



Iascach Intíre Éireann
Inland Fisheries Ireland

Inland Fisheries Ireland

Data Protection Impact Assessment (DPIA)

Body Worn Cameras (BWCs)

May 2024

Version Control					
Version No.	Status	Authors(s)	Reviewed by	Approved by	Date of issue
V0.1	Draft	River Basin Director/ DPO	Privacy Engine		
V0.2	Draft	River Basin Director	DPIO		
V0.3	Draft	River Basin Director	Pembroke Privacy		
V0.4	Draft	River Basin Director	DPIO		
V1	Final	River Basin Director	DPIO	<i>barry fox</i>	10/05/2024 IST

Signer ID: NP0VTOYYEE...

Contents

.....	2
Guidance Notes	4
Why and when does a project or data processing activity need to complete a Data Protection Impact Assessment (DPIA)?	4
Who in the IFI should complete the DPIA?	5
Pre-screening test: Identify the need for a DPIA	6
Specification of the project/data processing activity	8
Section 1 Project/data processing activity - Description	9
Section 2: Analysis of Personal Data to Be Used	14
Section 3: Analysis of Project/Data Processing Activity/Technology's Application of Data Protection Principles	19
Section 4: Risk Assessments & Risk Remediation Solutions	33
Section 5: Documentation of DPIA Outcomes & Decisions.....	42
App. 1 - Guidance for completing a Risk Register	43
App. 2 – Conflict Management QQI Level 6 – Programme modules	45
App. 3 - Cloud Security Questionnaire_FINAL.pdf	46

Guidance Notes

Why and when does a project or data processing activity need to complete a Data Protection Impact Assessment (DPIA)?

A DPIA has three major functions:

- 1) It helps to identify any potential high risks to data subjects' rights when planning new or revising existing processes or functionality, and to design actions to mitigate these risks.
- 2) It is a useful tool to help organisations to demonstrate their compliance with data protection law.
- 3) DPIAs help with implementing Privacy by Design (PbD), as mandated by the GDPR & LED (as implemented by Part 5 of the Data Protection Act 2018) ['Data protection by design and by default' \[Art 25 of the GDPR - & section 76 of the 2018 Act\]](#)

The Data Protection Officer must be consulted when carrying out a DPIA [GDPR – Art 25].

A DPIA is required in cases described in Art 35 of the [GDPR - and section 84 of the 2018 Act](#); in the and in the [list provided by the Irish Data Protection Commission](#). Examples include instances when:

- data processing is likely to result in a high risk of harm to the individuals whose personal data are processed (e.g. when new technology or health data are used, or when a new service provider is being engaged to process the data)
- large volumes of data are being processed, or data sets are merged so that the overall amount of information on individual data subjects available becomes much richer
- New functionality or technology is being introduced with which the organisation is not familiar
- Personal data is going to be used for a new or different purpose, which might not have been envisaged when the data was originally gathered.

A DPIA should be carried out as early as possible in the development life cycle – preferably at the 'design' stage. To confirm whether a DPIA is required, the project team should complete the pre-screening test below.

Where it indicates that a DPIA is required, the DPIA should be completed before any processing of personal data is undertaken (as per the GDPR & 2018 Act) and before any key decisions are made that will be difficult or costly to revisit or amend. The project team should also allow time for any risks to be identified and mitigated or resolved.

If the project requires a funding proposal, it is advisable to undertake the pre-screening before submission of the proposal. Once funding is granted, to conduct the DPIA as soon as possible thereafter.

Additionally, it is necessary for projects and process owners to understand potential costs arising from data protection compliance (e.g. developing technical measures or organisational safeguards and data protection training), in case relevant costs have to be factored into the costing and the project/operations budget.

The project manager or process owner will also need to allow time in the project plan to develop and implement any mitigation actions arising from the risks identified. In summary, it is essential that a DPIA and resulting actions happen before any actual processing of personal data takes place. Should high risks be identified that cannot be mitigated against, it may be necessary for the IFI as Data Controller to consult with the Data Protection Commission prior to proceeding.

Failing to carry out a DPIA correctly or failing to consult the competent Supervisory Authority, where required, will be considered substantial non-compliance.

Who in the IFI should complete the DPIA?

The IFI, as a Data Controller, is responsible for ensuring that the DPIA is carried out and remains ultimately accountable for compliance with the GDPR & Part 5 of the 2018 Act- whichever is the applicable legal regime.

- As appropriate, the IFI project manager / process owner should own and complete the DPIA, and then submit the completed Assessment questionnaire to the IFI's Data Protection Officer for review
- Relevant internal and external stakeholders should be consulted throughout the DPIA assessment process to assist in identifying any project-related risks to a Data Subject's privacy and data protection rights, as well as their overall rights and freedoms provided in law
- The DPO remains available to be contacted throughout this process and to assist and support the DPIA completion where required
- Having reviewed the completed DPIA questionnaire, the DPO will respond to the project manager / process owner with an evaluation of the risk assessment as well as recommendations on how to proceed.

Pre-screening test: Identify the need for a DPIA

To ascertain whether your project/data processing change requires a DPIA to be completed, please consider the questions below and tick all where the answer is YES.

If you answer NO to all the screening questions, it is unlikely that you will need to carry out a DPIA. You should retain a copy of this completed sheet along with your justification for any your answers.

If you answer YES to one or more of the screening questions, you should proceed through the DPIA stages and complete the impact assessment. When completed, a copy of your finished screening questions, answers and notes should be retained along with the recorded DPIA documents.

Tick the box where the answer is 'Yes':

<input checked="" type="checkbox"/>	Will the project or its deliverables involve the collection of new information about individuals?
<input checked="" type="checkbox"/>	Will the project compel individuals to provide additional personal information about themselves?
<input checked="" type="checkbox"/>	Will information about individuals be disclosed to organisations or people who have not previously had routine access to this information?
<input checked="" type="checkbox"/>	Are you using information about individuals for a purpose for which it is not currently used, or in a way it is not currently used?
<input checked="" type="checkbox"/>	Does the project involve introducing new technology which might be perceived as being privacy intrusive? <i>(for example, the use of tracking or facial recognition technology, or requiring individuals to disclose information about themselves)</i>
<input checked="" type="checkbox"/>	Will the project result in making decisions or taking action against individuals in ways which can have a significant impact on them? <i>(for example, profiling of employee performance or client health information to indicate patterns)</i>
<input checked="" type="checkbox"/>	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? <i>(for example, health records, trade union membership or other information that people would consider to be particularly private)</i>
<input type="checkbox"/>	Will the project enable to contact individuals in new ways which they may find intrusive?
<input checked="" type="checkbox"/>	Will the project introduce new facilities or functionality that might be used to gather, process, analyse or share personal information in ways that would not previously have been possible?
<input checked="" type="checkbox"/>	Will the project involve the processing of personal data by third party service providers which was previously done in-house?
<input checked="" type="checkbox"/>	Will the project expose personal data to a higher level of security risk? <i>(for example, will the data be processed in another jurisdiction, or on a new or unfamiliar system or platform)</i>

<input checked="" type="checkbox"/>	Are stakeholders likely to have privacy concerns about the changes which the project is introducing?
-------------------------------------	--

[These screening questions are derived from <https://www.ucisa.ac.uk/groups/exec/pia> and based on <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>]

DPIA ID:	BWC May 2024	
Reviewed:	May 2024	
DPIA owner:	Sean Long	
Project:	new <input checked="" type="checkbox"/>	modified <input type="checkbox"/>

Overall risk identified:	
<input checked="" type="checkbox"/>	Low
<input type="checkbox"/>	Medium
<input type="checkbox"/>	High
<input type="checkbox"/>	Needs DPC approval

Specification of the project/data processing activity

Guidelines for projects which require a DPIA

Where the above pre-screening exercise indicates one or several 'Yes' responses, the DPIA must be completed.

The project manager or process owner should complete all questions on the DPIA questionnaire and forward the completed DPIA to the IFI Data Protection Officer (DPO). Having reviewed the completed questionnaire, the DPO will provide feedback on any risks arising from their processing of personal data as identified by the project/data processing activity.

Where appropriate, the DPO will also provide the project team with recommendations on how to mitigate or eliminate these risks. However, **it remains the responsibility of the project manager / process owner to ensure that the required controls are put in place and to sign off on any risks arising from the project [see Sections 4 & 5 of this document].**

It is also the project manager's / process owner's responsibility to take the recommendations of the DPO on board. If the project team does not follow the DPO's recommendations, it needs to have strong justification for not doing so. Such decisions should be documented and retained as part of the project library.

A Data Protection Impact Assessment is a 'living document' and should be revisited from time to time during the project in order to reflect any changes to the project objectives and deliverables which might have a material impact on the risks identified. Such changes in scope or objective may also introduce new risks which had not previously been considered.

Any risks identified by a DPIA must be managed throughout the project life cycle, and any risk mitigation measures must be followed through to completion. It is also the responsibility of the project team to apply the principles of 'privacy by design and default' to the design and implementation of the proposed solution.

The DPIA is a key mechanism by which the project team can demonstrate that this obligation has been understood and met.

Section 1 Project/data processing activity - Description

1.1 High-level outline of the project proposal: What do you plan to do?

Describe the background to the project and how has it come about. Please provide a high-level, 'plain English' summary of the project objective(s).

Inland Fisheries Ireland (IFI) are planning to provide body worn cameras (BWC) to field-based employees. This is to primarily ensure the safety of staff in the field when undertaking their enforcement duties in areas that are deemed high risk, where previous assaults have occurred.

1.2 Purpose of project: What is the project / processing change intended to achieve?

Who will benefit and how will it affect those whose personal data will be processed?

Purpose of deployment

IFI has identified two purposes for the deployment of BWCs to field operations staff.

Body Worn Cameras will be used by IFI Fisheries Officers primarily to de-escalate potentially hostile or 'hot' situations while secondarily preventing offences under fisheries legislation taking place in the field where IFI authorised officers are carrying out their duties. These offences cover two areas: fisheries offences under fisheries legislation and offences of assaulting, obstructing or impeding an authorised officer. These offences are set out in the [Fisheries Consolidation Act 1959, Local Government and Water Pollution Acts 1977 & 1990](#) and the [Sea Fisheries and Maritime Jurisdiction Act 2006](#).

Necessity Test

IFI is the state agency responsible for the protection, management and conservation of Ireland's inland fisheries and sea angling resources.

IFI is a 'competent authority' as defined by the LED as it is a public authority competent for the prevention, investigation, detection and/or prosecution of criminal offences as set out in [section 69\(1\) of the Data Protection Act 2018](#).

Under [section 71\(2\) of the Data Protection Act 2018](#), the processing of personal data shall be lawful where, and to the extent that the processing is necessary for the performance of a function of a controller for a purpose specified [in section 70\(1\)\(a\)](#)- that is for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

As a primary element of the requirement of lawfulness under data protection legislation, processing must, as a first step be necessary for the stated purpose.

Every year there is a significant number of serious incidents in which fisheries personnel have been assaulted and injured, some seriously so. These assaults on IFI personnel are generally instigated by persons illegally fishing or by persons attempting to stop Fisheries Officers from carrying out their statutory duties. IFI is under a statutory duty to enforce fisheries legislation and to play a role in the prevention, investigation, detection of fishing offences under that legislation as well as to prevent, investigate, detect the commission of offences specifically relating to the assaulting, obstructing, impeding of fisheries officers carrying out their statutory duties.

IFI intends to deploy BWCs to protect and reduce the incidences of assault, aggressive behaviour, and intimidation against fisheries officers and also to prevent, investigate, detect, prosecute fisheries offences under fisheries legislation.

Protection officers spent c146,000 hours on patrol duties in 2022 during which they inspected 34,650 anglers and commercial fishers for licence, permit and compliance with fisheries legislation. Officers initiated 107 prosecutions for fisheries offences, including assault, obstruction and impeding them in the exercise of their statutory duties. 52 incidents of hostile or aggressive behaviour were reported in 2022; many such incidents go unreported by officers.

Year	Protection Hours	Patrol	Incidents Reported	Average
2019	157,980		64	0.0405
2020	142,000		61	0.0429
2021	162,654		72	0.0442
2022	146,021		52	0.0356
2023	144,337		51	0.0353

Factual description of measures: the recording of video and audio footage by body worn cameras by IFI officers in the field (in- very limited and defined circumstances- **only when there is a reasonable belief that an offence under fisheries legislation has taken place or is about to be committed i.e fishing**

offences under fisheries legislation or the officer has a reasonable belief that they will be assaulted, obstructed or impeded in carrying out their statutory duties).

Fundamental rights and freedoms limited by the data processing: data subjects' fundamental rights to privacy and data protection will be impacted by the processing described above.

Objectives of the measure: The objective of the measure is to detect, investigate, prevent, prosecute offences under fisheries legislation- being fisheries offences and offences of assaulting, impeding or obstructing officers when carrying out their statutory duties under fisheries legislation. The overall objective of the measure is to ensure that IFI fulfils its statutory duty to ensure that illegal fishing does not take place and to protect, develop and manage Ireland's rivers and streams and prevent and detect activities that threaten same and are in breach of fisheries legislation. As well as general objectives of preventing fisheries offences and protecting Ireland's rivers and streams, the protection of the rights of the officers in carrying out their duties is a specific objective of the measure e.g to protect their person, safety while carrying out their duties by preventing and ideally deterring the commission of offences of assaulting, obstructing and impeding them in the carrying out of their duties.

Effective and least intrusive means to achieve objective: IFI have put significant effort and planning into utilising the least intrusive means to achieve its objectives and has **provided** staff with specific training relating to the use of body worn cameras in order to ensure the most effective and least intrusive use of same. The principal means by which this has been achieved is the policy by which the cameras are by default in non-record mode and that staff are specifically trained on dealing with a conflict situation and how to recognise a threat escalation and to assess and determine whether they have a reasonable belief that an offence under fisheries legislation has occurred or is about to be committed- after which assessment the cameras will begin to record if a threat is suspected. In order to achieve the objective of preventing, detecting, investigating, prosecuting such offences it is necessary to record the events happening in order to either a) prevent the incident from occurring or b) in order to investigate, detect, prosecute an actual offence under fisheries legislation once it has occurred. It is necessary to record evidence in order to successfully investigate, detect and prosecute such a case through the Irish Courts. It would not be possible to carry out the statutory functions of IFI without having recorded such evidence and successfully investigate, prosecute the offences under fisheries legislation set out above.

Proportionality Test

There is a strong public policy objective in protecting Ireland's rivers and streams from offences taking place under fisheries legislation so that such natural amenities are preserved for the public to enjoy now and into the future. The measure in question (use of body worn cameras by IFI officers) meets this objective and especially in light of the safeguards deployed in the use of such cameras, does not go beyond what is necessary to meet this objective.

The scope, extent and intensity of the processing, for the reasons set out below is low as there are a very limited number of data subjects captured by the cameras, which are only switched to record mode, when trained IFI staff form a reasonable belief that an offence under fisheries legislation has occurred or is going to be committed. Therefore, on a fair balance assessment, the measure (deployment and use of body worn cameras by trained IFI staff in very limited circumstances) is considered proportionate to the aim sought to be achieved- i.e the statutory duty of protection and conservation of Ireland's rivers and streams.

IFI anticipates that data capture will be the exception rather than the norm and has developed a threat test that must be met prior to the activation of the camera. In addressing this threat to the officer, the following must be assessed:

1. Proximity (The proximity of the threat);
2. Ability (The ability of the threatening person to carry out the threat);
3. Intent (The intent of the person to carry out the threat).

The use of these cameras will benefit IFI staff in the field in the event that they are involved in any incidents while working and reduce the incidences of threatening or aggressive behaviour or assaults on staff. It is hoped that offences under fisheries legislation would be deterred, prevented without the need to switch the cameras into 'record' mode.

1.3 What is the purpose of collecting the personal information within the project?

For example: client treatment, client administration, clinical research, clinical audit, business reporting, staff administration, etc.

The primary use of the BWC is as a deterrent. Any evidential data captured through use of the body worn cameras will be used as evidence in assault charges brought by either An Garda Síochána on behalf of Fisheries Officers or by IFI in cases of breaches of fisheries legislation, including assault of

an officer. **The secondary use of the BWC** is to collect video evidence in relation to breaches of fisheries legislation for which IFI is the law enforcement agency.

1.4 What are the potential privacy implications of this project?

Provide a brief summary.

IFI has identified the following privacy implications related to the processing of data through the body worn cameras:

Footage accessed by non-authorized persons on body cameras which have been lost/stolen during the course of protection duties. – not accessible outside DEMS(Digital Evidence Management Software)	May be admissible in a prosecution case to a judge	Other individuals seeking viewing of footage	Incidental recording of 3 rd party phone calls	Non-compliance with GDPR/ Data Protection Act 2018
Inappropriate footage being taken and retained	Risk of external hacking	Non-minimisation	Non-awareness	
Subject incapable of understanding the caution due to language barrier, intellectual disability or minor	Sharing through discovery for 'defence'	Inadvertent recording of juveniles/children/vulnerable persons	No supporting evidence	

1.5 What stakeholders are involved in this project?

Please list stakeholders (and stakeholder groups), including internal and external organisations (public/private/third-party) and groups that may be affected by the outcome of this project. Briefly outline the role they will have once the project is delivered.

Internally

- IFI Staff – implementing body worn cameras.
- Body Worn Camera Working Group

- Senior Management Team

Externally

- Butler Security Ltd – supplying the body worn cameras.
- Axon – providing the body worn camera training and the digital evidence management system (DEMS)
- PrivacyEngine – reviewed DPIA work completed to date (January 2022) and recommending actions to take to ensure compliance with GDPR and data protection laws.
- Pembroke Privacy – reviewing work completed to November 2023 with focus on LED/ part5 of the Data Protection Act 2018

1.6 Controllers and Processors: Identify below the status of the organisations involved in this processing activity.

- *Data Controllers are those decide how the personal data collected will be used.*
- *Joint Controllers collaborate with the Data Controller in order to process the data or deliver a service.*
- *Processors are organisations or individuals who process personal data on behalf of, and underwritten instruction from the Data Controller*
- *Sub-contractors support the Data Processor in the delivery of the processing activity.*

Institution / Organisation	Data Controller	Data Processor	Joint Controller	Sub-Contractor	Formal contract in place? (Y/N)
IFI	Y				N/A

Section 2: Analysis of Personal Data to Be Used

1. Describe the envisaged data processing activities and the lawful basis which will justify the intended processing of personal data.

(If a data flow map of the proposed processing is available, it should be included with your DPIA submission.)

Lawful Basis: The GDPR and the LED/Part 5 of the 2018 Act provide a set of Lawful Processing Conditions which legitimise the processing of personal data – at least one of these Conditions must apply for each processing activity listed below.

The Regulation differentiates between the list of Conditions to justify the processing of personal data (name, address, e-mail, mobile number, etc.) (derived from GDPR Article 6) and a separate set of Conditions to justify the processing of 'special category' data such as an individual's religious or political affiliation, ethnic identity, medical condition or trade union membership (derived from GDPR Article 9).

Proposed processing activity	Type of personal data processed	Lawful Basis for processing
Capturing video footage on body worn cameras	Individual's identity, image and audio	Processing necessary for purposes of prevention, investigation, detection, prosecution of offences under fisheries legislation.

What Personal Data are involved?
 What data is being collected, shared or used? (If you have a documentation to explain, please refer/link to that, or add as appendix to DPIA)

Data Type – Information that identifies/relates to the individual	Tick as appropriate	Purpose of Processing	Source of this data item (Clients, Employees, Public, etc.)	Is the data necessary for the intended processing activity?	
				Yes	No
2.1 Name	<input checked="" type="checkbox"/>	Captured on the body worn cameras to identify individuals for the purpose of preventing, investigating, detecting, prosecuting for assault,	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>

			impediment, obstruction and/or breaches of fisheries legislation			
	Postal Address	<input checked="" type="checkbox"/>	Potential as part of recording a fisheries/ water pollution offence including assault/obstruction/impediment of an officer	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Postcode / Eircode	<input checked="" type="checkbox"/>	Potential as part of recording a fisheries/ water pollution offence including assault/obstruction/impediment of an officer	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Date of Birth	<input checked="" type="checkbox"/>	Possible when determining the adult or minor status of an individual	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Age	<input checked="" type="checkbox"/>	Captured on the body worn cameras to identify age of individuals who may be minors - assault prosecution and or fisheries prosecution	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>	Captured on the body worn cameras to identify individuals - assault prosecution and or fisheries prosecution	Body worn camera footage captured by warranted authorised persons	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Sexual Orientation	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
	Nationality	<input checked="" type="checkbox"/>	Potential as part of recording a fisheries/ water pollution offence	Body worn camera footage captured by	<input type="checkbox"/>	<input checked="" type="checkbox"/>

			including assault/obstruction/impediment of an officer	warranted authorised persons		
	Tel no.	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
	Physical description	<input checked="" type="checkbox"/>	Captured on the body worn cameras to identify individuals	Body worn camera footage captured by warranted authorised persons.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Personal Identification no.(s)	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
	Mobile/home phone no.	<input checked="" type="checkbox"/>	Potential as part of recording a fisheries/ water pollution offence including assault/obstruction/impediment of an officer	Body worn camera footage captured by warranted authorised persons.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email address	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
2.2	Information on an individual's health (mental or physical); genetic information (biological samples such as chromosomal or DNA samples); biometric information (such as fingerprints or facial recognition)	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
2.3	Information on individual's family circumstances, lifestyle,	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>

	social media activity, demographic profile, etc.					
2.4	Information relating to criminal offences; alleged offences; or criminal proceedings	<input checked="" type="checkbox"/>	Captured on the body worn cameras to identify individuals- assault prosecution and or fisheries prosecution	Body worn camera footage captured by warranted authorised persons	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.5	Information on individual's education, qualifications or professional training	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
2.6	Individual's employment and / or career history	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
2.7	Information relating to the financial affairs of the individual	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
2.8	Information relating to individual's religious, political or other beliefs; or trade union membership	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
<p>Will the individuals be identifiable during processing?</p> <p>Select the appropriate choice. Please note that where possible information should be anonymised or pseudonymised in order to protect the privacy and confidentiality of the individual. However, this may not always be possible or practical. In such circumstances, please explain why the personal data cannot be anonymised or pseudonymised. If the data will be pseudonymised or anonymised, please specify at what point after collection this will happen</p>						
2.9	Identifiability of Data	If information will be pseudonymised or anonymised, indicate by whom and give a description of the type / technique used to do so:				
	Anonymised <input type="checkbox"/>					
	Pseudonymised <input type="checkbox"/>					

	Identifiable <input checked="" type="checkbox"/>	The data uploaded to DEMS will be identifiable as the body worn cameras capture video and audio footage of the individuals which is necessary to investigate, detect, prosecute offences (committed by identified individuals) under fisheries legislation.
--	--	---

Section 3: Analysis of Project/Data Processing Activity/Technology's Application of Data Protection Principles

Is the processing of personal data in your project/data processing activity / technology fair and lawful?

3.1	<p>What is the legal basis for processing the personal information?</p> <p>This is your valid legal reason (or reasons) for processing. These reasons are laid out in Article 6 & 9 of the GDPR & section 71 of the 2018 Act. Please ensure that the collection of each personal data type specified in Section 2 of this document (2.1 to 2.8) has one or more legal basis. Consider that different processing activities might draw on different legal basis, e.g. some processing operations will be based on people's consent, some might be based on legal or statutory obligations.</p>
	<p>The legal basis for processing personal data is section 71(2)(a) of the Data Protection Act 2018, whereby processing of personal data is lawful only if and to the extent that processing is necessary for the performance of a function of a controller for the purpose of the prevention, investigation, detection, or prosecution of criminal offences.</p> <p>The function (or task) of IFI can be found in the following fisheries legislation:</p> <p>The powers of a Fisheries Officer are derived from the following legislation:</p> <ol style="list-style-type: none"> 1. Fisheries Acts 1959 to 2017; 2. Local Government and Water Pollution Acts 1977 & 1990; 3. Sea Fisheries and Maritime Jurisdiction Act 2006. <p>Fisheries Officers are authorised to enforce this legislation through four separate warrants:</p> <ol style="list-style-type: none"> 1. Authorised Person (for the purposes of Part XVIII of the Fisheries Acts 1959-2017);

	<ol style="list-style-type: none"> 2. Authorised Officer / Inspector (for the purposes of Part XVIII of the Fisheries Acts 1959 – 2017); 3. Authorised Person (for the purposes of the Local Government and Water Pollution Act 1977 & 1990); 4. Authorised Person (Bass Warrant) (for the purposes of Section 51 of the Sea Fisheries and Maritime Jurisdiction Act 2006) <p>The production of the relevant warrant is sufficient for an Officer to exercise their powers as a Fisheries Officer.</p> <p>The processing of personal data collected via body worn cameras is necessary for IFI to perform its statutory duties under the above legislation.</p> <p>IFI is a 'competent authority' as it is a public authority competent for the prevention, investigation, detection and/or prosecution of criminal offences.</p>
3.2	<p>Have you complied with any other laws that apply to your processing, in addition to Data Protection Act 2018? Does your project/data processing activity fall under any other laws or regulations that apply, including domestic laws in other countries/Member States? Please specify below which other regulations and/or laws apply and how you comply with it.</p>
	<p>Due to the nature of the work conducted by IFI, compliance with and enforcing of the various Fisheries Acts (Fisheries Consolidation Act, 1959 and additional legislation to 2017), Local Government and Water Pollution Acts 1977 & 1990 and the Sea Fisheries and Maritime Jurisdiction Act 2006 are applicable to the processing of data using the body worn cameras. Also Part 5 of Data Protection Act 2018 in relation to the processing of data for the prosecution of offences/LED Article 8.1</p>
3.3	<p>Is your processing of an individual's personal information likely to interfere with their 'right to privacy' or with other rights under Article 8 of the 'European Convention on Human Rights' see > More</p>
	<p>There is an interference with 'right to respect for private life' under Article 8 of European Convention of Human Rights and the right to data protection under Article 8 of the EU Charter of Fundamental Rights..</p>
3.4	<p>Do you have Privacy Notices/Statements in place? It is important that clients affected by your project/data processing activity/technology are informed as to what is happening with their personal information.</p> <p>If this DPIA is for an existing project/data processing activity, is the Privacy Notice/Statements you provided to people previously still reflective of the current way data are processed or is revised communication needed? If yes, how do you intend to do this?</p>

	<p>Transparency and accountability are required to ensure that data subjects are made aware of how their personal data will be processed.</p> <p>As IFI staff will be capturing video and audio footage of individuals, it is important to ensure that a verbal Privacy Statement is provided prior to capturing any video footage and adequate warning signage is displayed on the BWC. Please refer to the BWC SOP for verbal Privacy Statement and visuals of warning signage pages 6 to 9.</p> <p>There will also be reference made to the full IFI Privacy Policy (which will be available on IFIs corporate website) where this can be located and who to contact if they have further questions or queries in relation to the processing. This is necessary for the purpose of public transparency and to give adequate notice. Officers wearing a BWC must carry a BWC information card on their person while on patrol and the badge displayed in the SOP (page 7) which informs the public that they are wearing a BWC. Please see SOP for images and Privacy Statement pages 6 to 9.</p>
3.5	<p>If you are relying on consent or explicit consent to process personal data, how will each type of consent be obtained and recorded (describe below), what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?</p> <ul style="list-style-type: none"> ▪ If you are processing data relating to children, please specify arrangements to ensure valid consent is obtained. ▪ If you are processing data relating to vulnerable individuals or individuals with limited capacity to consent, please specify how this will be carried out. <p>Please attach supporting documentation. Please summarise any particular risks in the table in Section 4 of this document, which looks at risks and risk mitigating measures.</p>
	N/A

Are you considering the purpose of your processing and purpose limitation?	
3.6	<p>Does your project/data processing activity/technology involve the use of existing personal data for new purposes? Is the new purpose aligned with the original purpose of collection? If yes, please describe below.</p>
	<p>The introduction of BWC does not involve the use of existing personal data. The processing activity is novel to IFI.</p>

3.7	Are potential new purposes likely to be identified as the scope of the project expands, e.g. 'scope creep'? If yes, please describe below. If the project is for scientific or historical or statistical purposes, can you envisage derogations becoming applicable? If yes, describe below.
	There are only two purposes outlined – protecting IFI staff from assault or aggressive behaviour and capturing evidence for possible prosecution for breaches of fisheries legislation- both purposes coming under the overall purpose of the prevention, investigation, detection or prosecution of offences under fisheries legislation. The dedicated BWC SOP and staff training ensures that no additional purposes for processing data using the body worn cameras are permitted.

What about the adequacy, quality and accuracy of the personal data processing in your project/data processing activity/technology?	
3.8	Data Quality: If you collect information from data subjects directly, do you have protocols and processes in place to assure data collection is consistent across the data set? If yes, please give short description. If you receive information indirectly, do you have mechanisms in place to judge its validity and origin? If yes, please give short description
	<p>Appropriate SOPs are implemented. This explains step by step how IFI staff should collect data while in the field and how it is classified and retained and who has access to the DEMS and at what level. To ensure transparency, the Privacy Statement should be verbally communicated to the individual prior to capturing footage and will be available online at https://www.fisheriesireland.ie/body-worn-cameras</p> <p>Appropriate SOPs and documents are:</p> <ul style="list-style-type: none"> • Body Worn Cameras SOP • IFI BWC Policy & Procedure • BWC Access Policy • IFI Communication of personal data breach to the Data Subject and Supervisory Authority • IFI DSAR Policy & Procedure • IFI Personal Data Retention Policy • Privacy Statement for Body Worn Cameras
3.9	Data Minimisation: Are you using the minimum amount of personal data possible, while still achieving your objectives? If yes, How do you make this decision?

	<p>Footage will only be captured once a body worn camera is activated following an on-the-spot assessment of the risk to an officer as detailed in section 1.2 above and below:</p> <p>IFI has developed a threat test that must be met prior to the activation of the camera. In addressing this threat to the officer, the following must be assessed:</p> <ol style="list-style-type: none"> 1. Proximity (The proximity of the threat); 2. Ability (The ability of the threatening person to carry out the threat); 3. Intent (The intent of the person to carry out the threat). <p>All IFI warranted officers undergo intensive Conflict Management QQI Level 6 training at the start of their employment with IFI where they learn to assess and manage conflict that may arise during the course of their enforcement work when interacting with stakeholders. All warranted officers underwent refresher training which occurred in late 2021-early 2022 with refresher training scheduled to take place every 3 years. Therefore, it is expected that Cameras will not be turned on unless the officers have identified through dynamic risk assessments that the situation has become hostile and is unsafe. All seasonal fishery officers undergo this training on employment with IFI at the seasonal fishery officers training college held in Spring every year if they are to become warranted officers.</p> <p>This ensures that the entire engagement with individuals is not captured which would be an excessive amount of data. Recording will only take place after the subject has been cautioned that filming is intended and that they are about to be recorded (Data Protection Act 1998 – 2018; GDPR (2006)) (Fair Notice) as follows:</p> <p><i>“This conversation will be recorded and may be used as evidence”.</i> Before recording commences followed by :</p> <p><i>“This conversation is being recorded on camera and may be used as evidence. You are not obliged to say anything but whatever you do say will be taken down in writing and may be given in evidence”</i>, once filming has commenced. Please see BWC SOP PAGE 10]</p>
3.10	Up-to-date information: Are you able to amend information when and where necessary to ensure currency and accuracy of personal information in your project and its applications?

The right to rectification is not relevant to the footage captured by the body worn cameras the only editing of images/ audio that can be undertaken is the use of the redaction studio in the DEMS (evidence.com)software. This allows the following:

The Redaction Studio includes options for frame-by-frame manual redaction, Spray Paint redaction (manual redaction during playback), object-tracking redaction, and audio redaction. These options can be used separately or together.

Redaction is a term used to describe the blurring of objects and removal of audio from video evidence. The following terms describe the components in Redaction Studio used to create a redaction:

- Video Mask — A rectangular area on the video that defines the objects that are redacted in a continuous segment of video frames. Video masks have their height and width defined by a Mask Frame and their duration defined by a Mask Segment.

There are two types of video masks, a Manual Mask and an Object Tracker mask.

- Audio Mask — A continuous segment on the Audio Track that defines the audio that is redacted. Audio masks have only duration, which is defined by a Mask Segment.

- Mask Segment — Defines the continuous series of frames that the audio or video mask redacts. A mask segment has a start and an end.

- Segment Timeline — The area below the audio track that shows all the video mask segments for the current redaction. This area allows users to easily find and select video masks.

- Video Mask Frame — Defines the rectangular area redacted by a mask in a video. Video mask frames can be manually moved and resized. After placement, Object Tracker video masks will automatically attempt to track the object they are placed over.

- Video Mask Frame Handle — Enables you to change the size and shape of the video mask frame.

- Spray Paint Redaction — A type of manual redaction where the user can click and hold on a manual mask during video playback at normal speed, half speed or rewind, and then use the mouse to follow the object the user wants to redact.

- Blur selector—Enables you to specify how blurred the area inside a video mask frame appears in the extracted video file. The selector supports five levels of blur and blackout:

 Extra Light blur	 Heavy blur
 Light blur	 Extra Heavy blur
 Medium blur	 Blackout

IFI's only action that will be taken to modify data is to blur images/audio of individuals- not applicable to case or data subject access request.

How long do you intend to keep the data and how do you justify your retention period?

3.11	What are the retention periods for the personal data or what are the criteria you use to decide for how long you will keep the personal data, and how will retention periods be implemented and assured?
	<p>The following are the determined automatic set retention periods for all data, they are as follows:</p> <p>Pre-classification</p> <ul style="list-style-type: none"> • Once camera placed in docking station any recordings are automatically transfer to the DEMS (Evidence.com) cloud and deleted from body worn camera. • Unclassified – 7 days (<i>i.e., recording made on camera, assessment made that <u>it does not</u> constitute a hostile/ aggressive incident, no action is made to categorise it to retain it past 7 days where it is automatically deleted from cloud.</i>) <p>Classifications (<i>Within pending review period, if prosecution is being brought the following categorisation must be set against the recording by end of 31 day pending review period. If not recording is automatically deleted from DEMS (Evidence.com) cloud</i>)</p> <ul style="list-style-type: none"> • Pending Review – 31 days (<i>i.e., recording made on camera, assessment made that <u>it does</u> constitute a hostile /aggressive incident and or a breach of fisheries legislation and time is given for it to be appropriately assessed and categorise for prosecution.</i>) • Assault on an Officer - 78 weeks (6 months to initiate a prosecution plus 12 months to go to court or appeal) • Fisheries Offence – 78 weeks (6 months to initiate a prosecution plus 12 months to go to court or appeal) <p>Retention periods are set by the authorised DEMS (Evidence.com) administrator. All uploaded data is 'uncategorised' until assigned a category. If not categorised within 7 days, data is automatically queued for deletion and deleted on the seventh day. Once categorised, the set retention period automatically applies.</p>
3.12	Could you envisage any exceptional circumstances for retaining certain personal data for longer than is necessary? If yes, will data be pseudonymised, in case data have to be retained?
	Data used as evidence in court may be retained for a longer period of time if a delay arises during court proceedings or in the event of a protracted appeal. The retention period can be amended to specific recordings as required by the DEMS (Evidence.com) administrator, who must give a reason as to why the data is being retained longer than the above stated retention periods.
3.13	How will personal data be fully anonymised or destroyed after it is no longer necessary or fit for purpose?

	<p>Data captured from the body worn camera is uploaded to the DEMS (Evidence.com) on docking and where it is then categorised within 7 days or automatically queued for deletion. Retention periods automatically apply to any categorised data. Uncategorised pending review data is erased per the automatically applied retention period (7days).</p> <p>When prosecutions are completed prior to the end of the set retention periods they can be queued for automatic deletion by the DEMS (Evidence.com) administrator, who must give a reason as to why the data is being deleted prior to the set retention period.</p>
--	---

How will you ensure that individuals can exercise their data subject rights?

<p>3.14</p>	<p>How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? Have you provided the data subjects with a copy of their rights? How and when? If there is a website associated with this body of work are data subject's rights displayed and easily referenced?</p> <p>Are your (technical) systems able to comply with any requests to exercise data subject rights? If no, detail how you intend to address this.</p>
	<p>IFI have a Subject Access Request Policy in place which will be adhered to if any requests are received. They will be managed and coordinated by the DPIO who will liaise with the appointed and appropriately trained River Basin District (RBD) administrator as per the BWC Access Policy and the regional BWC data guardians (River Basin Directors –Accountable data manager) to respond the request.</p> <p>The IFI website contains a link to the full Data Protection Policy in place which includes information on the exercise of data subject rights. IFI's data protection policies are undergoing review during 2024.</p> <p>The DEMS (Evidence.com) software has the ability to mark video footage on a timeline and generate standalone clips retaining all associated metadata and tags maintaining the integrity of the original footage as detailed in section 3.10 above. Data (with any appropriate redactions applied to third parties) may be shared to data subjects by a download link without the person downloading being able amend/edit the records/images by signing into Evidence.com.</p>

What appropriate technical and organisational measures will be put in place to protect data security and integrity?

<p>3.15</p>	<p>What governance structures are (will be) in place for this project? What procedures and policies are in place to ensure that all staff with access to the data have received adequate information governance training?</p>
--------------------	---

	<p>There is a BWC Access Policy that will be applied to the users of the DEMS (Evidence.com).</p> <p>All Pro-license users (Regional Administrators) received dedicated DEMS training on the 5-6th March 2024 at IFI HQ in Citywest by Axon.</p> <p>All Basic License users received training through regional roadshows on DEMs during April 2024.</p> <p>All fishery officers (camera only users) received training through regional roadshows during April 2024 on BWC SOP and how the DEMS works.</p>
<p>3.16</p>	<p>Security measures:</p> <ul style="list-style-type: none"> • What technical security will be in place e.g. encryption, firewalls, relevant Information Security Policies? • What organisational security will be in place e.g. secure disposal, staff training, limits on access? • How are staff authorised to access the data and how is access restricted? <p>Please detail below <i>what</i> is in place, <i>who</i> verified it and <i>when</i>. Please also detail what is not in place yet and when it will become available.</p>
	<p>Technical Measures</p> <ul style="list-style-type: none"> - Please see appendix 3 for- Cloud Security Questionnaire_FINAL.pdf - Axon only host IFI on their cloud system with their own force domain. IFI are the only ones with the ability to access and process the data captured on their body worn cameras on the DEMS system. <p>Organisational measures</p> <ul style="list-style-type: none"> - BWC Access Policy -to determine who has access to the data - BWC SOP for IFI field staff on how to use the cameras - DSAR Policy and Procedure - BWC Privacy Statement - Training staff on how to use the DEMS software – provided by AXON - Training staff on how to present the Privacy Statement verbally - Training staff on DSARs- how to use the redaction abilities on DEMS - Training staff on the use of BWCs <p>Access Restrictions</p> <ul style="list-style-type: none"> - Ensure that the hierarchy is outlined, and access is limited based on the roles within IFI – please see BWC Access Policy.

<p>3.17</p>	<p>Data processing and information format:</p> <p>Will you collect the information on paper, electronically, other?</p> <ul style="list-style-type: none"> • If you collect and process it electronically, how is the system you intend to use secured? • If you collect and process it in hard copy format, how will you assure it stays out of reach of any unauthorised individuals? <p>Provide a description of the data processing activities that will be carried out, e.g. chart review; client survey; etc.</p>
	<p>The data will be digitally captured by the body worn camera. Data will be erased from the camera on uploading to the cloud-based Digital Evidence Management System (DEMS – Evidence.com).</p>
<p>3.18</p>	<p>If your project receives a data subject access request, do you have a process in place that details how it has to be handled, by whom, who decides if it is valid or not, and who needs to be informed of the request, locally and centrally?</p>
	<p>IFI has a Subject Access Request Policy which will be referred to in the event that an access request is made. The process includes redacting any images/audio to ensure that there are no third parties identified.</p>
<p>3.19</p>	<p>Information transmission:</p> <p>What security measures will be used to transfer any identifiable information, i.e. to collaborators, processors, data subjects, etc.?</p> <ul style="list-style-type: none"> • Have you identified any potential risk that can affect transmission? • Considered the potential impact of any such risk on the data subject? • Evaluated the likelihood and severity of any risk? • Decided how you intend to deal with these risks?
	<p>Data may be shared outside of IFI by unauthenticated link from Evidence.com.</p> <p>Impact on data subject is the unauthorised access and or sharing of their personal data by third parties.</p> <p>Likelihood of this happening is low as the link will be provided to dedicated email address provided by the data subject, or they will be facilitated by nominating a solicitor from IFI's approved list of solicitors for the link to be sent to, to view. Audit report downloadable from DEMS on all viewings and actions undertaken in regards to shared data. Videos are only enabled to be viewed on guest DEMS link and video download has been disabled. Watermark on video which displays who is viewing the video so any over the shoulder third party recording can be traced back.</p>

Do you intend to transfer personal data either internally or externally (including international data transfer outside of the EEA (European Economic Area), or both?

3.20	Will individual's personal information be disclosed internally/externally in identifiable form and if so to whom, how and why?
	If a claim/proceeding is taken, this footage may be disclosed as evidence if applicable. This will only be shared via secure link to the nominated solicitor.
3.21	Will personal data be transferred to a country outside of the European Economic Area? If you use a cloud provider that has servers outside the EEA, this also constitutes transfer outside the EEA. It is your responsibility as data controller to check this and take measures to assure data subject rights are assured. If data transfer beyond the EEA happens, what arrangements will be in place to safeguard the personal data? Have you sufficiently informed your data subjects of such international data transfers? [Also see Rules for the protection of personal data inside and outside the EU]
	No – Axon servers are based in Ireland and the Netherlands
Consultation – link back to the stakeholders identified in Section 1 - 1.6 of this document	
3.22	Who should be consulted to identify privacy and any other risks related to a data subject's rights and freedoms? (Identify both internal and external stakeholders) How will risk identification be achieved? Describe below

Internally

- Data Protection & Information Officer
- Senior Management Team (SMT)
- Specific IFI staff involved with various management elements.
- Human Resources team
- Union representatives
- All staff via regional roadshows in April 2024
- Seasonal Fishery Officer Training College
- Body Worn Camera Working Group

External

- Angling Stakeholder Associations

Angling Council of Ireland	Trout Anglers Federation of Ireland
Irish Federation of Pike Angling Clubs	Irish Angling Development Alliance
Irish Pike Society	NCFFI
Irish Federation of Sea Anglers	Salmon and Sea Trout Recreational Anglers of Ireland
European Federation of Sea Anglers of Ireland	Federation of Irish Salmon and Sea Trout Anglers
National Angler Representative Association	Irish Trout Fly Fishing Association

- Axon -technical measures questionnaire and training on use of DEMS
- An Garda Síochána
- External Data Protection Advisors consulted with in terms of data protection risks and issues that should be addressed.

3.23

What risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.
You should also include consultation with the data subject or their representative organisations – have their views been sought?

	<p>Risks identified are listed in section 4 of this DPIA</p> <p>Public consultation with data subjects via: Angling Representative bodies and IFI staff members as above in section 3.22 and with IFI's Legal representatives in fisheries enforcement cases, have identified risks.</p>
What is the scope of the processing?	
3.24	<p>How big is the data set?</p> <p>Are you collecting 1) large amounts of data from a small number of people; 2) a limited number of data from a large number of people; 3) large amounts of data from a large number of people; 4) a limited number of personal data from a small number of people? Detail below the estimated data volumes, number of individuals or records, processing durations and the anticipated size of the final data set.</p>
	<p>The data collected will be very limited, and will relate to a very small number of people, as the body worn camera will only be used to record specific events and incidents that may occur. The activation of body worn cameras is seen as the exception. Staff are extensively trained in conflict management and the de-escalation of potentially hostile situations as per conflict Management QQI level 6 training as detailed above.</p>
3.25	<p>Identify 1) how often the personal data will be collected and 2) how often the processing will take place.</p>
	<p>1)The frequency of the data collection cannot be determined as it will depend on the occurrence of an incident. The body worn cameras will only capture footage once they have been activated.</p> <p>2) Activation of the camera will only occur if attempts to deescalate a situation has not been successful and there is a clear and imminent risk of assault to the officer(s) and/or a breach of the various relevant legalisations: Fisheries Consolidation Act 1959, Local Government and Water Pollution Acts 1977 & 1990 and the Sea Fisheries and Maritime Jurisdiction Act 2006.</p>
3.26	<p>Describe the geographical area(s) data subjects are from/reside in?</p>
	<p>Ireland, international tourists</p>
3.27	<p>Will the data processing be undertaken in more than one country? If yes, give details.</p>
	<p>No – Ireland only</p>

Did you use guidance and best practice?	
3.28	<p>List any national, sector specific or other guidance applicable to your project/data processing activity/technology that you used. Include WP29, EDPB, EDPS, ENISA, EU Commission etc., or other EU National SA guidelines or law firm guidance or legal opinion/advice. You can give a reference and link as well as append to DPIA.</p>

In Section 1 to Section 3 of this DPIA you and your team looked at your project/data processing activity description; you undertook an analysis of personal data to be used; and you did an analysis of project/data processing activity/technology application of data protection principles. Now your next step is to use these insights to identify any potential risks the processing of the personal data could pose to privacy and other rights and freedoms of data subjects involved. Considering severity, likelihood and impact of those risks you can start designing measures that will minimise or ideally eliminate those risks.

Section 4: Risk Assessments & Risk Remediation Solutions

Looking at risks involves assessing the level of risk before any measures are applied, and then the anticipated, and ultimately quantified, level of risk after the measures were applied. If risks still remain high, even after measures would be applied, it is very likely that the DPC will need to be consulted.

[See Appendix: App.1 for List of 'Types of Risks' & App.2 –'Guidance for completing a Risk Register']

Risk Ref No	Risk Title	Risk Description	Risk Score	Recommendation	Net Score
DPIAIFI/Risk1	Due Diligence: BWC Software/Evidence.com	During our documentation review, it has been noted that information from the cameras will be briefly stored on a cloud based Digital Evidence Management Systems, and that IFI data and backups will be held on Axon servers within the EU in Ireland and the Netherlands.	10 (Likelihood: 2, Impact: 5)	It is recommended that the company conducts a due diligence assessment of the data storage facility from both a technical and organisational perspective, as the data being stored in the EU does not necessarily connote organisational compliance with the data protection legislation, and due to the sensitivity of the data being stored in question, it would be most prudent for IFI to conduct a full review, particularly as they are necessitated by data protection legislation to ensure the processors they engage with are GDPR compliant.	0 (Likelihood: 0, Impact: 0)
DPIAIFI/Risk2	Tiered Access	It has been noted during the documentation review that users will 'have access to the system based on the scope of their responsibilities'. However, this has not been expanded upon within the DPIA itself.	10 (Likelihood: 2, Impact: 5)	An explicit access policy should be created for the purpose of accessing data as well as retention for staff use. It is recommended that access is tiered based on staff role, and that access is not granted to too many workers, but rather management staff only.	3 (Likelihood: 1, Impact: 3)
DPIAIFI/Risk3	Data Backup Process	During the review of the DPIA it has been noted that IFI intends to, but has not, outlined a process for backing up data.	12 (Likelihood: 3, Impact: 4)	IFI should outline a policy of how, and when, and by who, data will be backed up. This policy should also entail how, and when, and by who, data will be deleted, where appropriate. It is recommended that IFI engage with the service providers to ensure that this backup process is outlined.	6 (Likelihood: 2, Impact: 3)
DPIAIFI/Risk4	Data Processing Agreement: AXON evidence.com	It has been noted that evidence.com by AXON is used for storage data. It is not articulated as to whether a DPA or data protection addendum has been put into effect between IFI and Amazon Web Services.	15 (Likelihood: 3, Impact: 5)	Under section 80 of the Data Protection Act 2018 IFI needs to ensure that Amazon Web Services adheres to the requirements set out in compliance with section 80(1)(a) and (b). The contract in writing between the controller and the processor must comply with the requirements set out in section 80(2)(a)-(vi) of the 2018 Act.	3 (Likelihood: 1, Impact: 3)
DPIAIFI/Risk5	Pre-Record Function	Axon body cameras are constantly recording and overwriting the last 30 seconds. Therefore, when a user begins recording, the previous 30 seconds will also be recorded, albeit without sound. This feature is arguably not transparent to the data subject. The data subject will also have technically not received fair notice that processing has begun.	15 (Likelihood: 5, Impact: 3)	It is recommended that this feature is turned off due to the lack of fair notice given to the recorded individual prior to the recording commencing. If this function is not turned off, fair notice will have to be amended to reflect that footage is captured 30 seconds before the recording is started. One suitable approach may be to give the fair notice at the beginning of the interaction with the individual, outlining that they may utilise their body camera during the engagement, the purposes for recording (the safety of the inspector/officer) and where to find further information if required.	0 (Likelihood: 0, Impact: 0) If not enabled





DPIAIFI/Risk6	Body camera live-streaming	It has been noted during a review of the DPIA document, as well as a subsequent interview, that the body camera has the ability to livestream the incident to a manager within the IFI headquarters. Livestreaming is a different form of processing to recording, having different functions. This should be outlined by IFI, if a decision is made to go ahead with livestreaming.	25 (Likelihood: 5, Impact: 5)	Upon beginning to record, the recording individual should make it clear to the individual that the body camera is both recording and live-streaming the event to a person within the IFI headquarters. Similar access controls must be implemented in relation to access to the live-stream of these cameras. This function will not be utilised. IFI does not have a central headquarters or control room facility to monitor live events.	0 (Likelihood: 0, Impact: 0) If not enabled
DPIAIFI/Risk7	Process for Staff Identification of Situation in which Recording is to be Permitted	The DPIA conducted by IFI recognises that the only point at which an employee of IFI is allowed to record, is in the situation in which they are of the opinion that a fisheries offence has been, or is in the process of being committed, and or if they are concerned for their own safety in the circumstances that prevail, This is unclear and may cause confusion.	15 (Likelihood: 3, Impact: 5)	It is recommended that IFI outline a set of policies that employees will be liable to follow and understand as to how, and when, and where they can operate their BWCs. The conditions must be strictly adhered to, and it is recommended that training is conducted, as well as annual re-training to ensure on-going compliance. The sole justification/purpose for the cameras will be for the protection of employees of IFI when conducting engagement with the public.	6 (Likelihood: 2, Impact: 3) (Chance exists that staff will forget to identify themselves)
DPIAIFI/Risk8	Identity Verification	It has been noted during the documentation review and our interviews that there is no arrangement or policy set out for identity verification of person's requesting information. Due to the potentially sensitive information and the possibility of information being used in a criminal prosecution, it would be ill-considered to have no formal policy for employees to adhere to when responding to data subject access requests.	15 (Likelihood: 3, Impact: 5)	The IFI is recommended to determine how they would wish to identify identities of individuals who make data access requests. However, it is recommended that the IFI adheres to the Recital 64 of the GDPR, which states that a controller should use all reasonable measures to identify a data subject who requests access in particular in the context of online services and online identifiers, but they should not retain information for the sole purpose of identifying someone. Due to the potential sensitive nature of this information, it is recommended that the IFI has a policy and process for 'blurring' all persons in a video which are not the data subject, and that the IFI creates a process of identification.	3 (Likelihood: 3, Impact: 1)




DPIAIFI/Risk9	Body Worn Cameras: Monitoring of Employees	<p>During the documentation review, it has been noted that the selected cameras which will be used by employees have the potential to 'track employees' -- this has been selectively mentioned in the DPIA. The cameras have a 'GPS system' -- it is further noted that at the station with the Axon Evidence software, a GPS marker updates from 'grey' to 'green' when recording begins. This suggests that prior to this, IFI is able to see, in live-time, where an employee is. This is overbearing and may be used outside of the parameters of the original intention of usage to monitor employees.</p>	<p>25 (Likelihood: 5, Impact: 5)</p>	<p>The GPS being continuously enabled is over-handed for the purpose, and may actually extend beyond the initial purpose (explicit and identified purposes) and may even reveal sensitive information about an employee. It is also questioned as to whether employees are aware of how potentially invasive this feature may be. The Working Party under Article 29 has created an opinion piece on data processing at work on the 8 June 2017, stating that in the case a company or organisation wishes to monitor its employees, it cannot rely on consent, and technical and organisational measures must be in place. It is noted that the EU has not endorsed these guidelines, as it has with some others. However, it is recommended that this feature is entirely not enabled, and that it is not possible to be re-enabled by a singular individual overseeing the software due to the possibility of harassment arising out of this feature.</p>	<p>0 (Likelihood: 0, Impact: 0) If monitoring fully disabled, difficult to re-enable. 15 (Likelihood: 3, Impact: 5) If possible to easily re-enable monitoring.</p>
DPIAIFI/Risk10	Body Cameras: Stealth Recording Mode	<p>During the documentation review, it has been noted that the Axon cameras have a potential to enter 'stealth' mode, if a person presses and holds the Volume down button for 3 seconds. This entire feature poses a risk as it is in principle noncompliant with the GDPR principle of lawful, fair, and transparent processing. This is problematic not only on the sole basis of being not in compliance with the GDPR, but if a person were to accidentally enable this mode while collecting information which will be used in a criminal offence, this evidence may be made inadmissible -- there has been no cases on this in Ireland, but one may consider the British case of Mustard v</p>	<p>10 (Likelihood: 2, Impact: 5)</p>	<p>To ensure compatibility with the data protection legislation as well as ensuring that information used in criminal proceedings is admissible and not challenged on the fact it was obtained unlawfully, it is recommended that this mode is fully turned off and inaccessible to employees.</p>	<p>0 (Likelihood: 0, Impact: 0)</p>








		Flower and Others [2019] EWCH -- while evidence during a court case is not inadmissible just because it was obtained unlawfully, in this case, it was considered admissible on the basis the recording was made by a private person for their own purposes -- thus the GDPR does not cover them. However, in the case of IFI, they are not a private person recording for their own personal purposes with the data subject being themselves, as in the Mustard case.			
DPIAIFI/Risk11	Body Worn Cameras: Organisational Measures	It has been noted that for the videos to be accessible, that they must be physically docked into a station. To ensure organisational measures are followed as per the data protection legislation, it would be advised that the room where the camera docking station, and cameras themselves are kept, is locked and not accessible by every employee for accountability and transparency. All cameras must be docked on return if the record function was engaged.	10 (Likelihood: 2, Impact: 5)	To ensure ongoing organisational security and to foster a culture of data protection awareness, it is recommended that the room is inaccessible at most times to employees and that access is similarly tiered as to the videos and software itself.	3 (Likelihood: 1, Impact: 3)
DPIAIFI/Risk12	Enforcing Transparency: Irish Translation of Warnings for the Public	Under the Constitution, Irish is recognised as the primary language of Ireland. There has also been court cases wherein a person argued their right to	4 (Likelihood: 2, Impact: 2)	While it is highly unlikely that someone would challenge IFI on this basis, it is nonetheless recommended that IFI provides an Irish translation of information that is given out to persons who are fishing in Irish.	0 (Likelihood: 0, Impact: 0)


		receive official documentation translation in Irish.			
DPIAIFI/Risk13	Defined Retention Schedule	While it was noted during our interviews that the cameras have an overwrite function and the ability to delete videos from the docking station, these retention schedules have not been included into the DPIA. Furthermore, due to the lack of DPA with Axon, retention periods cannot be enforced.	16 (Likelihood: 4, Impact: 4)	It is recommended that IFI include a retention schedule into their DPIA and ensuing documentation. Furthermore, this retention period should be contractually enforced with Axon. A 30 day period for recordings that will not be followed up with a prosecution is recommended. This will also lighten the burden on the IFI in the case of a DSAR and will ensure that videos are not leaked or otherwise distributed.	4 (Likelihood: 2, Impact: 2)
DPIAIFI/Risk14	Deletion of Old Files	It has been noted that there is no agreement between Axon and IFI as to how and in what way files will be deleted.	16 (Likelihood: 4, Impact: 4)	It is recommended that a policy is drafted as to the uploading, review, and subsequent deletion handling. It is also recommended that this should be recorded in a ROPA or 'records of processing activities' but also should leave a paper trail to justify deletion of old files to ensure that in the case of a DSAR, a person handling the request is able to quickly and efficiently check why a certain piece of data has been removed.	4 (Likelihood: 2, Impact: 2)
DPIAIFI/Risk15	Breach Reporting Mechanism for Axon Body Cams	It has been noted that there is currently no breach reporting mechanism that has been identified within our DPIA analysis.	16 (Likelihood: 4, Impact: 4)	It is recommended a breach reporting policy is drafted to ensure that in the event that a breach does occur, employees understand what to do within the framework of a formalised structured response system. Furthermore, while the data protection legislation enforces the requirement of breach reporting functionalities between two parties undertaking a data sharing relationship and therefore must have procedures for data breaches, it would be beneficial if this policy was shared with Axon for potential feedback. It is also recommended that IFI discuss breaches with Axon to understand whether any have occurred and what the current response would feature.	6 (Likelihood: 2, Impact: 3)
DPIAIFI/Risk16	Unauthorised download of video/ jpeg files from DEMS	It has been noted that videos and jpegs can be downloaded from DEMS by Basic & Pro-Licence users	9 (Likelihood: 3, Impact: 3)	Recommended that this option is disabled by the system administrator so videos and or images cannot be downloaded.	3 (Likelihood: 1, Impact: 3)

Risk Mitigations Applied



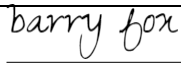

Risk Ref No	Risk Title	Actioned to	Action taken	Updated Net Risk Score	Risk Owner Signature	Date Completed
DPIAIFI/Risk1	Due Diligence: BWC Software/Evidence.com	Ian Carroll , Acting Head of ICT	ICT questionnaire undertaken for GDPR assessment & Data Protection Agreement (DPA) in place to ensure GDPR compliance	0 (Likelihood: 0, Impact: 0)	 Signer ID: ITR1HKOKVN...	10/05/2024 IST
DPIAIFI/Risk2	Tiered Access	Sean Long , Project Manager	BWC Access Policy completed and licenses and groupings assigned.	3 (Likelihood: 1, Impact: 3)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST
DPIAIFI/Risk3	Data Backup Process	Sean Long , Project Manager	BWC SOP details how, and when, and by who, data will be backed up, when deleted, where appropriate.	6 (Likelihood: 2, Impact: 3)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST
DPIAIFI/Risk4	Data Processing Agreement: Axon (Evidence.com)	Sean Long , Project Manager	Data Processing Agreement not required as AXON are not processing on behalf of IFI. They are hosting a force domain which IFI only have access to on evidence.com . Tender contract covers data protection concerns.	0 (Likelihood: 0, Impact: 0)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST
DPIAIFI/Risk5	Pre-Record Function	Sean Long , Project Manager	This feature has been turned off. No 30 second pre-recording will be enabled on any of the BWC this will be	0 (Likelihood: 0, Impact: 0) If not enabled	 Signer ID: AQO3VLJD7P...	10/05/2024 IST

			set by the Chief Administrator across all cameras			
DPIAIFI/Risk6	Body camera live-streaming	Sean Long , Project Manager	IFI does not have a central headquarters or control room facility to monitor live events. The live streaming functionality will not be turned on and has been disabled on DEMS.	0 (Likelihood: 0, Impact: 0) If not enabled	 Signer ID: AQO3VLJD7P...	10/05/2024 IST
DPIAIFI/Risk7	Process for Staff Identification of Situation in which Recording is to be Permitted	Sean Long , Project Manager	BWC SOP details when BWC should be operated. Training around this is currently been developed.	6 (Likelihood: 2, Impact: 3) (Chance exists that staff will forget to identify themselves)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST
DPIAIFI/Risk8	Identity Verification	Sarah Healy -DPIO	IFI have reviewed and updated their Data Subject Access Request Policy & Procedure. Due to the potential sensitive nature of this information, IFI will utilise the redaction studio on evidence.com for 'blurring' all persons in a video which are not the data subject,	3 (Likelihood: 3, Impact: 1)	 Signer ID: NVTBF1R99A...	10/05/2024 IST
DPIAIFI/Risk9	Body Worn Cameras: Monitoring of Employees	Sean Long , Project Manager	Location capture only available if 'Axon Respond feature is licenced.' .	0 (Likelihood: 0, Impact: 0) If monitoring fully disabled, difficult	 Signer ID: AQO3VLJD7P...	10/05/2024 IST

			IFI is not licencing this feature.	to re-enable. 0 (Likelihood: 3, Impact: 5) If possible to easily re-enable monitoring.		
DPIAIFI/Risk10	Body Cameras: Stealth Recording Mode	Sean Long , Project Manager	Stealth Recording Mode is fully turned off and inaccessible to employees.	0 (Likelihood: 0, Impact: 0)	 Signer ID: AQO3VLJD7P...	09/05/2023 10/05/2024 IST
DPIAIFI/Risk11	Body Worn Cameras: Organisational Measures	Sean Long , Project Manager	BWC Access Policy completed	3 (Likelihood: 1, Impact: 3)	 Signer ID: AQO3VLJD7P...	09/05/2023 10/05/2024 IST
DPIAIFI/Risk12	Enforcing Transparency: Irish Translation of Warnings for the Public	Sean Long , Project Manager	As detailed in pages 6-8 of BWC SOP signage will be in both Irish & English	0 (Likelihood: 0, Impact: 0)	 Signer ID: AQO3VLJD7P...	09/05/2023 10/05/2024 IST
DPIAIFI/Risk13	Defined Retention Schedule	Sean Long , Project Manager	Retention schedule has been included in this DPIA in section 3.11 and detailed in the SOP	4 (Likelihood: 2, Impact: 2)	 Signer ID: AQO3VLJD7P...	09/05/2023 10/05/2024 IST
DPIAIFI/Risk14	Deletion of Old Files	Sean Long , Project Manager Sarah Healy, DPIO	IFI'S ROPA updated, uploading, review, and subsequent deletion of data inputted into BWC SOP policy. Evidence.com keeps an audit trail which can be extracted in relation to any deleted data.	4 (Likelihood: 2, Impact: 2)	 Signer ID: AQO3VLJD7P...  Signer ID: NVTBF1R99A...	10/05/2024 IST 10/05/2024 IST
DPIAIFI/Risk15	Breach Reporting Mechanism for Axon Body Cams	Sean Long , Project Manager	IFI has the following policy & procedure in place Communication of personal data breach to the data	6 (Likelihood: 2, Impact: 3)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST

			subject & Supervisory Authority			
DPIAIFI/Risk16	Unauthorised download of video/ jpeg files from DEMS	Sean Long , Project Manager	IFI has disabled the ability to download videos and jpegs from DEMS and via shared links	3 (Likelihood: 1, Impact: 3)	 Signer ID: AQO3VLJD7P...	10/05/2024 IST

Section 5: Documentation of DPIA Outcomes & Decisions

Item	Name/date	Notes
Measures approved by:	Sean Long  10/05/2024 IST	Integrate actions back into project plan, with date and responsibility for completion
DPO advice provided:	Sarah Healy, 27 th February 2024	DPO should advise on compliance, measures and whether processing can proceed
<p>Summary of DPO advice:</p> <p>DPIO advises that staff who receive BWC for use as part of operational role, have both QQI Conflict Resolution Training received and training on use of BWC (Training on the SOP – Use of BWC). This is important as the conflict resolution training is cited in the DPIA for BWC in the Necessity and Proportionality Test and also as a mitigating factor for staff using BWC. It demonstrates that they are trained in identifying a 'hostile' or a 'hot' situation and have the tools to deescalate before having to turn on a BWC as a last resort.</p> <p>Important to have adequate training records in place to be able to demonstrate QQI conflict Resolution training has been completed and any required refreshers are within date for staff using BWCs.</p>		
DPO advice accepted or overruled by:	Sean Long  10/05/2024 IST	If overruled, you must explain your reasons
Comments:		
Residual risks approved by:	Barry Fox  10/05/2024 IST	If accepting any residual high risk, consult the Data Commissioner before going ahead
Consultation responses reviewed by:	Sean Long  10/05/2024 IST	If your decision departs from individuals' views, you must explain your reasons

Comments:		
This DPIA will be kept under review by:	Sean Long, Project Manager/ River Basin Director	The DPO should be informed of changes that affect the risk levels
Next Review Date:	13 th May 2025	

App. 1 - Guidance for completing a Risk Register

Impact	Likelihood				
	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Highly Likely
1 - Negligible	1	2	3	4	5
2 - Minor	2	4	6	8	10
3 - Moderate	3	6	9	12	15
4 - Major	4	8	12	16	20
5 - Critical	5	10	15	20	25

- What is the actual risk? Make sure the risk is clear and concise, well understood and articulated with appropriate use of language, suitable for the public domain.
- Risk Evaluation
 - Likelihood
 - Impact
 - Risk 'Score'
- Assignment of Risk Actions – who is responsible for mitigation?
- Heat Map: It is common to use a red / amber / green (RAG) matrix rating system for assessing risk. Each risk will be RAG-rated by multiplying the likelihood score by the impact score and plotting the risks using the matrix to the right.

Risk Mitigation Actions

- Embrace, but reduce likelihood
- Embrace, but reduce impact
- Deflect – Outsource
- Protect – Seek insurance
- Avoid – Discontinue

Risk Score	Number
1	
2	
3	
4	
5	
6	
8	
10	
12	
15	
16	
20	
25	
Total:	

App. 2 – Conflict Management QQI Level 6 – Programme modules

Programme outcome	Award Outcome	Assessment Method
Relevant legislation with respect to conflict resolution and self-defence.	LO2	Project
Legal aspects of powers to prosecute under Fisheries Acts	LO2	Project, Assignment
Removing ourselves from threatening situations and guidelines on dealing with anglers.	LO3, LO4, LO9	Project
Conflict resolution theory & techniques	LO1, LO3, LO4,	Project
Incident recording, reporting	LO8	Assignment
Debriefing	LO8	Learner record
Reporting to the Gardaí (When & how). Addressing assaults to officers when not on duty.	LO9	Assignment
The practical application of basic self-defence, control & breakaway techniques and an evaluation of trainee's ability to successfully perform techniques	LO5, LO6	Learner record
Using a fence and remaining a safe distance from potential aggressors.	LO5, LO6	Learner record
Techniques to break away from grabs & holds	LO5, LO6	Learner record
Court procedure		
Preparing and giving evidence, cross examination in the context of a fisheries case study	Lo3, LO4	

Training Outcomes

At the end of this programme you will be able to:

App. 3 - Cloud Security Questionnaire_FINAL.pdf

1 Overview

Theme	Topic/Question	Answer (Y, N, N/A)
1. Certifications		
Q1.1	Are you certified SSAE 16 SOC2 type 2?	YES
Comment	<p>Axon has achieved AICPA SOC 2 Type 2 reporting. A SOC 2 audit gauges the effectiveness of the Axon Evidence service based on the AICPA Trust Service Principles and Criteria. The Axon SOC 2+ report includes a comprehensive description of the Axon Evidence service in addition to an assessment of the fairness of Axon's description of its controls. The SOC 2+ evaluates whether Axon's controls are designed appropriately, were in operation on a specified date, and were operating effectively over a specified time period. Axon is audited annually against the SOC reporting framework by independent third-party auditors.</p>	
Q1.2	Are you certified ISO 27001? If so, what is the scope of the certification?	YES
Comment	<p>Axon is ISO certified, in addition to others listed below. Axon makes it a mission to adhere to and obtain widely accepted certifications and reporting processes that demonstrate industry-standard practices, which include:</p> <ul style="list-style-type: none"> • ISO 27001:2013 • ISO 27018:2014 • ISO 9001:2015 • CSA STAR (Level 1 and Level 2) • Achievement of AICPA SOC 2 Type 2 reporting and incorporation of additional criteria, including the UK NCSC Cloud Security Principles into our annual SOC 2 report 	

Q1.3	Are you certified PCI DSS 2.0 (applicable if credit card information is managed)?	N/A
Comment	This certification is not applicable to Axon's services or products.	
Q1.4	Are you certified SOX (if applicable)?	N/A
Comment	This certification is not applicable to Axon's services or products.	

Theme	Topic/Question	Answer (Y, N, N/A)
Q1.5	Are you certified HIPAA Through the Business Associate Agreement (BAA) (if applicable)?	N/A
Comment	This certification is not applicable to Axon's services or products.	
Q1.6	Are you certified SkyHigh Enterprise Ready?	N/A
Comment	This certification is not applicable to Axon's services or products.	
Q1.7	Are you certified against any other relevant external standard? If so, please indicate.	Yes
Comment	<p>Axon's compliance demonstrates our commitment to providing a trustworthy platform and offers customers a way to understand the controls that have been put in place to secure Axon Evidence and their data. Axon holds the following certifications for Axon Evidence.</p> <ul style="list-style-type: none"> • Axon Evidence is OFFICIAL SENSITIVE suitable • Axon is Cyber Essentials certified • CJIS Compliant • ISO Certifications, as mentioned above • SOC 2+ Report • Cloud Security Alliance - CSA STAR Attestation (Level Two) • Cloud Security Alliance - CSA STAR Self-Assessment (Level One) 	
2. Contract		
Q2.1	Do you accept a Non-Disclosure agreement / confidentiality clause to cover the contracting process and external supplier staff?	YES
Comment	Axon takes confidentiality and data privacy seriously. We take all precautions to ensure ours and customer data is protected at all times.	
Q2.2	Are you sub-contracting any activities within	NO
Comment	Axon is the sole provider of our product lines; everything from manufacturing to software development, to deployment and training is conducted in-house. We are uniquely suited to provide a solution within your desired timeline.	
Q2.3	Which countries will be hosting data (including the backup and disaster recovery)? Is personal data hosted outside of EU? If it is in USA, is your company part of the EU-US Privacy Shield?	YES
Comment	<p>Any IFI data will not live outside of your region and this includes backup data. The datacentres utilised that IFI can choose from are:</p> <p>EU – Ireland EU - Netherlands UK – London and Cardiff</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q2.4	Do you have and use a documented contract management process?	YES
Comment	Axon follows industry standards for contract and service management, including those under ITIL and industry best practises.	
Q2.5	Which legal jurisdiction is governing the contract or SLA?	YES
Comment	The legal jurisdiction for this contract and SLA is: Republic of Ireland	
Q2.6	Do you formally define in the contract the roles and responsibilities for contract, delivery and information security management?	YES
Comment	Axon has a contracts team that consist of legal representatives and information security personnel who are trained and subject matter experts on these topics within your region. All of these matters are defined within the contract so that roles, responsibilities, delivery, and information security management are clearly defined.	
Q2.7	Does the contract or SLA have a penalties schedule when failing to meet the contract's information security requirements?	YES
Comment	SLA's are clearly defined within Axon's contracts, ensuring all parties are aware of expectations and any applicable penalties.	
Q2.8	Do you allow for the 'right to audit' regularly and / or on demand?	YES – see notes
Comment	<p>With regards to customer audit requests, please see our responses below, broken out by audit request type:</p> <ul style="list-style-type: none"> • Audit of Axon: Yes, Axon can coordinate with the IFI to perform logical audits of Axon Evidence services with advance notice, in order to allow you to gain reasonable levels of assurance related to the security, integrity and confidentiality of your data. Upon request from IFI, our Information Security team will work with you to coordinate reasonable efforts on this matter, with the understanding that • Audit of Physical datacentres: No, Physical access to infrastructure data centres is prohibited for security reasons and to protect the integrity of the assets. The only access is through the application to ensure audit tracking. Redundant, geo-dispersed hardware and gateways are used throughout the Axon Evidence infrastructure. Customer data is replicated between two datacentres, with each one offering world-class security and system protection. Datacentres employ backup power, climate control, alarms, and seismic bracing. 	

Theme	Topic/Question	Answer (Y, N, N/A)
Q2.9	Do you allow penetration testing assignments on the outsourced assets / applications? Would this affect other clients?	See Notes
Comment	<p>Due to strict security protocols, customers are not authorised to conduct application security testing. However, Axon works with external security firms to perform penetration testing, as detailed below. This testing does not affect clients on the application.</p> <p>Vulnerability scans are performed monthly. Additionally, Axon Evidence penetration tests are conducted frequently to validate the security of our systems and adjust as necessary.</p> <p>Penetration tests are performed by external, industry-leading security firms and include testing against the OWASP Top 10. These tests are supplemented by monthly vulnerability scans conducted by our internal Information Security team. All discovered issues are managed and tracked through completion by the Axon Information Security team.</p> <p>As previously mentioned, Axon hires independent firms to perform security and penetration testing of Axon Products and is willing to work with customers on any customer-initiated testing activities as long as they conform to Axon's Penetration Testing & Vulnerability Disclosure Guideline, which can be reviewed here: axon.com/penetration-testing--vulnerability-disclosure.</p>	
Q2.10	Do you have a nominated contract responsible for handling the contract termination?	YES
Comment	Axon has dedicated personnel that specifically handle these tasks if a contract termination were to happen.	
Q2.11	Do you include in your contract clauses for data destruction, escrow, asset return and survival of obligation (e.g. data retention) (if applicable) on termination?	Yes
Comment	<p>Axon's contracts will include topics that are applicable to our products and services being provided to IFI, these can include topics such as:</p> <ul style="list-style-type: none"> • Asset return, if applicable • Data destruction, if applicable • Escrow, if applicable • Survival of obligation, if applicable <p>Axon's contracts are constructed to ensure that you retain all ownership of your data. All digital evidence stored n Axon Evidence is owned by IFI. Axon is only a data processor of IFI content; and IFI controls and owns all right, title, and interest in and to IFI data and Axon obtains no rights to it.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q2.12	Do you provide a certificate of return / or destruction?	YES
Comment	If requested, Axon will provide a certificate of return or destruction.	
Q2.13	What are the SLAs that you provide in your contract?	Yes
Comment	Please refer to: https://www.axon.com/products/axon-evidence/sla For information on general service availability and credits. Axon also provides and SLA for incident response – https://www.axon.com/security/cloud-services-incident-handling	
Q2.14	Does the contract provide the description of the incident management process with time recovery objectives?	YES
Comment	Additionally, Axon Evidence is designed for a zero RPO (Recovery Point Objective) and less than 15-minute Recovery Time Objective (RTO) in the event of most adverse actions.	
Q2.15	Does the contract define types of logs and reports available for the customer, their content and frequency of delivery?	YES
Comment	The contract defines how customers can access Axon Evidence system, which enables self-access to these items (e.g. logs, reports, and audit information). All customer tenant logs including access logs, user sessions, and data history, can be retrieved by IFI administrators. The following link provides a copy of the Administrator Reference Guide, which details how this data can be extracted by IFI: http://public.evidence.com/help/pdfs/latest/EVIDENCE.com+Administrator+Reference+Guide.pdf	
Q2.16	Does the contract explicitly state that customer data shall be used exclusively for the purpose as agreed between provider and customer?	YES
Comment	Axon is only a data processor of IFI content and data. Axon employees do not have access to a customer's evidence data without explicit authorisation from the customer. The only exception to this is for a small team of administrators who would only access evidence data in the event of a system emergency. Axon's contracts are constructed to ensure that you retain all ownership of your data. All digital evidence stored on Axon Evidence is owned by IFI. Therefore, all management of data is handled strictly by IFI.	

Theme	Topic/Question	Answer (Y, N, N/A)
3. Compliance		
Q3.1	Do you independently regularly check security (e.g. by a penetration test, review or audit of controls)?	YES
Comment	<p>Vulnerability scans are performed monthly. Additionally, Axon Evidence penetration tests are conducted frequently to validate the security of our systems and adjust as necessary.</p> <p>Penetration tests are performed by external, industry-leading security firms and include testing against the OWASP Top 10. These tests are supplemented by monthly vulnerability scans conducted by our internal Information Security team. All discovered issues are managed and tracked through completion by the Axon Information Security team.</p> <p>As previously mentioned, Axon hires independent firms to perform security and penetration testing of Axon Products and is willing to work with customers on any customer-initiated testing activities as long as they conform to Axon's Penetration Testing & Vulnerability Disclosure Guideline, which can be reviewed here: axon.com/penetration-testing--vulnerability-disclosure.</p>	
Q3.2	Do you regularly test Business Continuity Plans / Disaster Recovery (BCP/DR) arrangements (e.g. can you demonstrate compliance with ISO 25999)?	YES
Comment	<p>Axon's last business continuity/disaster recovery test was conducted in March of 2020. The results were satisfactory and in-line with our Business Continuity objectives.</p> <p>For security reasons, we don't share the test results, however; we can share our Business Continuity Plan Overview. To do so, we will need the email addresses of the recipients to provide access.</p> <p>ISO 25999 (aka: BS 25999) was withdrawn in 2012 and 2013 following the publication of ISO 22301. However, Axon's Business Continuity Plan and supporting recovery plans are ISO 27001 certified, which includes business continuity management; and are subject to an independent audit at least annually as part of Axon's Trust and Compliance programme.</p>	
Q3.3	Do you provide monthly information security management reports?	No
Comment	<p>Any major changes or topics that require notification to our customers, are handled as needed, per our ISO certification and Security Management policies.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q3.4	Can you demonstrate compliance with legislation (e.g. privacy, breach notification) in all relevant jurisdictions?	YES
Comment	<p>Yes, Axon is committed to compliance with privacy legislation in all relevant jurisdictions as outlined in the following policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>Axon Notifications</p> <p>Axon Evidence employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks. Axon maintains security incident response procedures and capabilities for Axon Evidence including prompt reporting to appropriate parties. These include robust attack detection, incident response procedures, logging, and monitoring standards, and reporting to appropriate parties. Incident Management policies and procedures are part of the Axon ISO/IEC 27001:2013 certification.</p> <p>Specific security event and incident handling practices have been implemented to ensure appropriate detection, analysis, containment, eradication, and recovery in the event of an incident. Any incident response activities such as review, analysis, identification, and remediation of any Security Events would be investigated and executed by Axon.</p> <p>If an incident is determined or reasonably believed to have impacted the security of customer data, then the customer will be notified within an appropriate timeframe, typically within 48 hours of incident determination. The notification will reasonably explain known facts, actions that have been taken, and make commitments regarding subsequent updates.</p> <p>If Axon becomes aware that customer data has been accessed, disclosed, altered, or destroyed by an unlawful or unauthorised party, Axon will notify relevant authorities and affected customers. Additionally, Axon agrees to notify customers if there are changes to the threat environment or existing safeguards that would have a significant impact on the security, integrity, or confidentiality of data.</p>	
Q3.5	If non-public personal data is managed, can the provider control data transfers between countries in compliance with applicable regulations?	Yes
Comment		

Theme	Topic/Question	Answer (Y, N, N/A)
Q3.6	Is there a vulnerability program management?	YES
Comment	<p>Vulnerability scans are performed monthly. Additionally, Axon Evidence penetration tests are conducted frequently to validate the security of our systems and adjust as necessary.</p> <p>Penetration tests are performed by external, industry-leading security firms and include testing against the OWASP Top 10. These tests are supplemented by monthly vulnerability scans conducted by our internal Information Security team. All discovered issues are managed and tracked through completion by the Axon Information Security team.</p> <p>As previously mentioned, Axon hires independent firms to perform security and penetration testing of Axon Products and is willing to work with customers on any customer-initiated testing activities as long as they conform to Axon's Penetration Testing & Vulnerability Disclosure Guideline, which can be reviewed here: axon.com/penetration-testing--vulnerability-disclosure.</p>	
Q3.7	Are there regular vulnerabilities scans?	YES
Comment	These scans are performed monthly, as detailed above.	
Q3.8	Do you review your third parties for compliance with your security policies?	YES
Comment	<p>Any third parties who are leveraged for these services are reviewed annually, according to our security management policies. Additionally, these services are performed by reputable, industry-leading security firms.</p> <p>Additionally, Axon performs an initial review of third-party contractor security practises to evaluate if they meet Axon's security and compliance expectations. Contracts with third-party providers must be reviewed and approved by the Axon Legal Department and include security and compliance expectations.</p>	
4. Governance		
Q4.1	Has an Information security governance framework been established, maintained and monitored?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy. Our teams are committed to compliance with security, privacy, and legislation in all relevant jurisdictions as outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy 	

Theme	Topic/Question	Answer (Y, N, N/A)
	<ul style="list-style-type: none"> Other certain information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA. 	
Q4.2	Do your information security staff hold professional qualification (e.g. CISSP, GIAC CISA and CISM)?	YES
Comment	<p>Axon's security staff hold the following qualifications:</p> <ul style="list-style-type: none"> CISSP GSEC CISA 	
Q4.3	Is education / training given to provide staff with an awareness of information security?	YES
Comment	All Axon employees are required to take the annual and role-specific security training implemented by our Information Security team. Additionally, our employees must complete security training upon being hired.	
Q4.4	Are there clearly defined security roles and responsibilities and hierarchy?	YES
Comment	<p>Axon employs a full-time Information Security Team, which has an established hierarchy and clear definition of roles and responsibilities.</p> <p>These items are clearly defined within Axon's Master Services and Purchasing Agreement (MSPA) and the Axon Evidence Terms of Use so that our customers are fully aware of these defined roles and expectations.</p>	
Q4.5	Is a rigorous information risk analysis undertaken consistently for each critical information system?	YES
Comment	<p>The Axon Evidence service undergoes numerous auditing processes. The overall objective of these activities is to ensure the Information Security Programme is effectively designed and executed to ensure security related risks and postures are appropriately managed, customer data is maintained securely, and customer security and compliance expectations are met.</p> <p>Please find our complete list of security standards and compliances by visiting https://www.axon.com/trust/compliance.</p> <p>Furthermore, Axon Evidence is suitable for supporting OFFICIAL and OFFICIAL SENSITIVE data. The Axon Evidence service is accredited to store, forward and process information, which is at Business Impact Level (BIL) 2 for Confidentiality, BIL 2 for Integrity and BIL 4 for Availability (2, 2, 4).</p> <p>The accreditation includes an annual IT Security Health Check (ITHC) performed by a CESG-approved CHECK security team. Additional information on compliance can be found on Axon's website https://uk.axon.com/security</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q4.6	Is a consistent identity and access management approach implemented that restricts access to information and systems to authorised individuals?	YES
Comment	<p>Information access via Axon Evidence is controlled through role-based access controls, managed by the system administrator, and features comprehensive audit trails. This administrator is the starting point for defining security settings, creating roles and associated permissions, adding users, creating evidentiary categories and associated retention periods, etc.</p> <p>Access to information stored on Axon Evidence is governed according to:</p> <ul style="list-style-type: none"> • Pre-defined roles • Pre-defined individuals • User account-specific passwords <p>Axon Evidence also includes the following security features:</p> <ul style="list-style-type: none"> • Customizable password length and complex password requirements • Customizable failed login limit and lockout duration • Enforced session timeout settings during idle periods • Mandatory challenge questions when authenticating from new locations • Multi-factor authentication options for user login and prior to administrative actions (one-time code via SMS text or phone call-back) • Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) • Detailed, tamper-proof administrator and user activity logging • Hosted, SAML and Active Directory • Access Control Lists (ACLs) that specify which agency networks can access the agency 	
5. E-Discovery / Forensics		
Q5.1	<p>Have you implemented eDiscovery or forensic capabilities and process? Preservation can require that large volumes of data be retained for extended periods. What happens if the preservation requirements outlast the terms of the SLA / contracts? Do you allow your client effectively download the data in a forensically sound manner so it can preserve it off-line or near-line?</p>	YES
Comment	Axon's contracts are constructed to ensure that you retain all ownership of your data. All digital evidence stored on Axon Evidence is owned by IFI.	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>Therefore, if the contract comes to an end, Axon will not delete any customer content during the 90 days following contract termination. A customer will not incur any additional fees if a customer downloads customer content from Axon Cloud Services during this 90-day period. Axon has no obligation to maintain or provide any customer content after the 90-day period and will thereafter, unless legally prohibited, delete all customer content stored in Axon Cloud Services. Upon written request, Axon will provide written proof that all customer content has been successfully deleted and removed from Axon Cloud Services.</p> <p><u>POST-TERMINATION ASSISTANCE</u></p> <p>Axon will provide customers with the same post-termination data retrieval assistance that is generally made available to all customers. Requests for additional assistance to a customer in downloading or transferring content will result in additional fees and Axon cannot warrant or guarantee data integrity or readability in the external systems.</p>	
Q5.2	Have you implemented mechanisms to ensure that only relevant information is retained for e-Discovery, and that not all the data in the cloud or in the application is retained?	YES
Comment	<p>Axon is only a data processor of IFI content and data. All digital evidence stored on Axon Evidence is owned and managed by IFI.</p> <p>Therefore, any data retention schedules and policies within the solution is managed my IFI Administrators. The IFI will define how long you want evidence data retained within the system prior to deletion. Multiple retention schedules can be maintained, based on evidence type and IFI retention policies.</p>	
Q5.3	Do you segregate log data applicable for each client and provide it to each respective client for analysis without exposing log data from other clients?	YES
	<p>Log data is separated by customer tenancy – IFI will have access to only IFI logs and data, and vice versa for other customers. Each customer will only have access to their own data and logs.</p> <p>The IFI will have access to the Axon Evidence system, which enables self-access to these items (e.g. logs, reports, and audit information). All customer tenant logs including access logs, user sessions, and data history, can be retrieved by IFI administrators.</p> <p>The following link provides a copy of the Administrator Reference Guide, which details how this data can be extracted by IFI: http://public.evidence.com/help/pdfs/latest/EVIDENCE.com+Administrator+Reference+Guide.pdf</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
6. Security policies		
Q6.1	Have you formalised an Information Security Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy. Our teams are committed to compliance with security, privacy, and legislation in all relevant jurisdictions as outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	
Q6.2	Have you formalised a Data Classifications and Handling Guidelines?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	
Q6.3	Have you formalised a Logical Access Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q6.4	Have you formalised a Password Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p> <p><u>Axon Evidence Password Policy</u></p> <p>The password configuration page in Axon Evidence allows administrators to define password settings for all users in the agency.</p> <p>The password configuration page allows administrators to define password settings for all users in the agency.</p> <ul style="list-style-type: none"> ▶ PASSWORD HISTORY – Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25] ▶ PASSWORD AGING – Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365] ▶ PASSWORD LENGTH – Determines how short passwords can be. [default 8, min 6] ▶ FAILED LOGIN LIMIT – Number of failed login attempts before the account is locked out. [default 5, min 1, max 25] ▶ LOCKOUT DURATION – Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720] ▶ SESSION TIMEOUT – Number of minutes a user can be inactive before the user is automatically signed out of Axon Evidence. [default 15, min 15, max 480] <p>Axon Evidence also includes the following features to provide robust access control.</p> <ul style="list-style-type: none"> ▶ Enforced session timeout settings during idle periods ▶ Mandatory challenge questions when authenticating from new locations ▶ Multi-factor authentication options for user login and prior to administrative actions (one-time code via SMS or phone call-back) ▶ Role-based permission management 	

Theme	Topic/Question	Answer (Y, N, N/A)
	<ul style="list-style-type: none"> ▶ Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) ▶ Restrict access to defined IP ranges (limit access to approved office locations) ▶ Detailed, tamper-proof administrator and user activity logging 	
Q6.5	Have you formalised a User Account Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	
Q6.6	Have you formalised a Security Patching Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	
Q6.7	Have you formalised a Backup Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.	
Q6.8	Have you formalised a Data Retention Policy?	No
Comment	<p>Axon is only a data processor of IFI content and data. All digital evidence stored on Axon Evidence is owned and managed by IFI.</p> <p>Therefore, any data retention schedules and policies within the solution is managed my IFI Administrators. The IFI will define how long you want evidence data retained within the system prior to deletion. Multiple retention schedules can be maintained, based on evidence type and IFI retention policies.</p>	
Q6.9	Have you formalised an Audit Logging Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p>	
Q6.10	Have you formalised an Anti-Virus, Malware and Content Filtering Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p> <p><u>CYBER ESSENTIALS</u> Axon has gained Cyber Essentials certification which validates implementation of controls in alignment with the UK government-backed</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>Cyber Essentials Scheme. The Cyber Essentials requirements assist organisations in mitigating risk from common internet-based threats. Cyber Essentials concentrates on five key controls.</p> <ul style="list-style-type: none"> • Boundary firewalls and internet gateways • Secure configuration • Access control • Malware protection, and • Patch management <p>You can find a copy of this certificate on the Privacy link above.</p>	
Q6.11	Have you formalised an Encryption Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p> <p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p> <p><u>Data Encryption</u> Data is protected by strong encryption on the Axon Evidence platform.</p> <ul style="list-style-type: none"> • Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256-bit ciphers, TLS 1.2, Perfect Forward Secrecy • Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) 	
Q6.12	Have you formalised a Network Security Policy?	YES
Comment	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <p>Axon Security: https://uk.axon.com/security Axon Privacy: https://uk.axon.com/privacy Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>All other information outside of what is publicly shared in the links above, can be further discussed in a meeting upon a signed NDA.</p> <p><u>Network Security</u></p> <p>Axon Evidence has a dedicated Information Security team solely focused on keeping our digital evidence management solution secure and uncompromised. Our team remains vigilant in ensuring formal security practises are implemented and regularly assessed for continued effectiveness. These practises include but are not limited to access management, configuration management, vulnerability management, and security monitoring & response.</p> <p><u>Protective Measures</u></p> <ul style="list-style-type: none"> ▶ DATA IN TRANSIT – Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256-bit ciphers, TLS 1.2, Perfect Forward Secrecy. ▶ DATA AT REST – Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256). ▶ ACCESS – Axon Evidence supports Dual-Factor Authentication, IP Restrictions, and robust approval workflow when attempting to delete evidence data. ▶ DATA INTEGRITY – Evidence data is hashed (SHA) to ensure a robust chain of custody. Original evidence data is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access. Evidence deletion is protected with an approval workflow and includes a 7-day remorse/recovery period. ▶ DATA AVAILABILITY – Axon Evidence is designed for maximum availability with redundant data centres and frequent encrypted evidence backups. Multiple data centres are used that meet international standards (e.g. ISO 27001). 	
Q6.13	Have you formalised a Secure Disposal & Destruction of Data and Services Policy?	YES
Comment	<p>Axon's data destruction techniques comply with industry standards and our ISO Certifications.</p> <p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy 	

Theme	Topic/Question	Answer (Y, N, N/A)
Q6.14	Have you formalised an Incident Response Policy?	YES
Comment	<p>Axon's incident response policy complies with industry standards and our ISO Certifications.</p> <p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy <p><u>Monitoring of Security Events</u></p> <p>Axon deploys a dedicated Security Operations Centre (SOC) to actively monitor the security of Axon Evidence and respond to any identified events. The SOC team monitors logs that are routed to and analysed by a centralised Security Information and Event Management (SIEM) tool. Alerts and escalation trees are established for activities that would indicate suspicious or malicious activity. Nodes throughout the Axon Evidence infrastructure, including all computers that store or process information, send applicable logs to the SIEM.</p> <p><u>Computer Incident Response Team (CRIT)</u></p> <p>Axon's dedicated Security Operations Centre (SOC) is responsible for providing Computer Incident Response Team (CRIT) services. In case of an incident, they will require contact with a liaison from IFI's team to deliver these services.</p>	
Q6.15	Have you formalised a Change Control Policy?	YES
Comment	<p>Axon's change control policy complies with industry standards and our security certifications.</p> <p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy 	
Q6.16	Have you formalised a Risk Management Policy?	YES
Comment	<p>Axon's risk management policy complies with industry standards and our security certifications.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy 	
Q6.17	Have you formalised a Business Continuity Policy and a consistent Disaster Recovery Plan?	YES
Comment	<p>Axon’s Business Continuity/Disaster Recovery Plan (BCDR) complies with industry standards and our security certifications.</p> <p>Axon maintains a rigid and comprehensive Security Policy, which includes this topic. Various details are outlined in the following public security policies and statements:</p> <ul style="list-style-type: none"> • Axon Security: https://uk.axon.com/security • Axon Privacy: https://uk.axon.com/privacy • Cloud Service Privacy : https://uk.axon.com/legal/cloud-services-privacy-policy <p><u>Business Continuity Results</u></p> <p>Axon’s last business continuity/disaster recovery test was conducted in March of 2020. The results were satisfactory and in-line with our Business Continuity objectives.</p> <p>For security reasons, we don’t share the test results, however; we can share our Business Continuity Plan Overview. To do so, we will need the email addresses of the recipients to provide access.</p> <p>Axon’s Business Continuity Plan and supporting recovery plans are ISO 27001 certified and are subject to an independent audit at least annually as part of Axon’s Trust and Compliance programme.</p>	
7. Data centre		
Q7.1	Are there strong Physical Security Controls to protect the Data centre?	YES
Comment	<p>Axon’s Infrastructure-as-a-Service (IaaS) Provider designs, builds, and operates datacentres in a way that strictly controls physical access to the areas where your data is stored. The IaaS Provider understands the importance of protecting your data and is committed to helping secure the data centres that contain your data. The IaaS Provider have an entire division devoted to designing, building, and operating the physical facilities</p>	

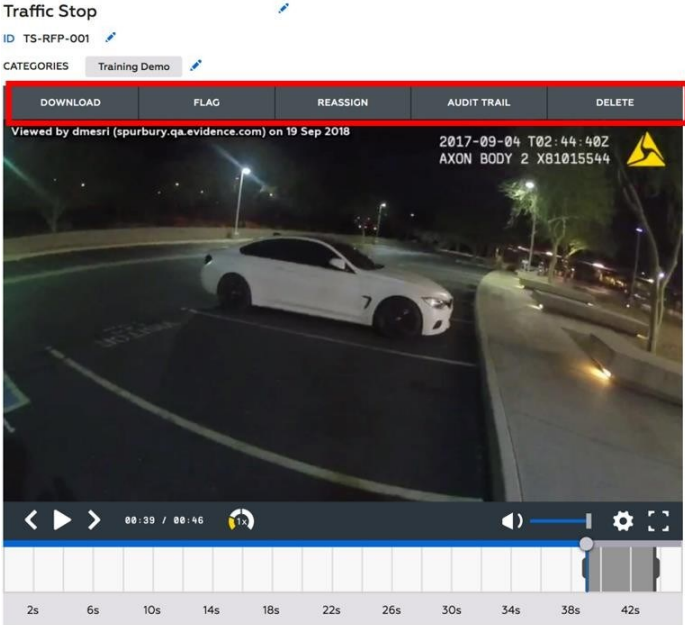
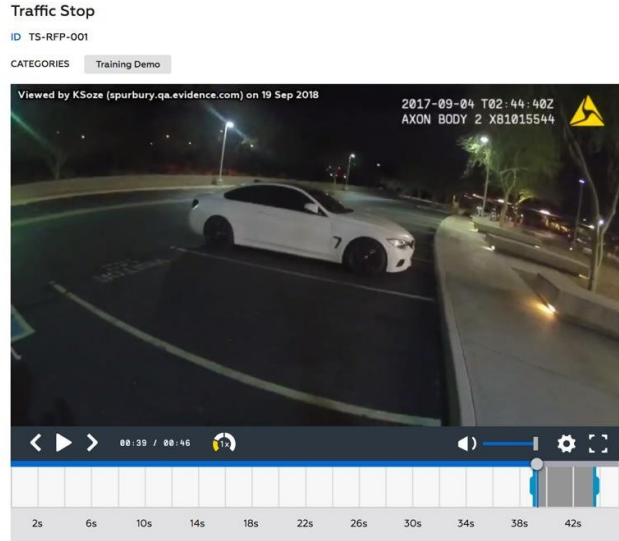
Theme	Topic/Question	Answer (Y, N, N/A)
	<p>supporting the cloud infrastructure. This team is invested in maintaining state-of-the-art physical security.</p> <p>The IaaS Provider takes a layered approach to physical security, to reduce the risk of unauthorised users gaining physical access to data and the data centre resources. Data centres managed by the IaaS Provider have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data centre floor. Layers of physical security are:</p> <ul style="list-style-type: none"> ▶ Access request and approval. You must request access prior to arriving at the data centre. You're required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by the IaaS Provider employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the data centres to the bare minimum. After the IaaS Provider grants permission, an individual only has access to the discrete area of the data centre required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire. ▶ Facility's perimeter. When you arrive at a data centre, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the data centres, with a security team monitoring their videos at all times. ▶ Building entrance. The data centre entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the data centre and monitor the videos of cameras inside the data centre at all times. ▶ Inside the building. After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the data centre. If your identity is validated, you can enter only the portion of the data centre that you have approved access to. You can stay there only for the duration of the time approved. ▶ Data centre floor. You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorised data entering or leaving the data centre without our knowledge, only approved devices can make their way into the data centre floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the data centre floor, you again must pass through full body metal detection screening. To leave the data centre, you're required to pass through an additional security scan. 	

Theme	Topic/Question	Answer (Y, N, N/A)
Q7.2	Are there redundant power supplies entering and throughout the Data Centre?	YES
Comment	Data centres are equipped with environmental controls such as fire detection and suppression systems, air conditioning and humidity monitoring systems, uninterruptible power supply (UPS) units, and generators.	
Q7.3	Are there Generator Backup and UPS Capabilities from the Data Centre to the Solution? Are there procedures for testing of generator backup, frequency etc.?	YES
Comment	See comments to Q 7.1 and 7.2	
Q7.4	Are there Environment Monitoring systems? (e.g. Early Moisture Detection and Alerting)	YES
Comment	See comments to Q 7.1 and 7.2	
Q7.5	Are there Air Cooling Systems, Capacity and Redundancy in case of failure?	YES
Comment	See comments to Q 7.1 and 7.2	
Q7.6	Is there multiple Demarcation Point to the Data Centre (including power and network connectivity)?	YES
Comment	See comments to Q 7.1 and 7.2	
8. Architecture		
Q8.1	Are there Host & Network Based Intrusion Detection/Protection Systems?	YES
Comment	<p>Axon Evidence uses intrusion detection and prevention solutions and restrictive networking rules to as part of a holistic approach to securing the application. Axon Evidence employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.</p> <p>Axon maintains a robust information security programme designed to provide a high level of protection against current and emerging threats. This includes logging all access to evidence data and systems, and robust audit reports within Axon Evidence. The Axon Evidence infrastructure utilises a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACLs. Axon Evidence utilises host-based firewalls on all applicable systems. Host based IDS and AV are deployed on applicable systems.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
Q8.2	Are dedicated servers used to store customer's information? Otherwise, how is the segregation performed?	YES
Comment	Axon Evidence utilises a multi-tenant architecture. Every customer will have their own isolated tenant and storage account. This improves security and also provides an environment where software upgrades and bug fixes will not impact any other tenants in the environment.	
Q8.3	What identity management architecture is supported – identity provider within cloud, external to the cloud (federated authentication)?	YES
Comment	<p>Axon customers can setup their tenant to require a username, password, and multi-factor authentication (MFA) code.</p> <p>For SSO, all SAML 2.0 services are supported with Axon Evidence including ADFS, but some less-common services may require client-side configurations.</p>	
Q8.4	Does provider support standard based assertion protocols such as OAuth and SAML?	YES
Comment	<p>Axon Evidence supports SAML 2.0 for single sign-on and SCIM provisioning (System for Cross-domain Identity Management) of existing users and groups.</p> <p>For example, IFI can synchronise their Active Directory and automatically create, update, and inactivate user accounts and groups in their Axon Evidence platform.</p>	
9. Application security		
Q9.1	Are passwords stored on a one-way encryption method? (Passwords are not stored in clear text and they can't be decrypted)	YES
Comment	The system does not display passwords during user entry; passwords in Axon Evidence are stored encrypted without a means to decrypt.	
Q9.2	Is it possible to enforce a password policy (renewal frequency, minimum length, dictionaries, banning guessable passwords, etc...)?	YES
Comment	<p>The password configuration page in Axon Evidence allows administrators to define password settings for all users in the agency.</p> <p>The password configuration page allows administrators to define password settings for all users in the agency.</p> <ul style="list-style-type: none"> ▶ PASSWORD HISTORY – Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25] 	

Theme	Topic/Question	Answer (Y, N, N/A)
	<ul style="list-style-type: none"> ▶ PASSWORD AGING – Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365] ▶ PASSWORD LENGTH – Determines how short passwords can be. [default 8, min 6] ▶ FAILED LOGIN LIMIT – Number of failed login attempts before the account is locked out. [default 5, min 1, max 25] ▶ LOCKOUT DURATION – Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720] ▶ SESSION TIMEOUT – Number of minutes a user can be inactive before the user is automatically signed out of Axon Evidence. [default 15, min 15, max 480] <p>Axon Evidence also includes the following features to provide robust access control.</p> <ul style="list-style-type: none"> ▶ Enforced session timeout settings during idle periods ▶ Mandatory challenge questions when authenticating from new locations ▶ Multi-factor authentication options for user login and prior to administrative actions (one-time code via SMS or phone call-back) ▶ Role-based permission management ▶ Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) ▶ Restrict access to defined IP ranges (limit access to approved office locations) ▶ Detailed, tamper-proof administrator and user activity logging 	
Q9.3	Are the passwords encrypted when transmitted to the application?	YES
Comment	Passwords in Axon Evidence are stored encrypted without a means to decrypt.	
Q9.4	Do you provide the ability to audit the credentials?	No
Comment	Axon Evidence does not contain credentials such as passwords.	
Q9.5	Do you provide alerts on every change in sensitive roles / credential?	No
Comment	Axon is a data processor of IFI content and data. All user management and permissions within the system is managed by IFI Administrators.	

Theme	Topic/Question	Answer (Y, N, N/A)
Q9.6	Is the application designed in a fail-secure manner? If a fault occurs on the system (or is generated on the system via missing parameters etc.), it should not give a higher level of access. Instead, the system should fail in a secure manner. An example of fail-safe would be to invalidate the session on errors (automatically logging the user out).	YES
Comment	Access is granted according to the principle of least privilege. Administrators can implement user access controls that adhere to this principle through customizable roles. The IFI is in complete control of user role configurations for Axon Evidence.	
Q9.7	Is the application designed using a secure-by-default principle? Where configuration options exist that vary in the level of security the most secure option should be the default and out-of-the-box configuration.	YES
Comment	<p>Axon Evidence is secured-by-default based on the principle of “least privilege.” This means, that options existing throughout the system are only available to users based on how the IFI Administrators setup access parameters.</p> <p>This means, that during deployment, IFI Administrators will define user roles and what those roles can and cannot access in the system. Then, when user accounts are created, they are assigned a role, therefore automatically restricting access to system features as that role allows (defined by IFI administrators).</p>	
Q9.8	Does the backend database users have minimum rights to the database? Specifically, they should be granted access to the specific tables with the specific create/read/update/delete privileges and no more. The DB user should not have schema-modification privileges, or command execution privileges unless required (e.g. SQL Server ‘sa’ user, Oracle DB ‘sysadm’ user etc should not be used).	YES
Comment	Axon Evidence is delivered as Software as a Service; therefore, neither Database Administrator (DBA) rights nor System Administrator Rights (SA) rights are required as the application is accessed via the internet, not installed locally.	
Q9.9	Are administrative interfaces private and segregated from user interfaces? Administrative logins and/or interface should be kept private and not available to the Internet or public audience (even if authentication is required) or at least deploy multifactor authentication.	YES
Comment	Axon Evidence provides functionality based on a user’s permissions (e.g., view, edit, download, delete, redact, share).	

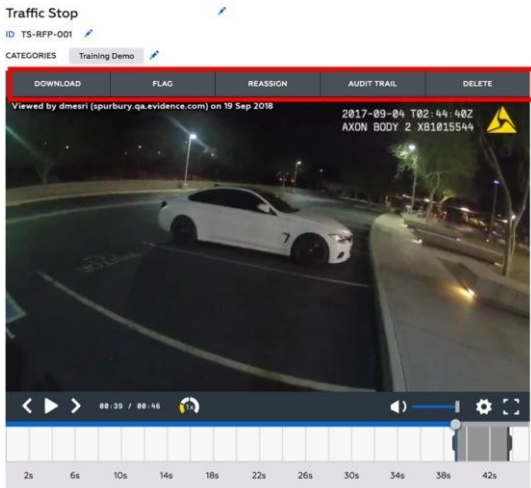
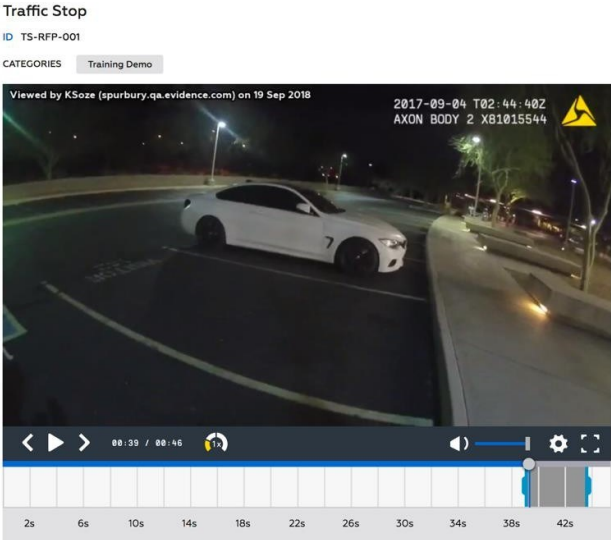
Theme	Topic/Question	Answer (Y, N, N/A)
	<p>As part of this, not only will the user only have the functions available to them, the user interface will also automatically adapt. For example, if a user has the permission to download, they will see the “Download” button on the video player, if a user does not have this permission, they will not see the “Download” button (as shown in Figure 1 & 2 below).</p> <p>This greatly simplifies the user experience and improves overall understanding. A user with all permissions enabled will see the options highlighted above from the view evidence screen</p>  <p>A user with permission to view only enabled will not have access to the functionality shown above from the view evidence screen</p> 	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>All permissions within Axon Evidence are based upon granular Role Based Access Controls (RBAC) that give IFI the ability to control what abilities a given role (or user) has such as viewing, editing, sharing, or downloading:</p> <ul style="list-style-type: none"> ▶ Any Evidence ▶ Only their own Evidence ▶ Prohibited (No Evidence) <div data-bbox="373 546 1316 667" style="border: 1px solid black; height: 50px; width: 100%;"></div>	
Q9.10	Are Verbose/Debug of error not presented to the user? (may be stored in server side logs). If an application error occurs, a generic error should be displayed to the end user. Are error messages and pages customisable?	No
Comment	Since Axon Evidence is a fully managed application, the Axon Engineering teams will monitor these aspects and handle internally. Any error message that occur are not visible to customers since the Axon team fully monitors the application 24/7. Furthermore, these logs are reported to the Axon Engineering team for handling – this is a benefit that our customers receive from the Axon service.	
Q9.11	If the application saves or works on files on the local file system, is the path and file details stored and generated inside the application? Specifically, the supplied filenames, paths or partial filenames should not be taken from supplied user input.	N/A
Comment	This is not applicable to the services or products supplied by Axon to IFI.	
Q9.12	Are HTTP POSTS used for delivering of user input instead of HTTP GET?	YES
Comment		
Q9.13	Is it possible to trace activity on the system through the use of an audit trail?	
Comment	Detailed audit logs track all evidence access and activity. Each audit trail entry shows the date, time, user, and details of each action. You can view the entire audit log or a portion of an audit trail, limiting the report to actions that occurred between a specified timeframe. Audit Trails are available in PDF format, except the User Audit Trail and Device Audit Trail, which are available in both PDF and comma-separated values (CSV) format.	

Theme	Topic/Question	Answer (Y, N, N/A)
	<ul style="list-style-type: none"> ▶ AGENCY AUDIT TRAIL – The Agency Audit Trail shows agency-wide changes to your Axon Evidence account. This report helps provide transparency on administrative actions across Axon Evidence. By displaying each action in detail, your agency can review who changed a setting, to understand the purpose and provide better accountability to each user. Only users with the “Edit Agency Settings permission” enabled can view the Agency Audit Trail. ▶ USER AUDIT TRAIL – A User Audit Trail shows many of the activities performed by the user, changes to the user account, and evidence-related user actions. In addition to evidence-related user actions, the User Audit Trail will show failed login attempts, when a user is locked out of their account due to multiple failed login attempts or when a user’s password has been reset or their account has been unlocked. ▶ CASE AUDIT LOG – The audit trail entry for Cases shared with a partner agency group use the same audit trail format as Evidence that is shared with a partner agency group. When a Case is shared with a partner agency group, the Activity column of the audit trail will show the group name and agency (instead of listing each member of the group). ▶ GROUP AUDIT TRAIL – The Group Audit Trail allows administrators to monitor the activity of groups within Axon Evidence and logs actions such as creating a group, adding or removing users from a group, changing permissions of a group, etc. ▶ EVIDENCE AUDIT TRAIL – Original evidence data is never changed; all modifications are handled by creating new, derivative files. Evidence Audit trails are created for every evidence file and list all related actions, as well as associated metadata. The original data associated with a video is never changed; all modifications are handled by creating new, derivative files. To ensure chain of custody, evidentiary files can be verified for authenticity by matching the SHA-2 hash of the original file ingested in Axon Evidence to that of any copy created. ▶ DEVICE AUDIT TRAIL – The Device Audit Trail shows events, actions, and changes for the selected camera. The audit information can be filtered to a particular date range or show the entire life of the camera. The Device Audit Trail can be used to audit actions performed on video while the file is still on the device (prior to upload). The audit information is available in both PDF and comma-separated values (CSV) format, with each event, action, or change shown on a different line in the audit trail. ▶ AXON RESPOND FOR DEVICES AUDIT TRAIL – The Axon Respond for Devices audit trail consolidates all Axon Respond for Devices information, such as which users accessed the Axon Respond for Devices map or a livestream, into a single audit trail. 	

Theme	Topic/Question	Answer (Y, N, N/A)
Q9.14	Is access to the source code of programmes, as well as to the design documents, specifications, testing schedule, etc., restricted to authorised personnel in order to prevent unauthorised changes?	YES
Comment	Only authorised individuals have access to our product source code of programmes, design documents, testing, etc.	
Q9.15	Have the application developers referred to the OWASP Top 10 and ensured their application does not contain exposures as detailed in the OWASP Top 10?	YES
Comment	Penetration tests are performed by external, industry-leading security firms and include testing against the OWASP Top 10. These tests are supplemented by monthly vulnerability scans conducted by our internal Information Security team. All discovered issues are managed and tracked through completion by the Axon Information Security team.	
Q9.16	Are all inputs centrally validated? This includes input provided in HTTP Headers, Cookies, URL query strings, and/or Form Inputs.	YES
Comment		
Q9.17	Are all input validation based on white-list validation? The allowed characters should be specified and all other received deny (default is to deny).	YES
Comment	Axon Evidence has security measures to protect against malicious inputs and injection attacks.	
Q9.18	Are users forced to authenticate before entering a private session? Specifically, it should not be possible to bypass this authentication stage. If a user tries to access a secure area without a login, they should be redirected to an appropriate page (e.g. login screen or error).	YES
Comment	<p>Access to the Axon Evidence platform is strictly governed by user login with their credentials. The password configuration page in Axon Evidence allows IFI administrators to define password settings for all users trying to access the system.</p> <p><u>Authentication and Authorisation</u></p> <p>Information access via Axon Evidence is controlled through role-based access controls, managed by the system administrator, and features comprehensive audit trails. This administrator is the starting point for defining security settings, creating roles and associated permissions, adding users, creating evidentiary categories and associated retention periods, etc.</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>Access to information stored on Axon Evidence is governed according to:</p> <ul style="list-style-type: none"> • Pre-defined roles • Pre-defined individuals • User account-specific passwords <p>Axon Evidence also includes the following security features:</p> <ul style="list-style-type: none"> • Customizable password length and complex password requirements • Customizable failed login limit and lockout duration • Enforced session timeout settings during idle periods • Mandatory challenge questions when authenticating from new locations • Multi-factor authentication options for user login and prior to administrative actions (one-time code via SMS text or phone call-back) • Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) • Restrict access to defined IP ranges (limit access to approved office locations) • Detailed, tamper-proof administrator and user activity logging • Hosted, SAML and Active Directory • Access Control Lists (ACLs) that specify which agency networks can access the agency 	
Q9.19	Are users restricted to the session for which they have logged in? Specifically it should not be possible for an intruder to break out from one user's session onto another for which a user is not authorized.	YES
Comment	Protective measures are put in place to restrict users to only accessing their session of the system. Axon Evidence provides configuration options for number of failed logins, password ageing, password history, and lockout duration to limit the effectiveness of brute-force attacks.	
Q9.20	Are users only able to view data and perform functions for which a user is authorized? Specifically it should not be possible (e.g. using parameter tampering or otherwise) for an intruder to view data belonging to another user/session or call upon a function for which they are not authorized.	YES
Comment	<p>As explained in Q9.9; Axon Evidence provides functionality based on a user's permissions (e.g., view, edit, download, delete, redact, share).</p> <p>As part of this, not only will the user only have the functions available to them, the user interface will also automatically adapt. For example, if a user</p>	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>has the permission to download, they will see the “Download” button on the video player, if a user does not have this permission, they will not see the “Download” button (as shown in Figure 1 & 2 below).</p> <p>This greatly simplifies the user experience and improves overall understanding. A user with all permissions enabled will see the options highlighted above from the view evidence screen</p>  <p>A user with permission to view only enabled will not have access to the functionality shown above from the view evidence screen</p>  <p>All permissions within Axon Evidence are based upon granular Role Based Access Controls (RBAC) that give IFI the ability to control what abilities a given role (or user) has such as viewing, editing, sharing, or downloading:</p> <ul style="list-style-type: none"> ▶ Any Evidence ▶ Only their own Evidence ▶ Prohibited (No Evidence) 	

Theme	Topic/Question	Answer (Y, N, N/A)
	<p>Download <input checked="" type="radio"/> ANY EVIDENCE <input type="radio"/> ONLY THEIR OWN <input type="radio"/> PROHIBITED</p> <p>Allows a user to download Evidence. Requires: Evidence View</p>	
Q9.21	Are session IDs stored in Cookie or Hidden Input delivered via POST Method?	YES
Comment	Session cookies are used.	
Q9.22	Apart from the Session ID itself, are all session data stored server side in the session object. Specifically, hidden fields should not be used to store state information.	YES
Comment	All session data is stored server side; Axon does not store hidden fields.	
Q9.23	Are database IDs such as primary keys etc. presented to the Client? Where possible, instead of presenting direct database Ids to the client temporary indexes/arrays should be presented to the browser which is mapped to the actual database Ids	No
Comment	The Axon Evidence is supplied to our customers through a Software-as-a-Service (SaaS) deployment. This means, the security and management of keys and database IDs are managed by the Axon product, security, and engineering teams.	
Q9.24	Do served file systems contain the files required for running of the production site only? Specifically, there should be no backup, test, redundant code or unneeded functionalities on the production server. For example, production systems should not contain any old, obsolete files (e.g. index.html.bak etc).	YES
Comment	Yes, Development and test environments are located in a separate region from the production environment so as not to disrupt any customer live regions.	
Q9.25	Have all comments in code been removed?	N/A
Comment		

Theme	Topic/Question	Answer (Y, N, N/A)
Q9.26	If automated password-reset or self-registration is required, is there secure procedure which does not allow for automated username enumeration?	YES
Comment	Password reset is allowed by the Axon Evidence system; however, username enumeration does not happen. If a user wishes to reset their password, they must enter their email address that is registered to their user account in the system. The email or username are not suggested by the system.	
Q9.27	Are all calls to the database performed via Stored Procedures? Specifically, Dynamic or inline SQL should not be used in the application	YES
Comment	Yes, API calls are used to communicate with the databases. Axon Evidence is a cloud-based solution; therefore, databases such as Oracle and SQL do not pose any issues related to the application's operability.	
10. Confidentiality		
Q10.1	How your customers' data are separated from each other?	Yes
Comment	Axon Evidence utilises a multi-tenant architecture. Every customer will have their own isolated tenant and storage account. This improves security and also provides an environment where software upgrades and bug fixes will not impact any other tenants in the environment.	
Q10.2	Are databases located on dedicated hardware or dedicated virtual machines?	N/A
Comment		
Q10.3	Is data managed on database instances dedicated to each customer?	No
Comment	Data is not managed on dedicated instances to each customer. Axon Evidence utilises a multi-tenant architecture. Every customer will have their own isolated tenant and storage account. This improves security and also provides an environment where software upgrades and bug fixes will not impact any other tenants in the environment.	
Q10.4	Is data managed on shared databases?	Yes
Comment	Axon Evidence utilises a multi-tenant architecture. Every customer will have their own isolated tenant and storage account. This improves security and also provides an environment where software upgrades and bug fixes will not impact any other tenants in the environment.	
Q10.5	Is data at rest encrypted?	Yes
Comment	Data is protected by strong encryption on the Axon Evidence platform.	

Theme	Topic/Question	Answer (Y, N, N/A)
	<ul style="list-style-type: none"> • Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256-bit ciphers, TLS 1.2, Perfect Forward Secrecy • Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) 	
Q10.6	Is data in transit over networks encrypted (TLS...)? What versions of TLS do you currently support? Do you periodically review and remove old versions and weak cyphers?	Yes
Comment	<p>Data is protected by strong encryption on the Axon Evidence platform.</p> <ul style="list-style-type: none"> • Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256-bit ciphers, TLS 1.2, Perfect Forward Secrecy • Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) <p>The Axon Engineering team reviews and enforces the latest cipher suites and deprecates older versions as needed.</p>	
Q10.7	Does the provider support the encryption keys being stored on the customer's premises instead of the cloud?	No
Comment	All encryption keys are managed and stored by the Axon Security team.	
Q10.8	How are customer data separated in the transmission (VLANs, VRFs, MPLS...)?	YES
Comment	VLANs are used for segmenting customer traffic and requests in the environment.	
Q10.9	Are backup media encrypted?	YES
Comment	<p>All data is encrypted, including backup data. Data is protected by strong encryption on the Axon Evidence platform.</p> <ul style="list-style-type: none"> • Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256-bit ciphers, TLS 1.2, Perfect Forward Secrecy • Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) 	
Q10.10	Does the service provide DLP (Data Loss Protection) mechanism and if so what protocols are supported (web, email, sftp..?)	YES
Comment	Axon Evidence is designed to be a fault tolerant application with geo-redundant architecture. Multiple security tools including anti-malware software and WAFs (Web Application Firewalls) are used to mitigate unauthorised access and extraction of data.	

Theme	Topic/Question	Answer (Y, N, N/A)
Q10.11	How are the media managed to guarantee the full erasure of data? Do you provide a certificate of destruction on storage media?	YES
Comment	<p>During the contract period, IFI is responsible for data management and deletion of data from the system, as defined by your retention schedules and policies.</p> <p>Post-Contract Data Deletion During the 90-day period following end of contract term, Axon will only delete customer content if requested by the customer. After the 90-day period post-termination, unless legally prohibited, Axon will delete all customer data stored in Axon Evidence without further notice.</p> <p>Upon written request, Axon will provide written proof that all of the customer data has been successfully deleted and removed from the Axon Evidence Services.</p> <p>Details regarding this type of data deletion are outlined in Axon Evidence privacy level statement, accessible from: https://uk.axon.com/privacy</p>	
Q10.12	Do you conduct security background check on personnel as part of the hiring process and do all your employees and sub-contractors employees sign NDA (Non-disclosure agreement) as part of their contract?	YES
Comment	<p>At a minimum, all personnel are screened for qualification and must submit to and successfully pass a background check and drug screening as a condition of employment at Axon.</p> <p>All Axon employees with access to evidence data are bound to a duty of confidentiality and undergo an extensive background check process. In addition to annual and role-specific security training. Our employees must also complete security training upon being hired. We also institute a breach notification process to alert customers and relevant authorities of a breach without an undue delay</p>	
Q10.13	Do you provide a facility to allow the full digital download of backups? Such as facility should not impact service bandwidth restrictions (if any).	Yes
Comment	<p>Axon's contracts are constructed to ensure that you retain all ownership of your data. All digital evidence stored n Axon Evidence is owned by IFI. Axon is only a data processor of IFI content; and IFI controls and owns all right, title, and interest in and to IFI data and Axon obtains no rights to it.</p> <p>Therefore, the IFI can export a copy of its data at any time during the contract period. This can be accomplished in a number of ways, as detailed below:</p>	

IFI Data Protection Impact Assessment (DPIA)

for Body Worn Cameras (BWC)

Theme	Topic/Question	Answer (Y, N, N/A)
	<ol style="list-style-type: none"><li data-bbox="490 376 1525 483">1. Axon can provide IFI with API documentation to facilitate the task. The Partner API can be used to integrate IFI's Axon Evidence data with other systems, including download to an on-premise storage solution.<li data-bbox="490 504 1525 719">2. Axon Evidence provides the ability to manually download digital media evidence at any time and will be available at no cost to the IFI. This process can be facilitated in a number of ways including the bulk export feature. If IFI wishes to extract all data stored in the application, data is exported in the format it was recorded (MP4 for Axon captured assets).	

Signature Certificate



Envelope Ref:dafa427a4518af2129a7baee41f1747381e620e4

Author: Sarah Healy Creation Date: 10 May 2024, 11:46:43, IST Completion Date: 10 May 2024, 15:51:54, IST

Document Details:



Name: DPIA IFI Body Worn Cameras V1 May 2024- Esign copy
Type:
Document Ref: 65bd117467cafa110fd3dc3b6bc2a6dd8d681abf13b4ea5115b8ac9390d0Of43
Document Total Pages: 80

Document Signed By:

Name: barry fox
Email: barry.fox@fisheriesireland.ie
IP: 137.191.231.147
Location: DUBLIN, D (IE)
Date: 10 May 2024, 12:03:30, IST
Consent: eSignature Consent Accepted


Signer ID: NP0VTQYYEE...

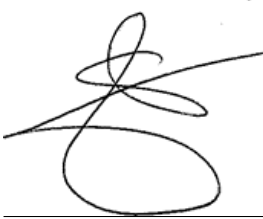
Security Level: Email
Name: Ian Carroll
Email: ian.carroll@fisheriesireland.ie
IP: 89.127.6.95
Location: TULLAMORE, OY (IE)
Date: 10 May 2024, 15:51:54, IST
Consent: eSignature Consent Accepted


Signer ID: ITR1HKOKVN...

Security Level: Email
Name: Sarah Healy
Email: sarah.healy@fisheriesireland.ie
IP: 137.191.231.147
Location: DUBLIN, D (IE)
Date: 10 May 2024, 12:00:39, IST
Consent: eSignature Consent Accepted


Signer ID: NVTBF1R99A...

Security Level: Email
Name: Sean Long


Signer ID: AQ03VLJD7P...

