Data Protection Impact Assessment

This plan is used to identify and define the work required to carry out a Data Protection Impact Assessment during a project, or a change to an existing system or service. The requirement to complete this plan is identified earlier from the DPIA screening document. Along with the plan, the Data Protection Impact Assessment Log contains specific aspect, risk, response, solution, approval and delivery details to complete the DPIA cycle. Read the Privacy Overview to find out more.

Please note that the EU General Data Protection Regulation (GDPR) come into effect 25th May 2018, updating the Data Protection Act 1998. The 3 main pillars of the GDPR are: Transparency, Accountability and Enhanced data subjects rights. This plan will be updated following any new advice from ICO.

Project / Service Name	**Stakeholder Management System (SMS)**	**Version**	Draft/Final

Contents

1 Confirm the need for a DPIA

Explain what the project or service aims to achieve, what the benefits will be to the organisation, to individual and to other parties. Link to the outline business case, project brief or benefits

The current stakeholder information across Food Standards Scotland (FSS) is patchy, unreliable and mostly held in Microsoft excel spreadsheets across branches. The incongruent stakeholders information have not been kept up to date over many years and not fit for purpose.

Recently, FSS embarked on an exercise to cleanse and consolidate the disparate stakeholder lists across the organisation into a single corporate stakeholder list to ensure that FSS can fulfil its obligation under the GDPR and Data Protection Act (DPA) 2018. The next logical step after the consolidation exercise is to establish a system/solution that provides a better management of the corporate stakeholder contact details and to further automate the often manual or inconsistent external communication and engagement processes in the organisation.

The new solution is required to efficiently manage stakeholder contact details, and all communication with external stakeholders. It is envisage that the solution will integrate with other line of business solutions like Outlook to maximise data sharing, monitoring and reporting.

2 Privacy Impact Screening

Summarise the PIA need from the Privacy Screening Assessment carried out earlier.

The Privacy screening assessment identified the collection and processing of stakeholders' personal contact details that will include: Title, Full Name, Email Addresses.

Telephone/mobile contact numbers, and Postal addresses are optional contact information that stakeholders may choose to provide.

The purpose for processing stakeholder contact details is in the performance of our statutory duties in the public interest to ensure that information and advice on food safety and standards, nutrition and labelling is independent, consistent, evidence-based and consumer-focused.

Stakeholders' special category or sensitive data will not be collected or processed on the system.

3 Who the information will be shared with

Will personal identifiable information about individuals be disclosed to organisations/people that have not previously had routine access to it? Provide details

SMS will only be used by FSS internal staff and contractors working on behalf of FSS to fulfil our statutorily duties as outlined in Food Standards (Scotland) Act 2015.

No personal identifiable information will be disclosed to other organisations or individuals.

Where and if required, a data sharing agreement will be drafted and agreed with any 3rd party organisation or data processor to access or process the data. A privacy notice will be developed to cover the terms of the sharing of the data.

4 Information flows

Describe the collection, use and deletion of personal data. State how many individuals will be affected by the new service/product, and in what capacity (e.g. stakeholder, citizens, staff processing data etc.) Flow chart/diagram, or other business process mapping approaches, can be provided as supporting material but always complete summary information in the table below.

Capacity/role affected	Number of individuals
FSS Staff	Initial 50 with varying levels of access.
Stakeholders	Can only access and update their own personal contact details and preferences.
System developers	2- 3, to develop the system and upload the contact details from Excel spreadsheet to the online solution

4.1 Data Collection

Data will be uploaded from the Official Stakeholder List on eRDM. New data to be provided to FSS select staff to upload to the system or by Stakeholders themselves. It is proposed that an online portal be made available for Stakeholders to use to: add new information about themselves, update their contact details, provide/update their preferences and interests, and if necessary and in accordance with data protection laws, exercise their rights for their personal details to be deleted from the system.

4.2 Data Storage and Access

Data to be stored on a secured ISO27001 compliant cloud system or Microsoft Azure on a UK server. There must be a robust backup regime to automatically take backups for disaster recovery. Backup files to be retained for an agreed number of days.

Any cloud identity and access management solution should integrate completely or be compatible with this, allowing internal users to authenticate against their central details. It is envisaged that cloud identity and access management solution will also maintain user permissions and active status.

The system should be able to allow multiple internal and external stakeholders to maintain complete operational independence on the Stakeholder Management System. External stakeholders will only be permitted access relating to their data. FSS Administrators should be able to selectively access or deny access to any data on the system by our own reports and staff where there is a requirement for data confidentiality and integrity purposes.

4.3 Data Processing

The data will be used primarily to fulfil the statutory obligations required by FSS under the Food Standards (Scotland) Act 2015 Section 19, which places a requirement on FSS to perform its other functions effectively and to operate in accordance with section 4. Food Standards Scotland is to acquire, compile and keep under review information about food matters and animal feeding stuffs matters. FSS will collect and use stakeholder details (Names, addresses, job titles, and email addresses, telephone numbers)to discharge its statutory duties in the public interest.

The processing of the data is necessary to communicate and engage with our stakeholders. The processing must be proportionate and must meet the public interest /legal obligation test (GDPR Article 6(1)(c) and (e)), and/or satisfies one of the conditions of Schedule 9 of DPA 2018 whereby the processing or disclosure of any information must outweigh any considerations of confidentiality attaching to it.

4.4 Data Retention and Disposal

Stakeholders will have access to their contact details and request for their data to be deleted from the system. A 2 yearly audit of all contacts on the SMS will be carried to ensure the accuracy of the contact details and that we are not keeping any stakeholder details on the system longer than necessary. Any stakeholder that has not been contacted or engaged with in 3 years, will be deleted from the system.

5 General Data Protection Regulation - Principles checklist

Answering these questions during the DPIA process will help identify where there is a risk that the project's deliverables will fail to comply with GDPR or other relevant legislation.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

5.1 Principle 1 – Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

a. Have you identified the purpose of the project/service?

The purpose of the project is described above in Section 1 and 4.3

b. How will individuals be told about the use of their personal data?

A privacy notice will be uploaded on the SMS with a link to FSS Privacy Policy on FSS website.

Exciting stakeholders were issued with privacy notices in line with GDPR requirements. Any further addition to the database will receive a privacy notice automatically sent to the stakeholder during registration.

c. ***Do you need to amend FSS's standard privacy notice****?*

Yes, a customised privacy notice is being drafted to be uploaded to the FSS Website. FSS Privacy notice guidance will guide the drafting of the privacy notice.

d. Have you established which conditions for processing apply – ICO Lawful Basis for Processing

Processing of Stakeholder contact details falls under:

- Article 6 (1) (a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- Article 6 (1) (c) – processing is necessary for compliance with a legal obligation to which FSS as controller is subject;
- Articles 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;
- Relevant conditions for the processing of law enforcement data under the conditions of Schedule 9 of DPA 2018

e. If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Where consent is required, consent must be explicitly given before the stakeholder's details is added to SMS. If the consent is withdrawn, the contact detail will be automatically removed from the system immediately.

f. FSS is subject to the Human Rights Act, you need to consider:

- *Will your actions interfere with the right to privacy under article 8?*
- *Have you identified the social need and aims of the project?*
- *Are your actions a proportionate response to the social need?*

Processing of Stakeholder data is in compliance with the Huma Rights Act (HRA) 1998 Article 8 requirement to respect an individual's private and family life, home and correspondence. There will be no interference with this right except in accordance with the law, and for the protection of public health.

5.2 Principle 2 – Purpose Limitation

> Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

a. Does your project plan cover all of the required purposes for processing personal data?

Yes it does.

b. Have potential new purposes been identified as the scope of the project expands?

No. If new purposes are identified by FSS, further consultation with stakeholders and a review of this DPIA will be undertaken.

5.3 Principle 3 – Data Minimisation

> Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

a. Is the information you are collecting/using adequate, relevant and limited to the purposes it is collected/ used for?

Yes

b. Which personal data could you not use, without compromising the needs of the project?

None identified

5.4 Principle 4 - Accuracy

> Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

a. If you are procuring new software does it allow you to amend data when necessary?

Yes it will on the instructions of stakeholders or by stakeholders using the self-service online portal.

b. How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Stakeholders will be given access to and control of their personal data and a 2 year audit of all information will be undertaken to ensure the accuracy of the information and that we are not keeping any personal data longer than necessary.

5.5 Principle 5 - Storage Limitation

> Personal data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

a. What retention periods are suitable for the personal data you will be processing?

Stakeholders will have access to their contact details and request for their data to be deleted from the system. A 2 yearly audit of all contacts on the SMS will be carried to ensure the accuracy of the contact details and that we are not keeping any stakeholder details on the system longer than necessary. Any stakeholder that has not been contacted or engaged with in 3 years, will be deleted from the system.

b. Are you procuring software which will allow you to delete information in line with relevant FSS retention periods?

The SMS will have an in-built function to securely delete information no longer required.

5.6 Principle 6 – Integrity and Confidentiality

> Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

a. Do any new systems provide protection against the security risks you have identified?

Yes. Protection of Stakeholder data is detailed in section 4 above particularly 4.2 and 4.3

b. If the project involves marketing or where consent is sought, have you got a procedure for individuals to opt out of their information being used for that purpose?

Stakeholders can exercise their rights to unsubscribe from receiving specific or all communication from FSS. The function will be embedded in the system.

c. What training and instructions are necessary to ensure that staff know how to operate a new system securely?

At an absolute minimum, we require the following from solution developers:

- Full project documentation, including database and entity relationship diagrams;
- Full training manual, bespoke to the project configuration;
- Full training manual, bespoke for the end user (not IT staff to include videos where required);
- Full on-site training at our Aberdeen office for multiple end users;
- Full on-site training at our Aberdeen office for a 'train the trainer' session;
- Full on-site technical overview, training and handover for our IT team;
- Detailed functional and technical specifications detailing the configuration of the project deliverables.

6 Privacy stakeholder consultation requirements

Explain what practical steps will be taken to ensure that you identify and address privacy issues.

Who will be consulted	**Internal (I) External (E)**	**How will the consultation be carried out?**	**When during what stages in the project will this be carried out?**
Data Protection Officer/Team	I	Review and approval of DPIA, privacy screen, privacy impact log and business case	Business case stage, commencement of project and where a privacy risk or concern is identified
Procurement partner and FSS Finance manager	I & E	Review of business case and completing specification document, tendering and award of contract	September to November 2018
Solution Developers	E	During project progress update/review	Monthly project progress meeting
Select FSS Staff and Stakeholders	I & E	During User Acceptance Testing (UAT) of solution	Late February 2019
SG Legal Team	E	Email and telephone meeting	Advice on privacy related issue that may result into a legal case when identified in course of the delivery of the project

Advice

The guidance in this action plan will be refreshed following further guidance from the UK Information Commissioner's Office

- This template can be used by staff to prepare the privacy impact assessment plan for any project or service which they are planning to introduce. This should be completed after a PIA screening identified the need for it.
- The project manager / information asset owner will lead the completion of the information, with support from the project/service team
- The source of the questions is the GDPR guidance from the UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
- Please change word "project" to "service" where the assessment is not a project to carry out the change, but is a service/product that the project will deliver.
- **Privacy Impact Assessments are a mandatory requirement of the General Data Protection Regulations (GDPR) from May 2018**

Further advice on the GDPR is available from the Data Protection Team or at the ICO's GDPR Page

Quality criteria

- Do not change the advice, numbering or any of the sub-questions in this layout. It is designed to ensure that the assessment is carried out fully and consistently.
- Complete at the project initiation stage. If some details are not known, it must be identified when they are expected to be known, and tasks factored into the plan of work ahead with expected dates.
- Retain the assessment as part of the formal outputs of the project
- This is the Plan - the Privacy Impact Register must also be completed.

Revision History [completed by

Date	Author	Summary of Changes
11/09/2018	Tigan Daspan	Draft for approval

Approvals

Name	Title	Date of Issue	Version
Garry Mournian	DPO and Head Corporate Services		

Distributions

Name	Title	Date of Issue	Version

Template v.1.0 privacyimp-plan.docx