compliance:

- EU Data Boundary Initiative: Microsoft announced a phased plan to enable all personal data of its European cloud customers, including automated system logs, to be stored and processed within the EU. This initiative aims to minimize data transfers outside the EU and enhance data sovereignty for European customers.
- Contractual Clarifications: Microsoft has worked on clarifying its contractual terms with customers, ensuring that the types of personal data collected and the purposes for processing are explicitly defined. This effort addresses the EDPS's concern about the lack of specificity in data processing agreements.
- Legal Challenge: Both Microsoft and the European Commission have filed complaints against the EDPS's decision, contesting the findings and the interpretation of data protection obligations. The outcomes of these legal proceedings may further influence Microsoft's compliance strategies.

  It should be noted that this remedy is **NOT** available to the UK. Thus, data subjects in the UK could be considered to have less protection.

  ### Microsoft Position - O365 for Law Enforcement

  Microsoft states in their own risk factors that O365 is not designed for processing the data that will be ingested by SPA.

  Microsoft does not state that Microsoft 365 (O365) is unsuitable for high-value processing (such as offending-related data), but rather they provide guidance and caveats regarding compliance, security, and regulatory requirements when processing sensitive or high-risk data, especially in

sectors like law enforcement, criminal justice, and national security.

1. Compliance with Regulatory Standards

Offending data in the UK is considered "special category" or "sensitive processing" under:

- UK GDPR Articles 9 and 10
- Data Protection Act 2018 (DPA 2018), Part 3, for law enforcement processing

This kind of data requires specific safeguards, such as:

- Lawful basis under Article 10 (criminal offence data)
- Policies on data retention, access, and security
- Proven protection against misuse and unauthorised access

O365 can technically support this, but only with correct configuration, policies, and third-party assurances. Microsoft warns that without these in place, its default configurations may fall short.

2. Data Residency and Sovereignty

Offending and criminal justice data often require guarantees about where the data is stored and processed.

Even though Microsoft offers UK data centres, O365 services may still involve:

- Global data transfers (for support, telemetry, etc.)
- Backup or processing outside the UK or EU

This could conflict with local data sovereignty requirements — for example, under the UK Law Enforcement Directive (LED).

3. Shared Responsibility Model

Microsoft follows a shared responsibility model, where:

- Microsoft secures the infrastructure
- The customer is responsible for configuring data protection, access control, compliance policies, etc.

If O365 is not set up properly (e.g. with Information Protection, Customer Lockbox, Purview, conditional access), it might not meet the high standards required for handling offending data securely. That said, Lockbox does not mitigate all the risks.

Summary

Microsoft 365 can be used for high-value data like offending information, but only if it's configured and governed appropriately — and that bar is high. Microsoft is cautious and advises organisations to:

- Perform data protection impact assessments (DPIAs)
- Review law enforcement or justice-specific compliance frameworks
- Implement advanced security and compliance tools
- Seek legal and regulatory advice

SPA has conducted a DPIA, reviewed the relevant legislation and sought Kings Counsels advice in respect of the use of Microsoft Hyperscale Cloud.

Appendix 1 – Risk Assessment

Scoring

Impact \ Likelihood	Rare	Unlikely	Possible	Likely	Highly Likely
Severe	5 Medium	10 Medium High	15 High	20 Very High	25 Very High
Major	4 Low	8 Medium	12 Medium High	16 High	20 Very High
Moderate	3 Low	6 Medium	9 Medium	12 Medium High	15 High
Minor	2 Low	4 Low	6 Medium	8 Medium	10 Medium High
Minimal	1 Low	2 Low	3 Low	4 Low	5 Medium

1-4 Low

- Minimal or no impact on individuals.
- Examples:
    - Disclosure of fully anonymised data.
    - Internal processing of low-sensitivity personal data (e.g., work email addresses) with strict controls.
- Impact on Rights/Freedoms:
    - No infringement of rights.
    - No distress, loss, or disadvantage to the data subject.
    - No notification required.

5-9 Medium

- Slight inconvenience or irritation to individuals.
- Examples:
    - Incorrect but easily corrected contact information.
    - Limited and reversible exposure of low-risk data.
- Impact on Rights/Freedoms:
    - Minor temporary impact (e.g., delay in service).
    - No long-term consequences.
    - Unlikely to require breach notification unless repeated/systemic.

10-14 Medium High Impact

- Noticeable impact with potential for short-term consequences.
- Examples:
    - Exposure of contact details combined with minor sensitive data (e.g., appointment for a routine checkup).
    - Delay or denial of access to a service.
- Impact on Rights/Freedoms:
    - Possible distress, embarrassment, or inconvenience.
    - May impair an individual's ability to exercise a right temporarily.
    - DPIA and/or breach notification to ICO/data subjects may be required depending on likelihood.

15 -19 High

- Serious impact on the individual's rights and freedoms.
- Examples:
    - Unauthorised disclosure of health, financial, or criminal records.
    - Misuse of data resulting in discrimination or identity theft.
    - Unlawful processing or transfer of data
- Impact on Rights/Freedoms:
    - Real risk of significant harm: financial, reputational, or psychological.
    - Could impact freedom of movement, expression, or access to services.
    - Likely to require a DPIA and notification to both ICO and individuals.

20-25 Very High

- Severe or irreversible harm to individuals.
- Examples:
    - Exposure of highly sensitive data leading to stalking, blackmail, or physical harm.
    - Systemic profiling or surveillance with discriminatory outcomes.
- Impact on Rights/Freedoms:
    - Long-term or irreversible damage to autonomy, privacy, reputation, or safety.
    - Serious infringement of GDPR rights (e.g., unlawful automated decision-making).
    - Mandatory DPIA, high regulatory scrutiny, and legal liability likely.

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Rare 2. Unlikely 3. Possible 4. Likely 5. Highly Likely	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low 1-4 Med: 5-9 Med High 10-14 High: 15-19 V High: 20-25		Eliminated Reduced Accepted		Yes No
1	There is a risk that PSoS will implement weeding/retention or other controls in O365 without consulting SPA or fail to advise of relevant issues.	3	3	9 Medium	Ensure ongoing dialogue with PSoS IA and ISO to ensure that SPA is sighted on any material changes/decisions in terms of the deployment, use and functionality of O365	Reduced	Low	Yes
2	Office 365 does not offer full back up for data (not to be confused with Geo redundancy).	5	4	20 Very High	PSoS will deliver back up (and any additional services required) in time for go live	Eliminated	N/A	
3	SPA is unable to determine compliance with Part 3 and in particular S59 and the use of sub-processors in countries without adequacy.	5	3	15 High	No current mitigation, although dialogue continues with MS	No change	High	

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Rare 2. Unlikely 3. Possible 4. Likely 5. Highly Likely	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low 1-4 Med: 5-9 Med High 10-14 High: 15-19 V High: 20-25		Eliminated Reduced Accepted		Yes No
4	Compliance with S73 DPA 2018. Microsoft is unable to specify what, if any, of our data will be processed in any 'hostile' countries or countries without adequacy due to their follow the sun support model. SPA is unable to take advantage of the S75/77 mitigations suggested by ICO as we are unable to move past S73.	5	3	15 High	No current mitigation, although the Data Use & Access Bill will partially remedy this issue when enacted. The final mitigation will be MS signing the Code of Conduct as per DUAB.	No Change	High	
5	CLOUD Act remains a threat given the ability for the USA to require MS to provide them with customer data in response to a Court Order. The Order could include a gagging clause meaning we would be unsighted/unable	3	5	15 High	There is evidence that Microsoft will challenge requests where appropriate and will always act in the customers interests. However, they will be unable	No change	High	

	Step 6 – Assess the risk Explain the risk and score them				Step 6: Identify Measures to Manage Risk Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Rare 2. Unlikely 3. Possible 4. Likely 5. Highly Likely	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low 1-4 Med: 5-9 Med High 10-14 High: 15-19 V High: 20-25		Eliminated Reduced Accepted		Yes No
	to challenge. Current issues in the USA may escalate this risk.				to consult with or advise us where a gagging order has been issued. The risk remains High due to the possible implications should the threat materialise.			
6	Section 702 of FISA is a risk given the more covert aspect of requests in this area. Current tensions between the UK/Europe and the USA give rise to concerns about the use of FISA.	3	5	15 High	A mitigation would be to encrypt our data and hold the key, however, this comes with its own risks (see risk detail). As SPA does not deliver its own IT we cannot mandate this control.	No Change	High	

	Step 6 – Assess the risk Explain the risk and score them				**Step 6: Identify Measures to Manage Risk** Identify measures you could take to reduce/eliminate Medium/High/Extremely High Risks			
#	**Describe the source of risk and nature of potential impact on individuals.**	**Probability**	**Impact**	**Overall Risk**	**Options to reduce/ eliminate risk**	**Effect on risk**	**Residual Risk**	**Approved**
		1. Rare 2. Unlikely 3. Possible 4. Likely 5. Highly Likely	1. Minimal 2. Minor 3. Moderate 4. Major 5. Severe	Low 1-4 Med: 5-9 Med High 10-14 High: 15-19 V High: 20-25		Eliminated Reduced Accepted		Yes No
7	Article 10 UK GDPR governs the processing of personal data relating to criminal convictions and offences. SPA is concerned that it cannot meet the obligations as there is no data processing agreement with MS and MS will provide access to data via FISA 702/CLOUD Act.	3	4	12 Medium High	Currently there is no method for SPA to mitigate this risk.	No Change	Medium High	

Step 7: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by: SPA IM Lead	[redacted]	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided: SPA IM Lead	[redacted] 04/2025	
Summary of DPO advice: Given the unresolved HIGH risks, the DPIA should be submitted to ICO.		
DPO advice accepted or overruled by: [redacted], SIRO		If overruled, you must explain your reasons
Comments: Advice accepted		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by: [redacted]		The DPO should also review ongoing compliance with Data Protection Law

Appendix 2

Between mid-2022 and mid-2025, Microsoft has reported at least seven major security incidents, spanning misconfigurations, cloud vulnerabilities, account compromises, and nation-state breaches.

1. Sep 2022 – "BlueBleed" Azure data leak
   A misconfigured Azure Blob Storage bucket exposed ~2.4 TB of data, affecting ~65,000 entities across 111 countries.

2. Dec 2019 (discovered late 2023) – Customer support database leak
   - Personal data of ~250 million users was exposed via misconfigurations in a support database.

3. Nov 2023 – Russian attackers (Midnight Blizzard)
   - A corporate test tenant was accessed via password-spraying; senior executive emails were compromised.

4. June–July 2023 – Chinese cyber-espionage
   - Hackers breached Microsoft Azure/Exchange systems affecting ~10,000 orgs and stealing diplomatic emails.

5. May 2024 – Storm-0558 compromised Azure AD & MSA security keys
   - Threat actors extracted private authentication keys, forging tokens and accessing emails/files.

6. Late 2024 – Office 365 document leaks
   - Misconfigured sharing settings exposed sensitive documents for finance and healthcare orgs .

7. Dec 2024 – Xbox user data compromised
   - Through social engineering, personal and payment data from thousands of gamer accounts was accessed .

Incident Frequency

- One major Azure/data misconfiguration leak per year (2022 & 2023)
- Two nation-state intrusions: Nov 2023 (Russian) and mid-2023 (Chinese)
- One key/exploit incident targeting Azure AD in May 2024
- Two consumer-facing breaches in late 2024 (Office 365 docs, Xbox)

Request 4. Communications between SPA and PSoS/Microsoft re Cloud

Email Trail

From: [redacted] <[redacted]
Sent: 09 April 2025 12:58
To: [redacted] <[redacted]@microsoft.com>; [redacted]
<[redacted]x@microsoft.com>; [redacted] <[redacted]@microsoft.com>;
[redacted] <[redacted]@microsoft.com>
Cc: [redacted] <[redacted]@scotland.police.uk>;
[redacted] <[redacted]@scotland.police.uk>
Subject: [EXTERNAL] Draft addemdum Rev PSOS [OFFICIAL]

OFFICIAL

Good afternoon all,

[redacted], thank you for the proposed amendment, I attach Police Scotland's proposed revised version.

In my last email I had also asked for clarity re the following points (some of which tie into the points in the revised addendum) and would be grateful if you could provide:

- As per previous discussion and email we would wish the amendments to the Contract to reflect that SPA is contracting also as Police Authority and contracting authority for PSOS and the Chief Constable of PSOS will require third party rights to enforce the Contract and Addendum as amended in relation to the processing of PSOS data thereunder.
- The Addendum (current form) does not make any reference to TRAs but it does commit to IDTA. Is it possible that the amendment can also reflect that for any international transfer there is a TRA in place re same?
- Regards the wording in the Addendum *Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request*. Does this mean that MSFT will hand over the encryption keys if they are satisfied that the data is not to be used for purposes other than those stated in the third-party request, or do you commit to not handing over the keys?
- For sub-processors, the terms state that Personal data processed by sub-processors is often pseudonymised, rather than always. Can you confirm re the

sub-processing activities undertaken by Akamai is the data pseudonymised/encrypted/both? With regards delivery of static assets are these still encrypted.

- Can it be confirmed whether changes made within the system does not provide sight of data within files and it relates to system changes themselves?
- Is it within the art of possible that we could rely on the EU data boundary in force after the contract was signed with regards to technical support? Could this be reflected in the amendments to the addendum?
- Is there an IDTA between SPA, PSoS and Microsoft Ireland (PSoS as third party to agreement) that goes with the Enrolment Contract ?
- Is the customer data encrypted in the UK before being transferred elsewhere or is that done in Ireland?
- Could I also request the full legal entity name of Intercom, Scuba Analytics, Akamai and Microsoft Inc. and the company numbers and addresses please.

If a call would assist matters then we would be happy to accommodate.

Thank you.

[redacted]

From: [redacted] <[redacted]@microsoft.com>
Sent: 27 May 2025 10:24
To: [redacted] <[redacted]@scotland.police.uk>
Cc: [redacted] <[redacted]@scotland.police.uk>; [redacted] <[redacted]@scotland.police.uk>; [redacted] <[redacted]@microsoft.com>; [redacted] <[redacted]@microsoft.com>; [redacted] <[redacted]@microsoft.com>
Subject: RE: Draft addemdum Rev PSOS [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.

Hi [redacted],

Thank you for bearing with us as we pulled this together. Please see my responses to your email below:

1 - As per previous discussion and email we would wish the amendments to the Contract to reflect that SPA is contracting also as Police Authority and contracting authority for PSOS and the Chief Constable of PSOS will require third party rights to enforce the Contract and Addendum as amended in relation to the processing of PSOS data thereunder.	**Please see additional wording in red below to give the Chief Constable of Police Scotland third party rights to enforce the terms of the DPA. SPA can already enforce the DPA as the contracting entity, but we have also added that the Chief Executive Officer of SPA can enforce the DPA just for completeness.** ***The Scottish Police Authority ("SPA") is responsible for maintaining policing, promoting policing principles and the continuous improvement of policing in Scotland. The SPA procures services for itself and on behalf of Police Scotland. The parties agree that, for the purposes of this DPA only, references to "Customer" shall be***

	deemed to include references to both the SPA and Police Scotland, and that, in accordance with the Data Protection Requirements, the Chief Executive Officer of the SPA and the Chief Constable of Police Scotland are each controllers of the Customer Data, Professional Service Data, and Personal Data (including all Police Data). ***In connection with the foregoing, the parties also agree that: (i) the Chief Executive Officer will act on behalf of the SPA, and the Chief Constable will act on behalf of Police Scotland in connection with the DPA and they will each be responsible for exercising the Customer's rights, and meeting the Customer's obligations and requirements, set out in the DPA; (ii) the Chief Executive Officer on behalf of the SPA and the Chief Constable on behalf of Police Scotland may rely on and enforce the terms of this DPA as they apply to the processing of Customer Data, Professional Service Data and Personal Data for which each of them is a controller (notwithstanding any exclusion of third party rights in the Customer's agreement, but subject to the terms of this DPA and the Customer's agreement); (iii) where Microsoft is required to notify or provide any information to the Customer, such obligation shall be satisfied by notifying or providing such information to either the SPA or its Chief Executive Officer, or to Police Scotland or its Chief Constable; and (iv) to the extent***

	that the SPA or Police Scotland provides instructions or directions to Microsoft in connection with the processing of Customer Data, Professional Service Data, and Personal Data, it does so on behalf of both the SPA and its Chief Executive Officer, and Police Scotland and its Chief Constable, and the Chief Executive Officer and Chief Constable hereby confirm that: (a) any such instructions or directions are approved and authorised for those purposes; and (b) Microsoft may rely on such instructions or directions as being made on behalf of the Chief Executive Officer and Chief Constable as controllers. ***Customer and Microsoft agree that Customer the Chief Executive Officer of the SPA and the Chief Constable of Police Scotland are the controllers of Personal Data and Microsoft is the processor of such data, except (a) if and when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms of the DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer.***

2 - The Addendum (current form) does not make any reference to TRAs but it does commit to IDTA. Is it possible that the amendment can also reflect that for any international transfer there is a TRA in place re same?	**Please see the additional wording in yellow.** ***All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services are subject to the terms of the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom are subject to the terms of the IDTA implemented by Microsoft. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018. Microsoft will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland, and for the avoidance of doubt Microsoft confirms that it has completed a transfer risk assessment for any transfers of Personal Data out of the United Kingdom which are governed by the IDTA. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as***

	described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

3 - Regards the wording in the Addendum - Does this mean that MSFT will hand over the encryption keys if they are satisfied that the data is not to be used for purposes other than those stated in the third-party request, or do you commit to not handing over the keys? ***Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.***	***By "third party", if we mean third party requests for data - we can confirm that "We do not provide any government with Microsoft's encryption keys or the ability to break our encryption."*** **For additional customer information about how Microsoft responds to government, law enforcement and other third-party requests, please see:** **o Microsoft Trust Center** **o Principles and Policies FAQ** **· You can also view Microsoft's Law Enforcement Request Report and U.S. National Security Order Report. Both resources are updated every six months and show that the vast majority of our customers are never impacted by government requests for data.** **Please see the DPA text (Disclosure of Processed Data section), Microsoft will not provide any third party the platform encryption keys used to secure Processed Data or the ability to break such encryption.** **Microsoft's approach: Microsoft takes strong measures to help protect Processed Data from inappropriate access or use by third parties. Microsoft will never provide a third-party with:** • **direct, indirect, blanket, or unfettered access to Processed Data;**

	• **platform encryption keys used to secure Processed Data or the ability to break such encryption; or** • **access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.** **Customer resources:** • **Microsoft Data Access Management**

4 - For sub-processors, the terms state that Personal data processed by sub-processors is often pseudonymised, rather than always. Can you confirm re the sub-processing activities undertaken by Akamai is the data pseudonymised/encrypted/both? With regards delivery of static assets are these still encrypted. **5 - Can it be confirmed whether changes made within the system does not provide sight of data within files and it relates to system changes themselves?**	**Microsoft requires all personal data in system-generated logs to be pseudonymized. Microsoft uses various techniques to pseudonymize personal data in system-generated logs, including encryption, masking, tokenization, and data blurring. Regardless of the specific method of pseudonymization, this protects user privacy by enabling authorized Microsoft personnel to do their work using logs containing only pseudonymized personal data. This enables our personnel to ensure the quality, security, and reliability of our online services without identifying or reidentifying users. For example, this enables DevOps personnel to identify the extent of a service issue across regions, including number of affected users in any given region, without these personnel being able to identify or reidentify specific individuals. For more information on the Microsoft DevOps model, see Remote access to data stored and processed in the EU Data Boundary. In the event of any unauthorized access to system-generated logs, pseudonymization helps protect user privacy. Controls on data that could enable reidentification of individuals from pseudonymized logs are the same as controls applied to Customer Data.** **Microsoft takes several steps to limit access to and usage of system-generated logs. Security controls include:** • **Data minimization via implementation of retention**

	policies set at the minimum retention time required for each type of log. • **Regular checks and scrubbing of system-generated logs to detect errors or policy non-conformance.** • **Limited usage of system-generated logs solely for purposes related to service operations.** • **Policies requiring access controls that limit the *rehydration* or *reidentification* of personal data such that it's returned to its original form.**

6 - Is it within the art of possible that we could rely on the EU data boundary in force after the contract was signed with regards to technical support? Could this be reflected in the amendments to the addendum?	**Only M365 customers with a sign-up location in a country or region in the EU or EFTA are in scope for the EU Data Boundary including technical support"**

7 - Is there an IDTA between SPA, PSoS and Microsoft Ireland (PSoS as third party to agreement) that goes with the Enrolment Contract ?	**This is the link to Microsoft's IDTA - General Data Protection Regulation and specifically here: Service Trust Portal . It applies to all customers and it is a Processor to Processor International Data Transfer Addendum to the EU SCCs - we don't have IDTAs with individual controllers / customers.**
8 - Is the customer data encrypted in the UK before being transferred elsewhere or is that done in Ireland?	**Please see this link which explains how encryption is applied: Encryption and key management overview - Microsoft Service Assurance | Microsoft Learn . Customer data is encrypted at rest in the Geo selected by the Customer, not just when it is transferred.**

9 - Could I also request the full legal entity name of Intercom, Scuba Analytics, Akamai and Microsoft Inc. and the company numbers and addresses please.	**Microsoft Limited (UK)** • **Company Number: 01624297** • **Registered Address:** **Microsoft Campus** **Thames Valley Park** **Reading, Berkshire** **RG6 1WG** **United Kingdom** **Microsoft Ireland Operations Limited (MIOL)** • **Company Number: IE256796** • **Registered Address:** **70 Sir John Rogerson's Quay** **Dublin D02 R296** **Ireland** **Intercom, Inc.** • **Full Legal Name: Intercom, Inc.** • **Registered Address: Unknown** **55 2nd Street, 4th Floor** **San Francisco, CA 94105** **United States** **Scuba Analytics, Inc.** • **Full Legal Name: Scuba Analytics, Inc. recently acquired by (Behavure AI Inc.)** • **California Entity Number: C3560978**

	• **Registered Address:** **425 Page Mill Rd.** **Suite 200** **Palo Alto, CA 94306** **Akamai Technologies, Inc.** • **Full Legal Name: Akamai Technologies, Inc.** • **Registration authority entity ID: 2933637** • **Registered Address:** **145 Broadway, Cambridge, Massachusetts, 02142**

Kind regards

[redacted]

Sent: Mon 03/03/2025 12:32

[redacted]@Microsoft.com

To [redacted]@scotland.police.uk>; [redacted]@microsoft.com>; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted]@spa.police.uk>; [redacted]@scotland.police.uk>

Subject: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [OFFICIAL]

Hi All,

Thanks for the call last week. We have copied the points from your email below in italics and added our responses in red. Happy to discuss any further questions on our call on Monday. [redacted] (CELA) and [redacted] (external counsel) can join this call too.

As we discussed, there is a heavy onus upon Police Scotland/SPA to demonstrate a granular understanding of where our data traverses, its security and that there are adequate safeguards to protect personal data in the event it is transferred / accessed outside of the UK. Section 59 of the DPA 2018 also places responsibilities on the data processor to provision evidence of IDTA or Addendum to the EU SCCs and that a Transfer Risk Assessment has been undertaken.

Microsoft response: We have provided extensive information about our data residency commitments for Microsoft 365 (Overview and Definitions - Microsoft 365 Enterprise | Microsoft Learn), the sub-processors we use (Service Trust Portal) and security measures we take to protect personal data (Security for Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn).

We also contractually commit in the Microsoft DPA to ensure that all transfers of personal data outside the UK are subject to the terms of the International Data Transfer Addendum and are subject to appropriate safeguards (for example, a TRA). Microsoft is also certified to the UK Extension to the EU-U.S. Data Privacy Framework. The IDTA can be found on the Microsoft Trust Center here: General Data Protection Regulation and specifically here: Service Trust Portal

The contractual arrangements we have in place within our group of companies and with our sub-processors, as well as any TRAs undertaken by us, are confidential and cannot be disclosed. Disclosure of those confidential agreements is not required under section 59 of the DPA 2018.

I attach a copy of the guidance Police Scotland received from ICO on the matter of Transfers by Processors and relevant safeguard due diligence. With regards to sub-processors and sub-sub processors, I understand that MSFT terms will flow down but the licensing documents and service trust portal do not provide the evidence we require to satisfy this provision as Data Controller. Evidence of the IDTA or Addendum to the EU SCCs for MSFT 365 sub-processors (who do not have adequacy) would assist Police Scotland with this.

Microsoft response: Microsoft has addressed the questions raised by the ICO in the attached letter. That letter does not require Microsoft to disclose any of its confidential contractual arrangements or compliance documents (such as TRAs). Should Police Scotland consider it necessary to carry out its own TRA regarding transfers of personal data in connection with Microsoft 365 (as per question 5 in the attached letter), we have published extensive information online in our Service Portal to help with that exercise. In case helpful, the ICO (also a competent authority under Part 3 DPA) has also published its DPIA in respect of its use of Microsoft 365, which you can find here; more recently, the ICO has also published its DPIA in respect of its use of Microsoft CoPilot 365.

[redacted] had highlighted the wording that gave some cause for concern and we advised we would send the link to you for ease of reference: Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

The extract is as follows:

Processing on a large scale [1] of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses	Office 365 is not designed to process special categories of personal data on a large scale. However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.

Microsoft response: It is clear from this extract that customers (including law enforcement customers) can use Microsoft 365 to process special category data or personal data relating to criminal convictions and offences, using the options available for customising the service and by reflecting that processing in its DPIA (should you decide that one is necessary).

DPA – we discussed that the addendum as is, is silent on UKGDPR and Law enforcement processing and that we would require amendment to this.

Microsoft response: We can provide the same amendment that we offered for Azure. See attached.

We previously sought clarity re the list of sub-processors dated 27 November 2024 and it includes the following which I assume will provide services to Police Scotland.

- Akami Technologies Inc| any MS online Service | Operating content delivery network (CDN) infrastructure to efficiently deliver content| Worldwide | HQ: USA | Customer and Personal data
- Edigo | any MS online service| CDN infrastructure to efficiently deliver content| Worldwide| HQ: USA| Customer and personal data
- Intercom, R&D, Unlimited Company| Visual Studio App Centre| | Customer chat and support| USA| HQ: Ireland| Pseudo data only
- Scuba Analytics| Teams stream SharePoint online, OneDrive for business| Customer experience analytics| USA| HQ: USA| Pseudo data only.

We asked if it was possible to provide dataflows to demonstrate the way customer data and personal data needs to be processed to deliver CDN but was advised this is commercially sensitive.

I also asked whether processing relative to CDN would include all the worldwide processing locations listed by the above sub-processors and was declined this information but understand from our call today that the position is that this cannot be further refined/narrowed down at this time.

With regards to Scuba and Intercom, I had asked for confirmation of specifically what pseudonymous data would be processed – again this was declined. It's important that as a Data Controller, Police Scotland understands 'how' and in what circumstance MSFT pseudonymise our data – for example, is it implicit that to pseudonymise it, it is accessed? '

Microsoft Response: Please see the latest record of subprocessors list: Service Trust Portal

We permit these subprocessors to process your data only to perform the work Microsoft has retained them to perform, and they are prohibited from using your data for any other purpose.
Akamai technologies is a provider with listed Headquarters in the United States and provide CDN infrastructure and Network traffic management globally.

I have provided a link to our Microsoft Learn page, which provides information on our sub processor management. Understand Microsoft Online Services subprocessor management - Training | Microsoft Learn

Personal Data processed by subprocessors is often pseudonymized, or de-identified allowing subprocessors to fulfill their job responsibilities without accessing identifiable attributes. Microsoft requires each type of subprocessor to use appropriate access controls to protect the data they process. Each type of subprocessor at Microsoft enforces appropriate access controls to protect customer and personal data. All subprocessors are required to maintain the security and confidentiality of customer and personal data and are contractually obligated to meet strict privacy and security requirements. These requirements are equivalent to or stronger than the contractual commitments Microsoft makes to its customers in the Microsoft Products and Services Data Protection Addendum.

I'd asked from the list updated 10 December 2024 whether all of the sub-processors will or will have the potential to work with Police Scotland Customer data – Appreciate that this is something that may be a future development but as it stands, my understanding is that whichever country has the requisite skillset to perform the task will have access to the customer data notwithstanding any security/controls wraparound you have in place e.g. No standing access, hierarchy of approval, time bound set of keys, managed desktops, logging and audits. As a customer, could we be provided with details of Microsoft's Security Policy? We also briefly discussed enabling Lockbox and it was highlighted that this would have the impact of slowing down fixes.

Microsoft response: We provide detailed information on service engineer access controls online (Microsoft 365 service engineer access control - Microsoft Service Assurance | Microsoft Learn), including Lockbox.

Regards

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: 26 February 2025 15:43
To: <[redacted]@microsoft.com>; [redacted]
<[redacted]@scotland.police.uk>; [redacted]
<[redacted]@microsoft.com>; [redacted]
<[redacted]@microsoft.com>; [redacted]
<[redacted]@spa.police.uk>; [redacted]
<[redacted]@scotland.police.uk>
Subject: [EXTERNAL] RE: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [OFFICIAL]

OFFICIAL

Hi [redacted]

The EU data boundary does not apply to the UK although we would both welcome and benefit from a similar boundary provision. For example, it would assist PSoS if sub-processing only occurred within those EU countries.

[redacted]

From: [redacted] <[redacted]x@microsoft.com>
Sent: 26 February 2025 14:42
To: [redacted] <[redacted]@scotland.police.uk>; [redacted]
<[redacted]@scotland.police.uk>; [redacted]
<[redacted]@microsoft.com>; [redacted]
<[redacted]@microsoft.com>; [redacted]
<[redacted]@spa.police.uk <[redacted]@scotland.police.uk>
Subject: Re: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [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.

Hi [redacted]

I have asked for an update but know that we referred some of these queries externally.

Also, I thought this recent blog would be of interest to Police Scotland: Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency - Microsoft On the Issues

From: [redacted]

Sent: Wed 26/02/2025 14:18

To [redacted]@scotland.police.uk[redacted] [redacted]@microsoft.com>; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted] [redacted]@spa.police.uk>; [redacted]@scotland.police.uk>

Subject: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [OFFICIAL]

All

I am aware that we have a meeting scheduled for Monday 3rd March, however in regard to the below request from [redacted] – do we have a response on this ahead of the meeting?

[redacted]
Digital Division
[redacted]

From: [redacted]

Sent: Wed 26/02/2025 14:18

To [redacted]@scotland.police.uk>; [redacted]@microsoft.com>; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted]@spa.police.uk>; [redacted]@scotland.police.uk>

Subject: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [OFFICIAL]

- [redacted] had highlighted the wording that gave some cause for concern and we advised we would send the link to you for ease of reference: Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

The extract is as follows:

Processing on a large scale [1] of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses	Office 365 is not designed to process special categories of personal data on a large scale. However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.

- DPA – we discussed that the addendum as is, is silent on UKGDPR and Law enforcement processing and that we would require amendment to this.

- We previously sought clarity re the list of sub-processors dated 27 November 2024 and it includes the following which I assume will provide services to Police Scotland.

- Akami Technologies Inc| any MS online Service | Operating content delivery network (CDN) infrastructure to efficiently deliver content| Worldwide | HQ: USA | Customer and Personal data
- Edigo | any MS online service| CDN infrastructure to efficiently deliver content| Worldwide| HQ: USA| Customer and personal data
- Intercom, R&D, Unlimited Company| Visual Studio App Centre| | Customer chat and support| USA| HQ: Ireland| Pseudo data only
- Scuba Analytics| Teams stream SharePoint online, OneDrive for business| Customer experience analytics| USA| HQ: USA| Pseudo data only.

We asked if it was possible to provide dataflows to demonstrate the way customer data and personal data needs to be processed to deliver CDN but was advised this is commercially sensitive.

I also asked whether processing relative to CDN would include all the worldwide processing locations listed by the above sub-processors and was declined this information but understand from our call today that the position is that this cannot be further refined/narrowed down at this time.

With regards to Scuba and Intercom, I had asked for confirmation of specifically what pseudonymous data would be processed – again this was declined. It's important that as a Data Controller, Police Scotland understands 'how' and in what circumstance MSFT pseudonymise our data – for example, is it implicit that to pseudonymise it, it is accessed? '

- I'd asked from the list updated 10 December 2024 whether all of the sub-processors will or will have the potential to work with Police Scotland Customer data – Appreciate that this is something that may be a future development but as it stands, my understanding is that whichever country has the requisite skillset to perform the task will have access to the **customer data**

notwithstanding any security/controls wraparound you have in place e.g. No standing access, hierarchy of approval, time bound set of keys, managed desktops, logging and audits. As a customer, could we be provided with details of Microsoft's Security Policy? We also briefly discussed enabling Lockbox and it was highlighted that this would have the impact of slowing down fixes.

I understand that you will consult with your own counsel and revert to us next week given the half term holiday etc.

Grateful for your consideration and input into next steps.

Kind Regards

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: 17 February 2025 16:50
To: [redacted] <[redacted]@microsoft.com>; [redacted]@microsoft.com; [redacted]@microsoft.com; [redacted] <[redacted]@spa.police.uk>; [redacted]@scotland.police.uk>
Cc: [redacted] <[redacted]@scotland.police.uk>
Subject: Police Scotland/SPA - M365 - Law Enforcement Due Diligence [OFFICIAL]

OFFICIAL

Hi, [redacted], et al,

Thank you for your time this morning.

As we discussed, there is a heavy onus upon Police Scotland/SPA to demonstrate a granular understanding of where our data traverses, its security and that there are adequate safeguards to protect personal data in the event it is transferred / accessed outside of the UK. Section 59 of the DPA 2018 also places responsibilities on the data processor to provision evidence of IDTA or Addendum to the EU SCCs and that a Transfer Risk Assessment has been undertaken.

- I attach a copy of the guidance Police Scotland received from ICO on the matter of Transfers by Processors and relevant safeguard due diligence. With regards to sub-processors, I understand that MSFT terms will flow down but the licensing documents and service trust portal do not provide the evidence we require to satisfy this provision as Data Controller. Evidence of the IDTA or Addendum to the EU SCCs for MSFT 365 sub-processors (who do not have adequacy) would assist Police Scotland with this.

- [redacted] had highlighted the wording that gave some cause for concern and we advised we would send the link to you for ease of reference: Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

The extract is as follows:

Processing on a large scale [1] of special categories of data (personal data	Office 365 is not designed to process special categories of personal data on a

revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), or of personal data relating to criminal convictions and offenses	large scale. However, a data controller could use Office 365 to process the enumerated special categories of data. Office 365 is a highly customizable service that enables the customer to track or otherwise process any type of personal data, including special categories of personal data. Any such use is relevant to a controller's determination of whether a DPIA is needed. But as the data processor, Microsoft has no control over such use and typically would have little or no insight into such use.

- DPA – we discussed that the addendum as is, is silent on UKGDPR and Law enforcement processing and that we would require amendment to this.

- We previously sought clarity re the list of sub-processors dated 27 November 2024 and it includes the following which I assume will provide services to Police Scotland.

  - Akami Technologies Inc| any MS online Service | Operating content delivery network (CDN) infrastructure to efficiently deliver content| Worldwide | HQ: USA | Customer and Personal data
  - Edigo | any MS online service| CDN infrastructure to efficiently deliver content| Worldwide| HQ: USA| Customer and personal data
  - Intercom, R&D, Unlimited Company| Visual Studio App Centre| | Customer chat and support| USA| HQ: Ireland| Pseudo data only
  - Scuba Analytics| Teams stream SharePoint online, OneDrive for business| Customer experience analytics| USA| HQ: USA| Pseudo data only.

We asked if it was possible to provide dataflows to demonstrate the way customer data and personal data needs to be processed to deliver CDN but was advised this is commercially sensitive.

I also asked whether processing relative to CDN would include all the worldwide processing locations listed by the above sub-processors and was declined this information but understand from our call today that the position is that this cannot be further refined/narrowed down at this time.

With regards to Scuba and Intercom, I had asked for confirmation of specifically what pseudonymous data would be processed – again this was declined. It's important that as a Data Controller, Police Scotland understands 'how' and in what circumstance MSFT pseudonymise our data – for example, is it implicit that to pseudonymise it, it is accessed? '

- I'd asked from the list updated 10 December 2024 whether all of the sub-processors will or will have the potential to work with Police Scotland Customer data – Appreciate that this is something that may be a future development but as it stands, my understanding is that whichever country has the requisite skillset to perform the task will have access to the customer data notwithstanding any security/controls wraparound you have in place e.g. No standing access, hierarchy of approval, time bound set of keys, managed desktops, logging and audits. As a customer, could we be provided with details of Microsoft's Security Policy? We also briefly discussed enabling Lockbox and it was highlighted that this would have the impact of slowing down fixes.

I understand that you will consult with your own counsel and revert to us next week given the half term holiday etc.

Grateful for your consideration and input into next steps.

Kind Regards

[redacted]

[redacted]

[redacted]

From: [redacted] <[redacted]@microsoft.com>
Sent: Friday, December 6, 2024 9:55 AM
To: [redacted] <[redacted]@scotland.police.uk>
Cc: [redacted] <[redacted]@microsoft.com>; [redacted] <[redacted]@scotland.police.uk>
Subject: Re: Data Protection - information request [OFFICIAL]

Hi [redacted]

Please find attached response.

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: Friday, December 6, 2024 08:49
To: [redacted] <[redacted]@microsoft.com>
Cc: [redacted] <[redacted]@microsoft.com>; [redacted] <[redacted]@scotland.police.uk>
Subject: [EXTERNAL] RE: Data Protection - information request [OFFICIAL]

Yes ah ok – I was confused with the discussion on commercials that was mentioned…Brilliant thanks [redacted]**. When do we expect the update?**

From: [redacted] <[redacted]@microsoft.com>
Sent: Friday, December 6, 2024 8:45 AM
To: [redacted] <[redacted]@scotland.police.uk>
Cc: [redacted] <[redacted]x@microsoft.com>; [redacted] <[redacted]@scotland.police.uk>
Subject: Re: Data Protection - information request [OFFICIAL]

Thanks [redacted]

Chasing it now - it was you that asked for our legal representative ([redacted]) to be included as she'd supported the ask last time around, hence awaiting a response from them. I believe she was wanting clarification on a couple of points that she now has. I think we both just want this to be sorted as soon as possible, so hopefully the update we provide will meet your requirements.

Kind Regards

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: Thursday, December 5, 2024 16:43
To: [redacted] <[redacted]@microsoft.com>
Cc: [redacted] <[redacted]@microsoft.com>; [redacted] <[redacted]@scotland.police.uk>
Subject: [EXTERNAL] RE: Data Protection - information request [OFFICIAL]

Thanks [redacted] – I am a little baffled why legal and commercials are part of this request to understand data flowing – not sure what I am missing with this, with any luck it will become clear on the response – or on Monday when we catch up.

From: [redacted] <[redacted]@microsoft.com>
Sent: Thursday, December 5, 2024 4:37 PM
To: [redacted] <[redacted]@scotland.police.uk>
Cc [redacted] <[redacted]@microsoft.com>
Subject: Re: Data Protection - information request [OFFICIAL]

Hi [redacted]

We have the responses back from legal and should have this with you by COP today.

[redacted]

From: [redacted] <[redacted]x@scotland.police.uk>
Sent: Tuesday, December 3, 2024 15:43
To [redacted] <[redacted]@microsoft.com>; [redacted]
<[redacted]@scotland.police.uk>
Subject: [EXTERNAL] RE: Data Protection - information request [OFFICIAL]

Hi [redacted], checking on in this and in particular the commercial issue and how this is impacting/delaying the delivery of this information being provided to us to ensure that we are able to move forward.

[redacted]

From: [redacted]
Sent: Monday, December 2, 2024 8:55 AM
To: [redacted] <[redacted]@microsoft.com>; [redacted]
<x[redacted]@scotland.police.uk>
Subject: RE: Data Protection - information request [OFFICIAL]

Thanks [redacted] and I hope you had a fabulous weekend, sounds excellent – are you able to confirm in regards to the commercial agreement and what's outstanding – I believe that [redacted] deals mainly with the commercials on the contract and not sure how these tie in?

From: [redacted] <[redacted]@microsoft.com>
Sent: Saturday, November 30, 2024 10:35 AM
To [redacted] <[redacted]@scotland.police.uk>; [redacted]
<[redacted]@scotland.police.uk>
Subject: Re: Data Protection - information request [OFFICIAL]

Hi [redacted]

Sorry I didn't get back yesterday - but hey, just checking in on a Saturday, so thought I'd give you a quick update.

We had a call with legal ([redacted]) and the commercial execs ([redacted] who you worked with previously). Legal are requesting additional support on a couple of the points and on the commercial side, they are providing more clarity. We're waiting on the legal responses, but I'll chase on Monday anyway and will arrange a check-in call. We are hoping that the information supplied this time will cover your requirements.

Kind Regards

[redacted]

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: Friday, November 29, 2024 16:34
To: [redacted] <[redacted]@scotland.police.uk>; [redacted] <[redacted]@microsoft.com>
Subject: [EXTERNAL] RE: Data Protection - information request [OFFICIAL]

[redacted], any update please on this engagement?

[redacted]

From: [redacted]
Sent: Tuesday, November 26, 2024 8:33 AM
To: [redacted] <[redacted]@scotland.police.uk>; [redacted] <[redacted]@microsoft.com>
Subject: RE: Data Protection - information request [OFFICIAL]

[redacted] – I am hopeful that this provides you with what you are looking for by way of what remains outstanding and would be keen to understand how we can progress this. Happy that you, [redacted] and I get on a call to discuss if that works better.?

The request for [redacted] specifically was the work that she had done on the DESC Side of things.

In regards to a previous question around

"whether the responses are required simply for your use of M365 or are now incorporating other services - such as Azure as was the case for DESC?"

Organisationally we are satisfied with the Azure piece as this was resolved in the main for DESC – I believe this is where the addendum will come into it as well. However, the M365 Exchange and SharePoint data does not sit in Azure, as such, but rather a specific product for M365 that Microsoft host separately (and has its own data residency location settings, as per my previous email). Albeit that is most likely in Azure on MS side, but it's a completely separate product, with Azure being more for hosting servers and other data. This does, however, include Sentinel data for the SIEM product that CSA use – but again, no personal or DPA relevant data is involved in that, as it's all device security logs and telemetry data for servers and security alerts.

Ultimately - the work that we have been driving towards for the past couple of years (with the input and assistance of [redacted], via the DESC along with MS legal and commercial team is to satisfy ourselves over the DPA provisions and location the data is processed in, with the aim of us moving data into the M365 (Azure) cloud environment.

[redacted]
Head of ICT Service Delivery
Digital Division

[redacted]

From: [redacted]@scotland.police.uk>
Sent: Thursday, November 21, 2024 11:13 AM
To: [redacted]@scotland.police.uk>; [redacted]
<[redacted]@microsoft.com>
Subject: RE: Data Protection - information request [OFFICIAL]

OFFICIAL

Thanks [redacted], good morning [redacted]

The elements we are unclear on and require for legislative due diligence purposes relate to the sub-processors in the main but in addition to this, we also require the addendum update.

The service trust portal provides a list of all sub-processors but Police Scotland needs to understand which of these applies to its tenant, which application they relate to and if that entails a transfer of data to third countries that do not have adequacy, we need to also understand specifically the service the sub processor provides and whether or not it is possible to use 365 without those sub-processors.

On the matter of Defender specifically, I'd like clarity regards whether this is USA based (implication being this would mean our emails would transfer to USA) and if so, is there any way to have this UK based?

I hope this is helpful.

Happy to discuss via teams or telephone if required.

Kind Regards

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: 21 November 2024 09:50
To: [redacted] <[redacted]@microsoft.com>
Cc: [redacted] <[redacted]@scotland.police.uk>
Subject: RE: Data Protection - information request

[redacted] the team feel that the answers to the questions that they posed have not been fully answered – I can get the detail if you wish however this was why the query was raised if we could discuss with [redacted] as she was key in the previous engagement and knew the detail we required.

The team reviewed the documentation set prev and the links before querying.

Happy to have a call with yourself on the details that we feel are missing, however we did raise some queries in our meeting previously when we were being pointed towards certain areas that we didn't feel this would meet the reqs.

Keen to get this bottomed out ASAP and feel that a lot of this can be managed through good conversation and understanding of what we required.

[redacted] – I have ccd you in on this – however notwithstanding the OS request to meet with [redacted].... Can you provide some additional context around the areas that are missing?

Thank you

From: [redacted] <[redacted]@microsoft.com>
Sent: Wednesday, November 20, 2024 4:36 PM
To: [redacted] <[redacted]@scotland.police.uk>
Subject: Re: Data Protection - information request

> **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.**

Hi [redacted]

I have been askes to check with Police Scotland on what is still outstanding and what you still need answers to so we can determine who is best placed to answer them

The below questions have been responded too, so what are you expecting as a follow up?

Let's you and me get on a call to chat through - when are you free over the next couple of days?

[redacted]

From: [redacted] <[redacted]@microsoft.com>
Sent: Wednesday, November 20, 2024 16:09
To: [redacted] <[redacted]@scotland.police.uk>
Subject: Re: Data Protection - information request

Hi [redacted]

I have raised with [redacted] **and she's suggested some other people I can engage with.**

Apologies about the response given not meeting the standards required - I'll make all parties aware obviously.

Bringing the points to the top, these are the ones that need addressing:

To allow us to progress on this work I have been asked to link in with yourself to progress through receipt of the below items? Is this something that you can take forward with your teams in Microsoft and look to provide to Police Scotland (via myself/[redacted]) at the soonest?

Items of note are below:

- **Documentation of the processing activities, data flows and responsibilities – can we be provided with a map of where the data traverses for each application (SharePoint and Webmail for example)?.**
- **Defender in Cloud - Confirmation whether or not is operated from the UK.**
- **Sub-processors we'd like to understand the landscape, can we have a list of these, their legal entity, their location and what they do as it pertains to each application within the 365 suite. How often do these change and how is notification made e.g. is it refreshed on a webpage that we can link to?**
- **s.75 DPA 2018 Compliance – how will the requirements be met, what assurances and evidence to support can be provided. Where sub-processor does not benefit from adequacy arrangements, provide copies of TRA, IDTA or Addendum re sub-processor/sub-sub processor chain.**
- **S61(3) & S66 how will the requirements be met – or, is it the case that the previously stated position *'that the product is not suitable for Part 3 data'* stands.**
- **Ss 61-62 of the DPA 18 How will the requirements of be met regards record keeping and logging?**
- **S59 DPA 18 - can Microsoft provide sufficient guarantees that MSFT will only engage overseas sub-processors with our authorisation and provide sufficient guarantees that it has in place "appropriate technical and organisational measures that are sufficient to secure that the processing will (a) meet the requirements of [Part 3] and (b) ensure the protection of the rights of the data subject."**
- **DP addendum - we need to have in place the supplementary agreement to the DPAdd for both Police Scotland and SPA that was negotiated for Axon via**

the DESC project as we are the direct customers for 365. I am aware that your standard addendum is not fit for Law enforcement processing – and will be aware or have experienced via the DESC piece but that was with AXON as the customer as opposed ourselves.

[redacted] **asked whether the responses are required simply for your use of M365 or are now incorporating other services - such as Azure as was the case for DESC?**

Kind Regards

[redacted]

From: [redacted] <[redacted]@scotland.police.uk>
Sent: Thursday, November 14, 2024 15:41
To: [redacted] <[redacted]@microsoft.com>
Subject: [EXTERNAL] RE: Data Protection - information request

Hi [redacted]

The team are reviewing the information but already feel its not answering the questions in the detail that we require.

They have already been through a number of the documentation pieces that are referenced and cant find the answers to the questions that they require. We have kind of been here with the DESC elements and I wonder if we could get access to [redacted] **who was instrumental in getting us the info required for the DESC work and completely turned it around.**

Ideally a 1 hour call with the same PS representation as the last time we met would be ideal.

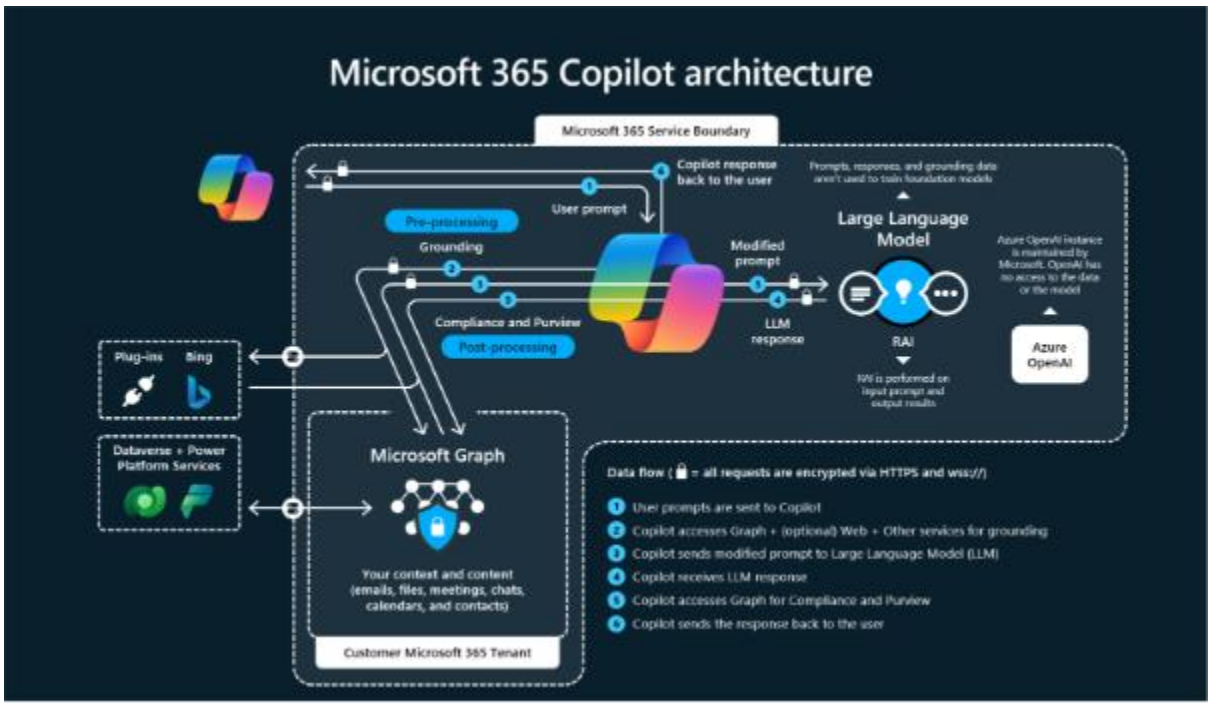
[redacted]

From: [redacted]
Sent: Wednesday, November 13, 2024 11:27 PM
To: [redacted]
Cc [redacted]
Subject: Re: Data Protection - information request

> **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.

Please see below responses:

Documentation of the processing activities, data flows and responsibilities – can we be provided with a map of where the data traverses for each application (SharePoint and Webmail for example)?.



Data Processing may take place outside of the UK

Please see relevant clause From DPA: Licensing Documents

Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services are subject to the terms of the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom are subject to the terms of the IDTA implemented by Microsoft. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European

Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018. Microsoft will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

Location of Customer data at rest

1. Source: DPA Licensing Documents]

For the Core Online Services
Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.
Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

2. Source; Product Terms Microsoft Product Terms
For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows except as otherwise provided in the Online Service-specific terms:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Brazil, Canada, the European Union, France, Germany, India, Japan, Norway, Qatar, South Africa, South Korea, Sweden, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, (4) Microsoft Teams chat messages (including private messages, channel messages, meeting messages and images used in chats), and for customers using Microsoft Stream (Classic) (on SharePoint) meeting recordings, and (5) any stored content of interactions with Microsoft 365 Copilot to the extent not included in the preceding commitments. If Customer purchases an Advanced Data Residency subscription, then Microsoft will store certain Customer Data at rest in the applicable Geo in accordance with this section and the "Advanced Data Residency Commitments" section of the product documentation at https://aka.ms/adroverview.

Defender in Cloud - Confirmation whether or not is operated from the UK.

Data is stored at rest in UK
Data is processed in line with DPA.

Microsoft Defender for Cloud Apps – privacy - Microsoft Defender for Cloud Apps | Microsoft Learn

- **Sub-processors** we'd like to understand the landscape, can we have a list of these, their legal entity, their location and what they do as it pertains to each application within the 365 suite. How often do these change and how is notification made e.g. is it refreshed on a webpage that we can link to?

  You are notified in the portal of changes and you can access updated list of subprocessors here: Service Trust Portal

  Compliance questions:

- **s.75 DPA 2018 Compliance** – how will the requirements be met, what assurances and evidence to support can be provided. Where sub-processor does not benefit from adequacy arrangements, provide copies of TRA, IDTA or Addendum re sub-processor/sub-sub processor chain.

- **S61(3) & S66** how will the requirements be met – or, is it the case that the previously stated position *'that the product is not suitable for Part 3 data'* stands.

- **Ss 61-62 of the DPA 18** How will the requirements of be met regards record keeping and logging?

  Response to all Compliance Questions:
  Please see information in DPA Licensing Documents, in Appendix A which provides the security measures that Microsoft take with the data.

  Source: We process all data in accordance with the DPA Licensing Documents. It is up to Scottish Policing to assess whether these requirements are met. Further information can be found in Service Trust Portal

  All the information regarding our use of subprocessors and transfers of data to

third countries can be found here.

- **S59 DPA 18** - can Microsoft provide sufficient guarantees that MSFT will only engage overseas sub-processors with our authorisation and provide sufficient guarantees that it has in place "appropriate technical and organisational measures that are sufficient to secure that the processing will (a) meet the requirements of [Part 3] and (b) ensure the protection of the rights of the data subject."

  [redacted]: As per the DPA – See Attachment 1- GDPR Terms Licensing Documents

  Notification: "Software as a service (SaaS) administrators (Microsoft 365, Dynamics 365) for tenants located in the European Economic Area (EEA) and the United Kingdom will receive automatic notifications of updates to this list via the Service Message Center. Infrastructure as a service (IaaS) and platform as a service (PaaS) customers (Azure) and any other users of SaaS services may sign up to receive notifications of updates to this disclosure via My Library on the Service Trust Portal"

- **DP addendum** - we need to have in place the supplementary agreement to the DPAdd for both Police Scotland and SPA that was negotiated for Axon via the DESC project as we are the direct customers for 365. I am aware that your standard addendum is not fit for Law enforcement processing – and will be aware or have experienced via the DESC piece but that was with AXON as the customer as opposed ourselves.

  OK can you please share the specific amendments that you would like to make to the DPA and we can assess the viability of these.

Apologies for the delay in this response.

Please reply all with any further input/information requested.

[redacted]

From: [redacted]
Sent: Tuesday, November 12, 2024 08:38
To: [redacted]
Cc: [redacted]
Subject: [EXTERNAL] RE: Data Protection - information request

[redacted]

Still nothing received – can you confirm that this is being worked on please?

Also, please see attached that may be useful.

Thank you

From: [redacted]
Sent: Thursday, November 7, 2024 3:12 PM
To: [redacted]
Cc: [redacted]
Subject: Re: Data Protection - information request

> **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.

Hi [redacted]

We're aiming to get this back to you by close of play tomorrow - just back today after being out of the office this week.

Kind Regards

[redacted]

From: [redacted]
Sent: Thursday, November 7, 2024 13:40
To: [redacted]
Cc: [redacted]
Subject: [EXTERNAL] RE: Data Protection - information request

Hi [redacted] and [redacted]

I am wondering if there is any movement on providing responses to the queries raised and discussed last week.

Thank you

[redacted]

From: [redacted]
Sent: Wednesday, October 23, 2024 3:40 PM
To: [redacted]
Cc: [redacted]
Subject: Re: Data Protection - information request

Hi [redacted]

Here's some availability for a call:

28th 930, 1pm

29th 2pm

30th 2pm

Are any of these any good for you?

I'm also chasing for an update.

[redacted]

From: [redacted]
Sent: Wednesday, October 23, 2024 13:04
To: [redacted]
Cc [redacted]

Subject: [EXTERNAL] RE: Data Protection - information request

Hi both, I am wondering if there has been any update on provision of this info?

In the meantime would it be possible to set up a call to start to discuss this?

[redacted]

Police Scotland / Poileas Alba

2 French Street

Dalmarnock

G40 4EH

From: [redacted]
Sent: Friday, October 11, 2024 7:25 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Data Protection - information request

Thanks [redacted]

[redacted]

Police Scotland / Poileas Alba

2 French Street

Dalmarnock

G40 4EH

[redacted]

[redacted]

From: [redacted]
Sent: Friday, October 11, 2024 5:41 PM
To: [redacted]
Cc: [redacted]
Subject: Re: Data Protection - information request

> **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.

Hi [redacted]

Yes, I forwarded this internally.

[redacted] can you please provide [redacted] with an update?

Thanks

[redacted]

From: [redacted]

Sent: Friday, October 11, 2024 16:59
To: [redacted]
Cc: [redacted]
Subject: [EXTERNAL] RE: Data Protection - information request

Hi [redacted]

I hope you are well.

I just wanted to check in and make sure you received this ok and that this is being progressed.

[redacted]

[redacted]

Police Scotland / Poileas Alba

2 French Street

Dalmarnock

G40 4EH

[redacted]

[redacted]

From: [redacted]
Sent: Monday, October 7, 2024 9:25 AM
To [redacted]
Cc: [redacted]

Subject: Data Protection - information request

Hi [redacted] I hope you are well!

At our MS account catch up and I am sure in subsequent discussions with [redacted], you have been made aware of the ongoing discussions and development of agreement on utilising MS Cloud within Police Scotland and the work that we are doing with our information Assurance and Security team to allow us to move forward in this space.

To allow us to progress on this work I have been asked to link in with yourself to progress through receipt of the below items. Is this something that you can take forward with your teams in Microsoft and look to provide to Police Scotland (via myself/[redacted]) at the soonest?

Items of note are below:

- **Documentation of the processing activities, data flows and responsibilities** – can we be provided with a map of where the data traverses for each application (SharePoint and Webmail for example)?.
- **Defender in Cloud** - Confirmation whether or not is operated from the UK.
- **Sub-processors** we'd like to understand the landscape, can we have a list of these, their legal entity, their location and what they do as it pertains to each application within the 365 suite. How often do these change and how is notification made e.g. is it refreshed on a webpage that we can link to?
- **s.75 DPA 2018 Compliance** – how will the requirements be met, what assurances and evidence to support can be provided. Where sub-processor does not benefit from adequacy arrangements, provide copies of TRA, IDTA or Addendum re sub-processor/sub-sub processor chain.
- **S61(3) & S66** how will the requirements be met – or, is it the case that the previously stated position *'that the product is not suitable for Part 3 data'* stands.
- **Ss 61-62 of the DPA 18** How will the requirements of be met regards record keeping and logging?
- **S59 DPA 18** - can Microsoft provide sufficient guarantees that MSFT will only engage overseas sub-processors with our authorisation and provide sufficient guarantees that it has in place "appropriate technical and organisational

measures that are sufficient to secure that the processing will (a) meet the requirements of [Part 3] and (b) ensure the protection of the rights of the data subject."

- **DP addendum** - we need to have in place the supplementary agreement to the DPAdd for both Police Scotland and SPA that was negotiated for Axon via the DESC project as we are the direct customers for 365. I am aware that your standard addendum is not fit for Law enforcement processing – and will be aware or have experienced via the DESC piece but that was with AXON as the customer as opposed ourselves.

Thanks in advance [redacted]

[redacted]

Police Scotland / Poileas Alba

2 French Street

Dalmarnock

G40 4EH