Project Name	Central Logging of Intelligence Operations (CLIO)	Version	V. 1

Table of Contents

1. Introduction 2
2. Document metadata 2
3. Date for review of Data Protection Impact Assessment (DPIA) 2
4. Description of the project 3
5. Personal Data to be processed 3
6. Authority to process and control personal data of FBOs 3
7. Authority to process and control personal data of AO's and Data Subjects 5
8. UK GDPR Principles 5
9. Justification for processing and controlling personal data 7
10. Principle, General and other FSS statutory duties and powers 8
11. How will the Personal Data be processed 13
12. How is the CLIO Data protected 14
13. Who has access to the CLIO Data? 14
14. How will data be disposed of? 14
15. Management and accuracy of the data 15
16. Sharing of data 15
17. Changes to data handling procedures 15
18. Statutory exemptions/protection 15
19. Stakeholder Consultation 16
20. Risks identification and incorporation of privacy risks into planning 16

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the use of FSS Incidents Case Management System known as Central Logging of Intelligence Operations (CLIO) in the recording, investigating, monitoring and management of Food Incidents.

2. Document metadata

2.1	Name of Project	**CLIO**
2.2	Author of report	**Christina Anthony**
2.3	Date of report	**24/03/2021**
2.4	Name of Information Asset Owner (IAO) of relevant business unit	**Ron McNaughton**
2.5	Data Protection Officer	**Garry Mournian** 
2.6	Date of DPO approval of this report	**29/03/2021**

3. Date for review of Data Protection Impact Assessment (DPIA)

3.1	Unless otherwise provided for at 3.2, a full privacy impact review will take place annually.
3.2	FSS will carry out a privacy impact review as soon as practicable if one or more of the following occurs:
	• A notifiable data protection breach takes place; • There is a change in data protection law; • The DPIA requires updating; or • Any circumstance in the opinion of FSS allows for a review.
3.3	A privacy impact review must be documented and must in the least record:
	• The date of the review; • The details of the review; • The start and completion dates of the review; • The name of the official carrying out the review; • Findings and recommendations; • Date the review is approved by FSS Data Protection Officer (DPO).

4. Description of the project

4.1	Description of the work:
	Background CLIO (Central Logging of Intelligence Operations) is a software database provided by Badger Software Ltd and utilised by Food Standards Scotland for management of incidents and logging of food crime intel. CLIO spans two servers, which are hosted in a "Demilitarised Zone" (DMZ) part of the SCOTS network. This means the servers reside on Scottish Government infrastructure, but are accessible from outside SCOTS, via the internet. The CLIO servers are segregated from the SCOTS network to ensure that data does not flow between the two. The two CLIO servers (one hosting the (SQL) database used by CLIO and one hosting the webpage through which CLIO is accessed externally) require SCOTS administrator credentials to access. CLIO user accounts are needed to log onto CLIO. The servers are regularly updated and patched, and administrator accounts expire after 120 days.

5. Personal Data to be processed

Personal data	**Data source**
Food business or trading name	FSS, Local Authority
Food business trading name if different from name	FSS, Local Authority
Food business operator (FBO)/owner name and surname	Local Authority
Food business address	Local Authority
Food business operator or premises email address	Local Authority
Environmental Health Officer (EHO) name and surname	Local Authority

6. Authority to process and control personal data of FBOs

From 1 January 2021, any references to EU Regulations should be read as meaning retained EU law which can be accessed via the EU Exit Web Archive. Retained EU law should be read alongside any EU Exit legislation which was made to ensure that retained EU law operates correctly and is published on legislation.gov.uk.

Statute	**Provision**	**Competent Authority**
Regulation (EU) 2017/625	Article 8 and 11 Confidentiality obligations of the competent authorities and Transparency of Official Controls	FSS
	Article 10 Operators, processes and activities subject to official controls	FSS/ Local Authorities
The Official Feed and Food Controls (Scotland) Regulations 2009	Regulation 4 - Exchanging and Providing Information	FSS
	Regulation 8 - Power to request information relating to enforcement action	FSS
Food (Scotland) Act 2015	Section 26 - Power to request information in relation to enforcement action	FSS
UK General Data Protection Regulation and Data Protection Act 2018.	Article 6(1)(e) (UK GDPR) and Section 8 (DPA 2018) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	FSS/ Local Authorities
Data Protection Act 2018	Section 31 - The Law Enforcement Purposes. Sharing of information necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	FSS/ Local Authorities

7. Authority to process and control personal data of AO's and Data Subjects

Statute	Provision	Competent Authority
UK General Data Protection Regulation and Data Protection Act 2018.	Article 6(1)(e) (UK GDPR) and Section 8 (DPA 2018) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	FSS/ Local Authorities
Data Protection Act 2018	Section 31 - The Law Enforcement Purposes. Sharing of information necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	FSS/ Local Authorities

8. UK GDPR Principles

Principle	Compliant	Description
Article 5(1)(a) - lawfulness, fairness and transparency	Yes	See *9. Justification for processing and controlling personal data*
Article 5(1)(b) – purpose limitation	Yes	There will be no further distribution or use of the personal data beyond the requirement for Incidents monitoring, prevention and control or audit purposes as required by legislation and regulation and outlined in section 6 of this DPIA.
Article 5(1)(c) – data minimisation	Yes	The CLIO system will not collect any new personal information from Local Authority and other Law enforcement partners that is not required for the

		management of Food Incidents
Article 5(1)(d) – accuracy	Yes	Data is collected from all local authorities in Scotland and stored on the CLIO system. All Local Authorities have access to CLIO. It is the responsibility of the Local Authority service delivery partner, as required by Food Law and the Food Law Code of Practice (Scotland), to ensure the accuracy of data entered into the CLIO by their authorised officers.
Article 5(1)(e) - storage limitation	Yes	The data is stored on CLIO hosted on a secure Scottish Government Network. Backup on all SCOTS systems takes place in accordance with the Terms of Supply for the Provision of ICT Services (September 2018).
Article 5(1)(f) - integrity and confidentiality'	Yes	All data in CLIO is accessible via individual user accounts which require authentication. CLIO maintains its own users. The login password is stored in CLIO and does not use authentication via Enterprise log ins. The logins do have permissions which allow for restricted access to relevant data. We are exploring supported Single Sign On using standards like SAML. Access to data is only granted to FSS personnel and authorised officers of approved service delivery

		partners who need access to the information to perform FSS functions.
Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	Yes	FSS objectives include protecting public health from the risks that may be caused by food. This includes risks resulting from the way food is produced or supplied or consumed. To do this, a system of "Official Controls" is in place. Official Controls are delivered as defined within Regulation (EU) 2017/625 , as are the checks such as inspections, surveillance and sampling, that are carried out to monitor if businesses are complying with the requirements set out in law. The majority of the checking and monitoring activity will be conducted by service delivery partners under delegation from the Competent Authority (FSS)

9. Justification for processing and controlling personal data

9.1	<u>FSS Official functions</u> • Food Standards Scotland (FSS) was established Food (Scotland) Act 2015 (the 2015 Act) and came into being on 1 April 2015. It has three statutory objectives, namely: a) to protect the public from risks to health which may arise in connection with the consumption of food; b) to improve the extent to which members of the public have diets which are conducive to good health; and c) to protect the other interests of consumers in relation to food. • FSS has the power to request information relating to enforcement action. • FSS and Local Authorities are permitted to exchange amongst themselves any information received by them in the execution and enforcement of relevant food and feed law.
9.2	<u>What the personal data allows FSS to do</u>

	The data sharing is necessary for the purpose(s) of Law Enforcement purposes defined under Part 3 of the Data Protection Act 2018 to accomplish the following: • Incident management; • The prevention and detection of crime; • The apprehension and prosecution of offenders; • To prevent, protect, prepare and pursue, Serious Organised Crime Groups who impact on the communities of Scotland; • To increase public safety; and • To establish an effective communication structure between FSS and Local Authorities
9.3	<u>What FSS will not be able to do without this data</u> Not having access to real time and up to date data will not allow FSS to: • Respond in a timeous manner to a food incident; • Identify/predict potential incidents before they occur; • Identify links between FBOs and food incidents located in different locations across Scotland; • Identify linked food Incidents through information sharing with other competent and authorised agencies (such as FSA); • Utilise data and information to better formulate food and feed control policies; • Properly advise the Scottish Ministers on matters relating to food and feed hygiene and safety; • Keep the public adequately informed about matters which significantly affect their capacity to make informed decisions about food and feed matters; • Reduce administrative burden on Local Authorities (or other service delivery partners) through effective and accessible monitoring of performance in the promotion of best practice. The availability of the data in consistent format and real (or near to real) time will enhance monitoring and audit practices and minimise regional variation in the delivery of Official Controls.

10. Principle, General and other FSS statutory duties and powers

Statute	Provision	Competent Authority
Regulation (EU) 2017/625	Article 4 – Designation of Competent Authorities	FSS
	Article 6 – Audits of Competent Authorities	FSS
	Article 8 and 11 Confidentiality obligations	FSS

	of the competent authorities and Transparency of Official Controls	
	Article 10 Operators, processes and activities subject to official controls	FSS/ Local Authorities
	Article 113 Annual Reports	FSS
The Official Feed and Food Controls (Scotland) Regulations 2009	Regulation 7 – Monitoring of Enforcement Action	FSS
	Regulation 8 – Power to request information relating to enforcement action	FSS
	Regulation 11 – Offences relating to regulations 8 and 9	FSS
Food (Scotland) Act 2015	Section 2 – Duty to protect the public from risks to health which may arise in connection with the consumption of food and protect the interests of consumers in relation to food and diet.	FSS
Food (Scotland) Act 2015	Section 3 (1) (a) – Duty to develop (and assist Scottish Ministers and public bodies and office holders) policies in relation to food matters and animal feeding stuffs matters.	FSS
	Section 3 (1) (b) Duty to advise, inform and assist the Scottish Ministers and public bodies and office holders in relation to food matters and animal feeding stuffs matters	FSS

	Section 3 (1) (c) Duty to keep the public adequately informed about and advised in relation to matters which significantly affect their capacity to make informed decisions about food matters.	FSS
	Section 3 (1) (d) Duty to keep users of animal feeding stuffs adequately informed about and advised in relation to matters which significantly affect their capacity to make informed decisions about animal feeding stuffs matters.	FSS
	Section 3 (1) (e) Duty to monitor the performance of, and promote best practice by, enforcement authorities in enforcing legislation.	FSS
Food (Scotland) Act 2015	Section 16. Power to do anything which it considers necessary or expedient for the purposes of, or in connection with, its functions.	FSS
	Section 19 – Duty to acquire, compile and keep under review relevant information.	FSS
	Section 20 – Observations with a view to obtaining information.	FSS
	Section 21 – Powers for persons carrying out observations.	FSS

	Section 23 – Setting performance standards.	FSS
	Section 25 – Reporting on enforcement action by others.	FSS
	Section 27 – Offences in relation to section 26.	FSS
Regulatory Reform (Scotland) Act 2014	Section 5 – details the provisions for the Scottish Regulators' Strategic Code of Practice.	FSS
Scottish Regulators' Strategic Code of Practice	**Risk and Evidence** Principle 5. Regulators should consider risk at every stage of their policy planning and decision making processes to help ensure that action is targeted where it is most needed. In support of this, regulators should also take an evidence-based approach, taking informed decisions on where and how to focus effort. This should include measuring the effectiveness of interventions in achieving measurable outcomes. The emphasis, where possible, should be on preventing problems from occurring in the first place or from escalating significantly.	FSS
	Clear and Effective Communication Principle 13. Regulators should also publish details of their approach	FSS

Scottish Regulators' Strategic Code of Practice	to checks on compliance, including inspections. The aim should be to clearly set out what businesses and regulated bodies should be able to expect as well as what businesses should do to optimize the process and indeed the outcomes. These details should, as appropriate, cover any circumstances in which inspections or visits will or will not be announced in advance, and an assurance that feedback, ideally written, will be provided together with an explanation of appeal procedures. They should also set out what can be expected during an inspection or visit, including showing identification, explaining the purpose of the visit and how it will be carried out. They should also provide the business with information about their role in terms of, for example, any necessary access to information, individuals or premises, as appropriate. Understanding those they regulate and tailoring approaches accordingly.	
Scottish Regulators' Strategic Code of Practice	Principle 9. Regulators should also share information about compliance and risk, following the principle of collect once, use often when requesting information from business and others.	FSS/ Local Authorities
	Principle 10. Data	FSS/ Local Authorities

	Protection legislation rightly constrains the way organisations use information, but in the limited circumstance where the law allows, regulators with common interests or activities should agree secure mechanisms for sharing information. This benefits both the regulated and the regulators, helping target resources, activities and minimise duplication.	
UK General Data Protection Regulation and Data Protection Act 2018.	Article 6 (1) (e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	FSS/Local Authorities
Data Protection Act 2018	Section 8 - processing is necessary for the exercise of official authority and public interest	FSS/Local Authorities
Data Protection Act 2018	Section 31 - The Law Enforcement Purposes. Sharing of information necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	FSS/Local Authorities

11. How will the Personal Data be processed

Personal data collected, processed or shared within CLIO is only done where there is a lawful basis under Article 6 of the UK GDPR and Section 31 of DPA 2018 for doing so.

FSS has robust internal processes necessary to ensure that staff are suitably qualified and trained in terms of the processing of personal identifiable information on CLIO

All computers accessing CLIO will be on a protected network. All computers will be password protected

12. How is the CLIO Data protected

CLIO spans two servers, which are hosted in a "Demilitarized Zone" (DMZ) part of the SCOTS network. This means the servers reside on Scottish Government infrastructure, but are accessible from outside SCOTS, via the internet. The CLIO servers are segregated from the SCOTS network to ensure that data does not flow between the two.

The two CLIO servers (one hosting the (SQL) database used by CLIO and one hosting the webpage through which CLIO is accessed externally) require SCOTS administrator credentials to access. CLIO user accounts are needed to log onto the CLIO website.

The servers are regularly updated and patched, and administrator accounts expire after 120 days.

CLIO meets the requirements of the Scottish Government Cloud Assurance Scheme and On-Premise Assurance Scheme.

The risk of loss or corruption of data on CLIO is low.

13. Who has access to the CLIO Data?

Access to the CLIO portal will be via unique username and password, using a role based authentication model. Within FSS, access to CLIO is controlled and limited to two FSS system administrators who have the ability to grant access to FSS personnel, provided there is business justification to do so.

CLIO is only accessible to registered, trained users. Within the system, only those with a requirement to access an operation through their role will be granted access to the information i.e. an LA will only be able to access data relevant to them. FSS undertake regular security audits on the system to ensure the controlled access set up is secure.

The risk of unauthorised use or access to data held on CLIO is low.

14. How will data be disposed of?

Local Authorities and FSS have well-established processes for the safe storage and appropriate disposal of data compliant with data protection legislation and the Public Records (Scotland) Act 2011.

The Information held on CLIO will be retained as follows:

- Serious resolved cases – retain for current year + 12 years from the date made known to the FSS.
- Standard Cases (resolved & unresolved) – retain for current year + 6 years from the date made known to FSS.

15. Management and accuracy of the data

The data on CLIO will be owned and managed by FSS as the Data Controller. FSS and Local Authorities and key service delivery partners (Public Health Scotland, SRUC and APHA) will be responsible for ensuring the accuracy of data collected and entered into CLIO.

16. Sharing of data

Part or parts of data may be shared within Scottish Government and UK Government and its agencies as well as EU Commission as permitted within the remit of the law.

17. Changes to data handling procedures

There will be no new or changed data collection policies or practices that may be unclear or intrusive or inconsistent with the FSS CLIO system

There will be no changes to data quality assurance or processes and standards that may be unclear or unsatisfactory.

There will be no new or changed data security access or disclosure arrangements that may be unclear or extensive.

There will be no new or changed data retention arrangements that may be unclear or extensive.

There will be no changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before.

18. Statutory exemptions/protection

FSS is not aware of any exemptions from the Data Protection Act which would apply to this project.

19. Stakeholder Consultation

A formal public consultation was carried out as detailed below :		
Presentation to board	FSS Board Seminar	November 2016
Internal training of all FSS staff	Training by Badger Software	March 2017
Training and roll out to SRUC	Training and presentation by SFCIU	August 2018
Training and roll out to APHA	Training and presentation by SFCIU	January 2019
Training and roll out to PHS	Training and presentation by SFCIU	January 2019
Training and roll out to LAs	Training and presentation by SFCIU	March 2019

20. Risks identification and incorporation of privacy risks into planning

Risk	Ref	Result
Personal data is inadvertently collected, processed and stored by Local Authorities and FSS on CLIO as part of their respective functions as a competent authority		Acceptable. Data sharing requirements and protocols to be discussed and agreed prior to implementation, including reference to legal advice if/where required.

DPIA History

Completed by

Date	Author	Summary of Changes
24/03/2021	Christina Anthony	Drafted and Sent for Approval

Approvals

Name	Title	Date	Version
Ron McNaughton	Head of SFCIU and IAO	29/03/2021	1.0
Garry Mournian	FSS DPO	29/03/2021	1.0

Distributions

Name	Title	Date of Issue	Version