Scottish Parliament Corporate Body

DATA PROTECTION IMPACT ASSESSMENT

Project Name:	Complaints procedure relating to compliance with the Scottish Biometrics Commissioner's Code of Practice under Section 15 of the Scottish Biometrics Commissioner Act 2020
Completed by:	Diego Quiroz, Operations Manager
Date:	February 2023
Review Frequency:	12 months. This as a live working document so that we can review it and update it as is necessary
Next Review Date:	February 2024

Revision history:

Version	Date	Amended By	Summary of Changes

OVERALL RISK ASSESSMENT (*TO BE COMPLETED BY THE DATA PROTECTION OFFICER*)

I have scored this as a 6 on the scale for severity and likelihood of risk. Whilst the processing as part of the complaint service will not involve the use of biometric data itself, the matter has an inherent sensitivity given the links to the processing of biometric data by the Police Service of Scotland, SPA and PIRC. As the processing is in response to a legal obligation – in terms of the Scottish Biometrics Commissioner Act 2020, this reduces the severity of the risk to 3. For the likelihood of risk, the processing of complaint related information is by a small number of staff who have carried out their GDPR online training and from an organisational approach personal data is stored on a secure eRDM system with strong security measures.

Robin Davidson – Data Protection Officer

	Severity of Risk					
Likelihood of risk	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**2**	**3**	**4**	**5**
2	**2**	**3**	**4**	**5**	**6**	**7**
3	**3**	**4**	**5**	**6**	**7**	**8**
4	**4**	**5**	**6**	**7**	**8**	**9**
5	**5**	**6**	**7**	**8**	**9**	**10**

PART G: DPIA DECLARATION

We confirm that the data protection impact of this project to the relevant data subjects has been minimised to the extent reasonably possible to ensure that the processing of their personal information will not be unwarranted or unfairly prejudice their interests and that it is reasonable and proportionate to take the remaining risks in all the circumstances. We confirm that the use of the personal information described in this DPIA for the purposes of this project is necessary and justified and that the use of this personal information as part of this project should comply with all applicable data protection laws as at the date of this DPIA.

Project Lead	**Office Holder**
Signed: Diego Quiroz	Signed: 
Name: Diego Quiroz	Name: Dr Brian Plastow
Date: 23 February 2023	Date: 23 February 2023 Updated: October 2023
Job title: Operations Manager, SBC.	Job title: Scottish Biometrics Commissioner

GLOSSARY

In this document, the following terms have the following meanings:

"anonymisation"	the process of turning personal information into a form which does not identify individuals and where identification is not likely to take place.
"controller"	the person or entity who determines the purposes and means by which personal information is processed.
"personal information"	information relating to/about identified or identifiable individual(s) (called 'data subjects').
"process"	any operations in relation to personal information throughout the information lifecycle, including obtaining, storing, using, accessing, disclosing, destroying, erasing or anonymising personal information.
"special category of personal information"	personal information revealing: • racial/ethnic origin; • political opinion; • religious/philosophical belief; • trade union membership;

	• genetic or biometric data; • health; or • sexual life/orientation.
"supervisory authority"	the relevant data protection supervisory authority. In the UK, this is the Information Commissioner's Office.

DATA PROTECTION IMPACT QUESTIONNAIRE

Data Protection Impact Assessment

To be completed by the Project Lead with input (as required) from the Data Protection Officer:

Address:
Scottish Biometrics Commissioner
Bridgeside House
99 McDonald Road
Edinburgh
EH7 4NS
Email: Contact@biometricscommissioner.scot
Tel: 0131 202 1043

PROJECT OVERVIEW

NO	QUESTION	RESPONSE	COMMENTS/NOTES
1	Explain the aims of the project, the anticipated benefits to the organisation, to individuals and to other parties.	▪ This is a complaints procedure established by Section 15 of the Scottish Biometrics Commissioner Act 2020. Therefore, the legal basis for processing data is for the purpose of complying with this statutory provision on our Act. ▪ This complaints procedure is a process whereby an individual can complain to the Scottish Biometrics Commissioner (SBC) about failures to comply with the SBC's Code of Practice. The Code of Practice regulates 'the acquisition, retention, use and destruction of biometric data for criminal justice and policing purposes in Scotland by the Police Service of Scotland (PSoS), the Scottish Police Authority (SPA), or the Police Investigations and Review Commissioner (PIRC). ▪ The procedure will provide an effective remedy to the public when the public bodies above do not comply with the SBC's Code of Practice. It will also encourage and enable best practice in the use of biometric data in the criminal justice system in Scotland.	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		▪ The SBC will only accept complaints from a data subject or their representative – the definition of which is 'someone whose biometric data is held by PSoS, Scottish Police Authority or Police Investigations and Review Commissioner. The SBC will absolutely not accept complaints that do not relate to a specific data subject. ▪ Personal information, which triggers the investigation under Section 15 of our Act, is provided on a voluntary basis by the complainer. ▪ The complaints procedure is available on the SBC website. It will receive publicity via print and social media. Hard copies will be available to any person who requests it.	
2	Describe the personal information affected in terms of data sets.	▪ The complaint will include: name, date of birth, address and contact information of the complainer or a representative acting on behalf of the complainer. ▪ Any personal information will be provided on a voluntary basis to the SBC	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		by the complainer to initiate the procedure. ▪ On receipt of a complaint, the Commissioner will appoint an investigating officer, who will firstly contact the complainer to ensure that we understand the exact nature of the complaint and have the necessary information upon which to proceed. ▪ If a person withdraws their complaint or does not wish to proceed, we reserve the right to conduct a full investigation if the specific nature of the allegation suggests that it is in the public interest to do so. ▪ A separate privacy notice and data sharing agreements are to be prepared for the complaints procedure. ▪ SBC will not handle biometric data.	
3	Are any of these data sets considered to be high risk? If so, why?	▪ The complaints process may receive criminal offence data of an individual by virtue of the fact that a complaint is being made that the relevant authorities have failed to comply with the SBC's code of practice. In those case we will	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		comply with Schedule 1 of the Data Protection Act 2018.	
4	Describe the proposed collection, use and deletion of personal information and identify the relevant data controllers and data processors involved. It may be useful to refer to a flow diagram or another way of explaining the data flows.	▪ On receipt of a complaint (about the alleged failure of any of the 3 public bodies holding personal biometric data to comply with the Scottish Biometrics Commissioner's Code of Practice) the SBC will adopt the following three-stage complaint handling process: **Stage 1** ▪ SBC will acknowledge receipt of a complaint within three working days. The complaint will include the name, address date of birth and contact information of the complainer. ▪ SBC will record the complaint and initial assessment. Where appropriate, we will seek to discuss the complaint with the complainer so that we have a full understanding of all relevant circumstances and are confident the complainant fully understands our privacy notice. The SBC will store the complaint and associated documents	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		within eRDM which has high security measures. ▪ If the complaint does not relate to our statutory area of responsibility, we will advise the complainer and end our involvement. We will ensure manual deletion of any personal information within 5 working days. ▪ SBC will allocate the complaint for investigation and will contact the public body the complainer highlights may be breaching the SBC's Code of Practice and seek any information we require to investigate the complaint. SBC will not reproduce or hold any biometric data and will have in place data sharing agreements with PS, SPA and PIRC to ensure any personal data shared is secured in line with the Data Protection Act 2018 and the Scottish Biometrics Commissioner Act 2020. ▪ Following SBC investigation, the findings will be presented by the investigating officer to the Commissioner who will produce a written determination on whether there has been a breach of the	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		SBC's Code of Practice. A copy of this written determination will be provided to the complainer and the public body involved, explaining the decision. ▪ If the Commissioner determines that there has been a breach of the Code of Practice, then in accordance with the provisions of Section 20(1) of the Scottish Biometrics Commissioners Act 2020 the Commissioner must prepare and publish a report about that failure unless the Commissioner considers that it is sufficiently minor not to merit it. Any such report will identify any organisational learning but will not disclose the personal identity or details of the complainer. In this case we will anonymise any personal data. ▪ If there has been a failure to comply with the Code, the Commissioner may issue a 'Compliance Notice'. If PS, PIRC or SPA fail or refuse to comply with a compliance notice, without reasonable excuse, that may be reported to the Court of Session (Sections 23 to 27 of Act).	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		▪ SBC will manually delete a complainer's personal data 26 months after the date of the SBC determination or last significant contact with the complainer e.g. Stage 3. A statutory right to appeal is not provided by the legislation. Retention periods differ across the personal data but details are included within the privacy notice which can be found on the SBC website. ▪ Within the SBC team, all members of staff (of which there are three staff and the Commissioner) will be data controllers with the ability and authority to process the data as required as part of the complaint process.	
5	Is the information obtained from the individual data subjects, themselves or from third party sources? Provide details.	▪ The information obtained is provided from the individual data subjects i.e. the complainer or through their representative on a voluntary basis via a complaint procedure established by Section 15 of the Scottish Biometrics Commissioner Act 2020. ▪ Personal data may be provided to SBC by PS, SPA and PIRC. Therefore, SBC will also have in place data sharing agreements	*This will impact on the information communicated to data subjects. Where the information is obtained from third parties due diligence should be undertaken to ensure processing is lawful and then can be disclosed by that third party and used lawfully and fairly by the Scottish Parliament.*

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		with PS, SPA and PIRC to ensure processing is both lawful and proper.	
6	Describe why it is necessary to process personal information for this project. Explain the purposes for which the personal information will be processed.	▪ Personal data is required in order to undertake the complaint, which our statutory duty under Section 15 of the Scottish Biometrics Commissioner Act 2020. ▪ The aim of the complaints procedure is to provide an independent mechanism to the public in cases of failure to comply with SBC's Code of Practice. ▪ Personal information is required to identify the complainer and enable an investigation into their particular complaint as per Q9 which describes the complaints procedure adopted by the SBC.	
7	On what legal basis will you rely to process the information? Have you consulted Solicitor's Office to confirm that this is the correct legal basis?	▪ Legal obligation. ▪ Section 15 of the Scottish Biometrics Commissioner Act 2020 - 'Complaints about failures to comply with the code: (1) The Commissioner must provide for a procedure by which an individual, or someone acting on an individual's behalf, may make a complaint to the	For further info see ICO Processing Conditions Guidelines.

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		Commissioner that a person who is required by section 9(1) to comply with the code of practice has not done or is not doing so in relation to the individual's biometric data.'	
8	If applicable, on what legal basis will you rely to process criminal offence data? Have you consulted Solicitor's Office to confirm that this is the correct legal basis?	▪ Processing of criminal offence data in terms of Article 10 of the UK GDPR and Paragraph 6(2)(a) of Part 2 of Schedule 1 to the Data Protection Act 2018.	For further info see ICO Processing Conditions Guidelines.
9	If you are relying on consent/explicit consent, do you have an appropriate procedure in place for: • Obtaining and recording in an auditable way that consent has been given?; • Stopping any processing based on that consent and, if necessary, deleting the personal data provided in the event that the data subject indicates that they are withdrawing consent?	▪ SBC legal basis for processing personal data is Section 15 of the Scottish Biometrics Commissioner Act 2020. ▪ If SBC decides not to proceed with an investigation, we will manually ensure deletion of the personal data provided within 5 working days. We reserve the right to conduct a full investigation if the specific nature of the allegation suggests that it is in the public interest to do so. ▪ The complainer is informed through the complaints procedure and privacy notice: ▪ that the SBC is the data controller for their personal data,	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		▪ how their personal data is processed, including sharing and retention, ▪ their individual rights requests.	
10	Do you believe that the Scottish Biometric Commissioner's current global privacy statement gives sufficient information to affected individuals about the processing that will be conducted?	▪ No, however, a separate privacy notice will be prepared to cover the complaints procedure and will be publicly available on the SBC website.	*Consider the language of the privacy statement, and whether it needs updated in light of the processing to be undertaken in this project, or whether a stand-alone privacy notice specific to this project is required (a link to which can be added to the global privacy statement).*
11	Which stakeholders, individual data subjects or representatives (such as trade unions) (if any) should be consulted, internally and externally? How will you carry out the consultation? This should be linked to the relevant stages of the project management process. Consultation can be used at any stage of the DPIA process.	▪ SBC will undertake the investigation and decision making independently. The Commissioner will produce a written determination on whether there has been a breach of the SBC's Code of Practice. ▪ SBC consulted widely on the project management process (the draft complaints procedure). The consultation included expert groups on the area of biometrics, criminal justice, and data protection. A public consultation was held in September 2022.	
12	Is it possible for individuals to restrict the purposes for which the	▪ If SBC receives a request for rectification, SBC will take reasonable steps to ensure	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
	organisation will process the personal information?	that the data is accurate and rectify the data if necessary. SBC will consider steps to restrict processing whilst clarification is obtained. This may include: making the personal data unavailable to users or temporarily removing published data from a website. ▪ Personal information will be used solely in connection with the investigation of a specific complaint or reporting obligation under our Act.	
13	Are decisions being made on the basis of the personal information that will be processed?	▪ Yes. The aim of the complaints procedure is to provide an independent mechanism to members of the public in cases of a failure to comply with the SBC's Code of Practice. Therefore, personal data is required to identify the complainer and initiate/enable an investigate into their circumstances subject to the complaint and individual.	
14	If the answer to 13 is yes, will these decisions have legal or significant effect on the individuals concerned?	▪ Under Section 23 of our Act, the Commissioner has the power to issue a Compliance Notice requiring PS, SPA or PIRC to take the steps as set out in the Notice to address their failure to comply with the Code of Practice. For example, a	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		Compliance Notice could recommend PS, SPA or PIRC to remove the complainer's personal data from any/all Scottish biometric databases.	
15	Is the processing by automated means?	▪ No, it will be manual. SBC has anticipated a low level of complaints at this point related to the Code of Practice.	*There are specific provisions that apply to automated processing. These should be considered if the answer to this question is yes.*
16	Are procedures in place to provide individuals access to personal information about themselves?	▪ Yes. SBC's complaints procedure informs the complainer about individual data requests. The complainer or their representative can make a Subject Access Request verbally or in writing. SBC will verify the identity of the complainer, if necessary. SBC will respond within one month of receipt of the request. Where the request is complex or voluminous the SBC can extend the period for responding to the request by a further 2 months. The complainer will receive a copy of the SAR to ensure accuracy.	*Consider the sufficiency of resources, IT and technology used in the project to ensure compliance with data protection obligations to allow data subject to access personal information about themselves.*
17	Can the personal information be corrected by the individuals, or can individuals ask for correction of the information?	▪ Yes. If SBC receives a request for rectification SBC will take reasonable steps to ensure that the data is accurate and rectify the data if necessary. This may include a restriction on the	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		processing of the personal data involved pending satisfaction as to the accuracy of the personal data. ▪ Personal information can be corrected by the complainer at any time. The complainer will receive a copy of the amended data to ensure accuracy of their personal data.	
18	Do you check the accuracy and completeness of personal information on entry?	▪ Yes. SBC has simplified the data entry process by creating a form. There are only a few options (name, date of birth and personal contact details) to limit potential errors and standardise the information. A folder will be created to store personal information related to complaints in eRDM. The complaint and the letter of acknowledgment will also be stored here. Any changes to be made will be completed via this system and updated automatically. ▪ SBC has assigned permission to the IMSO to change data. This will limit the changes of information being edited incorrectly. Furthermore, it is an offence if the Commissioner or Commissioners' staff disclose confidential information obtained during the exercise of the	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		office's functions under Section 19 of the Scottish Biometrics Commissioner 2020. ▪ SBC will proactively perform data audits on a regular basis to ensure improvement and compliance.	
19	How often will the personal information you process be updated?	▪ The personal information held by the SBC will only be updated if requested by the complainer. ▪ In the event the information provided to us during the complaint investigation is inaccurate we will contact PS, SPA or PIRC with a request for them to correct the inaccurate personal data. The decision, however, will lie with them.	
20	How severe would you deem the consequences, in case you process outdated personal information for the individuals it refers to?	N/A	
21	Which measures and/or procedures will be adopted as a safeguard or security measure to ensure the protection of personal information?	▪ SBC has simplified the data entry process by creating a form. ▪ Personal data in relation to the complainer will be stored in the eRDM system.	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		▪ We have assigned permission to the IMSO to edit personal data and delete personal data 26 months after the date of the SBC determination or last significant contact with the complainer e.g. Stage 3 of the complaint. However, all members of the SBC team have permission to edit and/or delete personal data as part of the complaints process. SBC will manually delete any personal data and proactively perform data audits on a regular basis to ensure improvement and compliance issues.	
22	Do you use pseudonymisation and/or anonymisation? If so, give details.	▪ SBC may report on the outcome of an investigation, for example to the Scottish Parliament, in compliance with the Scottish Biometrics Commissioner Act 2020. When we do so we will not name individuals or include any personal or identifiable information. We may use information we collect to compile statistics and undertake research and analysis. In these cases, personal information will be completely anonymised.	
23	If you will use encryption, are you responsible for encrypting and	N.A.	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
	decrypting the personal information that you process?		
24	Does your project, research or application involve processing personal data outside the EEA? Yes/No If no, please go to question 29.	No.	
25	Will you transfer, disclose or permit remote access to personal information to/from a country or territory outside of the EEA? If so, which ones? If no, please go to question 29.	No.	
26	Is the country or territory that is outside the EEA covered by an EU Commission adequacy decision? If so, please let us have details. If no, please go to question 27.	N.A.	
27	Are measures in place to ensure an adequate level of security when the personal information is transferred outside of the EEA? What are they?	N.A.	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
28	If the intention is to rely on standard contractual clauses (SCCs) or binding corporate rules (BCRs) to process personal data outwith the EEA, are you satisfied that local law in the destination country will not prevent or hinder the safeguards in the SCCs or BCRs from providing data subjects with effective legal remedies in relation to processing in that country? For example, is there any reason to believe that law enforcement or intelligence agencies may have rights that are contrary to the rights and remedies that data subjects have under GDRP?	N.A	
29	Please explain the steps that will be taken to ensure "privacy by design and default" as part of this project.	▪ The project since the inception has put data privacy of the complainer at the centre of the process. The complaints procedure has undergone a number of expert consultations through the lifecycle, including with the ICO and SPCB's DPO. ▪ The personal data has been standardised and simplified via a form. Withdrawal of	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		personal data or the complaint is considered. Section 15 can only be initiated by an individual submitting a compliant to SBC. However, if a person does not wish to proceed, we reserve the right to conduct a full investigation if the specific nature of the allegation suggests that it is in the public interest to do so. ▪ Through the eRDM system and business practice, personal data is secure and protected. The SBC will retain personal information only if necessary and under strict time limits (26 months). We will manually delete personal data. ▪ SBC's complaints procedure will be written in 'plain English language'. ▪ SBC has also updated their current complaints-related data protection polices in relation to this project to reflect 'privacy by design', run a DPIA and is putting in place three data sharing agreements with PS, PIRC and SPA to ensure compliance with data protection and privacy issues.	
30	What retention period(s) will be applied to the information?	▪ SBC will retain personal data on a complaint for 26 months after the date	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		of the SBC determination or last significant contact. A statutory right to appeal is not provided by the legislation. However, the SBC process considers the possibility to request the Commissioner for a clarification on the final decision. If not satisfied, the complainer can initiate a petition for judicial review. There is a 3-month time limit on seeking judicial review (Courts Reform (Scotland) Act 2014). Retention periods are stated on the complaints procedure and privacy notice (SBC website). ▪ When keeping information for the purposes of the Scottish Biometrics Commissioner Act 2020 (e.g. reporting to Parliament or for statistical purposes) we will anonymise the personal data. ▪ The personal information will be manually deleted. ▪ All personal data will be deleted after a period of 26 months has elapsed since the date of the last action on the complaints file. Thereafter, the complaints file will be anonymised and retained in accordance with the SBC's File Plan retention policy (destroyed 7	

NO	QUESTION	RESPONSE	COMMENTS/NOTES
		years from the date that the complaints folder is opened).	

PRIVACY AND RELATED RISKS

Identify the key privacy risks and the associated compliance and corporate risks. Additional columns may be required for additional risks in Parts B, C, D and E.

		Risk 1	Risk 2	Risk 3
31	Privacy issue	Data collected being used for anything other than the specified purpose.	Unauthorised processing of personal data by members of staff and/or third parties.	
32	Risk to individuals	Unlawful processing of personal data.	Personal data breach.	
33	Compliance risk	Failing to comply with data protection principles under UK GDPR.	Failing to comply with security principles in terms of the UK GDPR.	
34	Associated risk to the organisation	Reputational and possible action by the ICO as the regulatory body.	Potential for loss of rights and freedoms of the data subject (whose personal data has been accessed), reputational damage to the SBC and	

			loss of confidence in the organisation by service users/stakeholders. Fines and/or enforcement action by the ICO.	

RISK TREATMENT

Describe the privacy treatment options or controls[1] that could be taken to reduce the risks identified above and any future steps that would be necessary (e.g., the production of new guidance or future security testing for systems).

		Risk 1	Risk 2	Risk 3
35	Potential treatment options and/or controls	▪ Data to be used only for the specific, explicit and legitimate purpose, which is the complaints procedure which has been stated clearly within complaints procedure document. ▪ The information will be secured in the eRDM system. ▪ SBC will also set up data sharing agreements to ensure purpose specification.	▪ Small organisation with limited number of staff who have access to personal data (only 3 members of staff). ▪ All members of the SBC team have permission to change data as required, authorised and appropriate as part of the complaints process. ▪ All staff required to complete mandatory data protection	

1 Controls could include, for example, anonymisation, pseudonymisation, data minimisation, reducing the extent and purposes of processing, period of storage, accessibility or technical and organisational information security measures, such as those identified in ISO 27001.

		Risk 1	Risk 2	Risk 3
		▪ When keeping information for the purposes of the Scottish Biometrics Commissioner Act 2020 (e.g. reporting to Parliament or for statistical purposes) we will anonymise the personal data. ▪ SBC will raise awareness on both the complaints procedure and Code of Practice once they are published. ▪ SBC will strengthen training of staff regarding purpose specification and data protection, including subject access request rights. ▪ All members of the SBC team have permission to change data as required, authorised and appropriate as part of the complaints process. ▪ SBC will manually delete personal data on a complaint 26 months after the date of	training annually, including what to do when a breach occurs. ▪ Disclosure of personal data by staff working for the SBC is a criminal offence. ▪ SBC will strengthen training of staff regarding subject access request rights. ▪ SBC will proactively perform data audits on regular basis to ensure improvement and compliance issues to minimise errors or unauthorised modifications to the personal data. ▪ Personal data retained on secure systems. ▪ The information will be secured in our eRDM system.	

		Risk 1	Risk 2	Risk 3
		the SBC determination or last significant contact. ▪ Include a specific paragraph within the complaints procedure related to the complainer's right to request and correct personal information. ▪ SBC will proactively perform data audits on regular basis to ensure improvement and compliance issues to minimise errors or unauthorised modifications to the personal data ▪ SBC will cross-check information received from an individual with the relevant organisation who may also have the individual personal data. ▪ Personal information can be corrected or withdrawn by the complainer at any time. The complainer will receive copy		

		Risk 1	Risk 2	Risk 3
		of the complaint to ensure accuracy and information. ▪ When the complaint is withdrawn SBC will manually secure deletion of the personal data provided within 5 working days. However, if a person withdraws their complaint or does not wish to proceed, we reserve the right to conduct a full investigation if the specific nature of the allegation suggests that it is in the public interest to do so.		
36	Result: Is the risk eliminated, reduced, or accepted if the treatment(s)/control(s) is/are implemented?	Risk sufficiently mitigated.	Risk sufficiently mitigated.	Risk sufficiently mitigated.
37	Evaluation: Is the final (i.e. residual) impact on individuals after implementing this treatment/control a justified, compliant and proportionate	The overall risk is low due to the nature and purpose of the data needed to resolve a complaint. There is no specific indication of likely high risk, but we will review this regularly.	The overall risk is low due to the steps taken. There is no specific indication of likely high risk, but we will review this regularly.	The overall risk is low due to the steps taken. We will only share information to resolve a complaint according to the purpose specification of this project.

		Risk 1	Risk 2	Risk 3
	response to the aims of the project?			
38	Should this treatment/control be implemented? (If not, indicate the reason.)	N/A	N/A	N/A
39	Decision taken by			