

## General Data Protection Regulation (GDPR) – FSS Compliance Update

### 1 Purpose of the paper

- 1.1 The purpose of this paper is to update the Board on GDPR compliance progress across all FSS business areas in preparation for the enforcement of the new data protection law from 25<sup>th</sup> May 2018.
- 1.2 The Board is asked to:
- **Note and comment** on FSS GDPR compliance progress in relation to the UK Information Commissioner's Office recommendation; and
  - **Discuss and provide a view** on the recommendations for the ways by which FSS can continue to earn the trust and confidence of our stakeholders in the appropriate use of their personal data in line with the new data protection law.

### 2 Strategic Aims

- 2.1 This work supports FSS Strategic Outcome: 5 – FSS is a trusted organisation, 6 – FSS is efficient and effective.

### 3 Background

- 3.1 The General Data Protection Regulation was first floated around seven years ago and has seen many variations during the negotiating process between European member states. The final version was published in April 2016, and will become enforceable from 25 May 2018. The GDPR mandates that FSS demonstrates effective accountability arrangements towards the protection of all personal identifiable information within the organisation, including technical and organisational measures to fulfil the enhanced rights of data subjects. The GDPR fundamentally changes the enforcement regime meaning higher fines and a more significant risks. The risk is not just financial (up to 4% of global turnover or 20 million Euros) – the reputational damage can be long lasting leading to a very real risk to the existence of businesses and jobs from the financial impacts and reputational damage.
- 3.2 The UK Data Protection Bill 2017 - 2019 will become law when enacted as the Data Protection Act. The Bill is currently at the House of Commons: Report Stage. It will explicitly bring provisions of the GDPR into UK law and establish continuity of the GDPR in the UK post Brexit. The Act will legislate in areas where the GDPR allows flexibility at national level. It will also introduce legislation on processing for law enforcement purposes (in support of the EU Law Enforcement Directive) and by the intelligence services, and make provision for the Information Commissioner (as the UK regulator).

## 4 Discussion

- 4.1 Achieving compliance with the GDPR will have significant resource implications in FSS with the production of comprehensive GDPR complaint policies, processes and procedures.
- 4.2 The successful agreement of FSS Record Management Plan (RMP) provided a good basis to work from. The requirements of the GDPR were taken into consideration in the development and implementation of our RMP. Some of the new requirements of GDPR are:
- The need to identify and publish the legal basis for processing all personal data (meaning organisations must demonstrate the justification for processing personal data using specific provisions provided for in the legislation);
  - Changes to privacy notices and the use of consent. The major shift in the new law is about giving data subjects control over their data.
  - Mandatory reporting of all data breaches that infringe on the rights of a data subject;
  - A number of exemptions that FSS use under existing legislation to process data will require additional domestic (UK) legislation to be passed. FSS will need to keep the progress of secondary legislation under review;
  - FSS must be able to demonstrate data protection by “design and default” for systems and processes that process personal data. At the very least, this requires a review of existing contracts;
  - The appointment of a Data Protection Officer, who will have duties defined by the Regulation.
- 4.3 We reviewed our data protection arrangements and concluded that we needed to put in place an action plan to update our data protection policies and processes, and to provide assurance to the Board and Senior Management Team of FSS readiness to comply with the new data protection law from 25th May 2018. This paper provides an update on the activities undertaken and documentation developed to date, to raise awareness of the new laws and demonstrate GDPR compliance across all FSS business areas.
- 4.4 Our conclusion, based on the above, is that we now have clearer processes, procedures, and a governance structure to satisfy the requirements of the new data protection law.

## 5 Progress appraisal

- 5.1 The following items demonstrate what progress has been made with regards to ensuring GDPR compliance to date:
- Training of all FSS Information Asset Owners (IAOs);
  - Registration of 47 information assets on Scottish Government Information Asset Register (IAR);
  - Mandatory annual data protection and protecting information training for staff and contractors;

- 2 x staff awareness sessions – An introduction to information assets;
- 4 x staff awareness sessions – Data protection law is changing;
- Internal GDPR readiness assessment exercise;
- GDPR implementation process flowchart (Annex A);
- FSS SMT approval of GDPR action plan (Annex B);
- Appointment of Garry Mournian (Head Corporate Services) as Data Protection Officer (DPO);
- Weekly GDPR compliance update – CEO's weekly update;
- 2 x half day external GDPR workshops and documentation audits – delivered by Union Data;
- Development and update of our GDPR policies, processes and procedures (Annex C);
- Stakeholder Lists : consolidation exercise including issuing email privacy notices to 3,515 stakeholders;
- Privacy by Design and Default resource suite added to Programme & Project Management (PPM) toolbox;
- On-going review of contracts and agreements in line with new law including seeking GDPR assurances from data processors;
- On-going update of a personal data processing register – documenting the purpose and legal justification for processing personal data;
- On-going GDPR support to teams and individuals.

## **6 Identification of risks and issues**

- 6.1 The issuing of privacy notices will be challenging with FSS having over 50,500 stakeholders without email addresses. We are in consultation with Local Authorities (LAs) to find a mutually beneficial solution where the LAs confirm to Food Business Operators (FBOs) that the purpose of which their personal data was initially collected by LAs at the local level, is similar to the purpose of processing a subset of the data at the national level through Scottish National Database (SND). This approach will reduce the number of stakeholders that we are required to issue hard copy privacy notices from 50,500 to under 5,000.
- 6.2 To demonstrate GDPR key principles of transparency and accountability in the processing of personal identifiable information in FSS, it is imperative that we look to develop a solution that enables the organisation and its Branches to centrally manage all communications and interactions with current and potential stakeholders. This will ensure that we have accurate contact details of stakeholders, audit trail of all large external communications from FSS, and we are not keeping stakeholder information longer than necessary.

## **7 European Union considerations**

- 7.1 The UK Secretary of State for Digital, Culture, Media and Sport – Matt Hancock urged UK organisations to prepare now for GDPR...“There will be no regulatory ‘grace’ period” for noncompliance. GDPR will apply to anyone who offers services to EU citizens regardless of where they are based. The UK will still need to prove ‘adequacy’ in protecting personal data to trade with EU post Brexit.

## 8 Conclusion/Recommendations

8.1 FSS is well prepared to comply with the GDPR which will become enforceable from 25<sup>th</sup> May 2018. GDPR compliance is a work in progress for us, however, with the processes and governance structure that we have in place, we are in a good position to demonstrate compliance to the new law. We will:

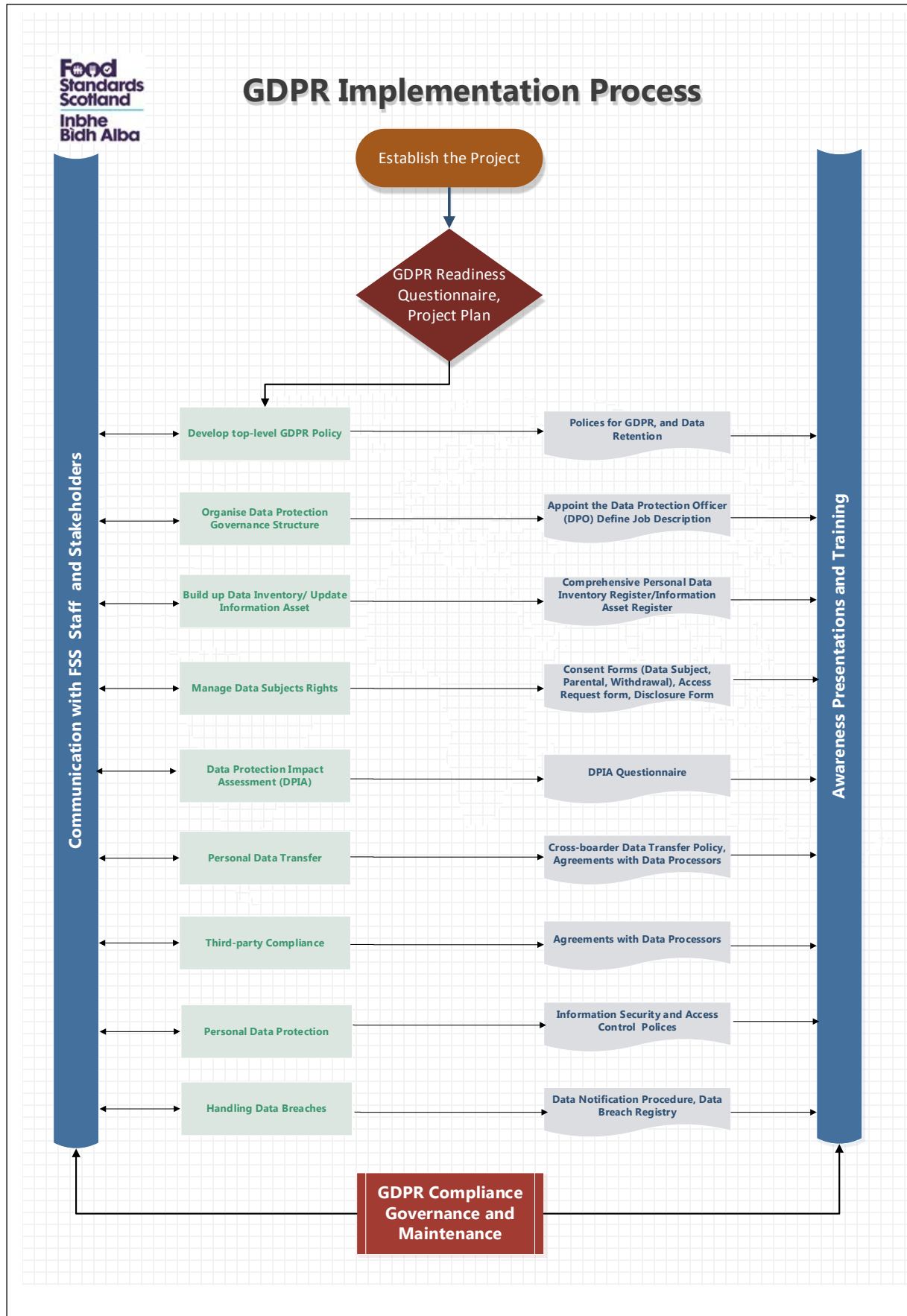
- continue to engage with our internal and external stakeholders to make certain that all stakeholders are equipped with up-to-date information about our collective responsibility to demonstrate compliance to GDPR. To ensure that our messaging and processes are up-to-date, we will commission a GDPR audit review in August 2018. The recommendations from the audit will feed into our internal GDPR implementation programme;
- continue to engage with other data protection practitioner networks to learn and share best practices;
- adopt 'Privacy by Design and Default' principles through the integration of our privacy impact resource suite to the PPM toolbox to ensure that every data sharing activity is cleared with legal and data security experts and supported by enforceable contracts;
- Identify our business requirements and specify a solution that will allow the storage, updating and tracking of all communications sent and received between FSS and stakeholders. This will further safeguard and support the enhanced rights and freedom of data subjects.

8.2 The Board is asked to:

- **Note and comment** on FSS GDPR compliance progress in relation to the UK Information Commissioner's Office recommendation; and
- **Discuss and provide a view** on the recommendation for the ways that FSS can continue to earn the trust and confidence of our stakeholders in the appropriate use of their personal data in line with the new data protection law.

Tigan Daspan  
Records Manager  
[Tigan.Daspan@fss.scot](mailto:Tigan.Daspan@fss.scot)

26<sup>th</sup> April 2018



## Annex B - FSS SMT approval of GDPR Action Plan



**(GENERAL DATA PROTECTION REGULATION  
(GDPR) – ACTION PLAN**

<b>Date of Issue:</b>		19 <sup>th</sup> February 2018
<b>Revision Date:</b>		30 <sup>th</sup> May 2018
<b>Version Number:</b>		Version 1
<b>Document Location:</b>		Objective ID: A19628023
<b>Number of Pages:</b>		10
<b>AUTHOR</b>	<b>Name:</b>	Tigan Daspan
	<b>Position/Role:</b>	Records Manager
	<b>Signature:</b>	
<b>APPROVER</b>	<b>Name:</b>	Garry Mournian
	<b>Position/Role:</b>	Head of Corporate Support
	<b>Signature:</b>	

**VERSION HISTORY**

<b>Version no.</b>	<b>Date</b>	<b>Description of Changes</b>
0.1	27/11/2017	Initial draft
0:2	25/01/2018	approval at SMT
1.0	19/02/2018	Approved by SMT

**TABLE OF CONTENTS**

<a href="#">1.0</a>	<a href="#">PURPOSE AND SCOPE</a>	9
<a href="#">2.0</a>	<a href="#">REFERENCE DOCUMENTS</a>	9
<a href="#">3.0</a>	<a href="#">GDPR IMPLEMENTATION PROJECT</a>	9
<a href="#">3.1</a>	<a href="#">PROJECT OBJECTIVE</a>	9
<a href="#">3.2</a>	<a href="#">PROJECT RESULTS</a>	9
<a href="#">3.3</a>	<a href="#">GDPR IMPLEMENTATION EVENTS/ACTIVITIES</a>	12
<a href="#">3.4</a>	<a href="#">PROJECT ORGANISATION</a>	13
<a href="#">3.4.1</a>	<a href="#">PROJECT SPONSOR</a>	13
<a href="#">3.4.2</a>	<a href="#">PROJECT MANAGER</a>	13
<a href="#">3.4.3</a>	<a href="#">PROJECT TEAM</a>	13
<a href="#">3.5</a>	<a href="#">MAJOR PROJECT RISKS</a>	14
<a href="#">3.6</a>	<a href="#">TOOLS FOR PROJECT IMPLEMENTATION, REPORTING</a>	14
<a href="#">4.0</a>	<a href="#">MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT</a>	14
<a href="#">5.0</a>	<a href="#">VALIDITY AND DOCUMENT MANAGEMENT</a>	14



## 1. PURPOSE AND SCOPE

The purpose of the Project Plan is to clearly define the objective of the European General Data Protection Regulation (GDPR) implementation project, documents to be written, deadlines, and roles and responsibilities in the project.

The Project Plan is applied to all activities performed in the GDPR implementation project.

## 2. REFERENCE DOCUMENTS

- GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Data Protection Bill 2017
- ICO GDPR and Data Protection Bill Web pages

## 3. GDPR IMPLEMENTATION PROJECT

### 3.1 Project Objective

Project objective is to implement the GDPR Management System in accordance with the General Data Protection Regulation (EU GDPR 2016/679) of the European Parliament and of the Council standard by 31 December 2018 at the latest.

### 3.2 Project Results

In order to ensure the most efficient project planning, FSS will use the GDPR Readiness Questionnaire to determine which areas of GDPR compliance need the most work.

The appointment of a **Data Protection Officer (DPO)** is crucial to the successful implementation of the GDPR action plan. The [minimum](#) tasks as defined in Article 39 of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).
- To have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purpose of processing

During the GDPR implementation project, the following 33 documents (some of which contain appendices that are not expressly stated here) will be updated or written:

- **General Personal Data Protection Policy** – a policy meant to establish the general data protection principles as well as to prove the commitment of FSS to those principles;
- **Employee Data Protection Policy** – a policy to set out the conditions under which FSS processes personal data of its employees;
- **General Data Protection Notice** – a notice to set out the conditions under which FSS processes personal data of its stakeholders/website visitors;
- **Register of General Data Protection Notices** – a document where published notices will be listed;
- **FSS Data Retention Policy** – a policy to set out the period for which personal data may be kept by FSS;
- **Data Protection Officer Job Description** – a document that describes the responsibilities of the data protection officer;
- **Guidelines for Processing Activities Inventory** – a document which explains how to list all the data processing activities;
- **Inventory of Processing Activities** – a document to be used by FSS to prove compliance with the requirements of Article 30 of the GDPR;
- **Data Subject Consent Form** - a document used by FSS to obtain consent from the data subjects for processing personal data for a specific purpose;
- **Data Subject Consent Withdrawal Form** - a document used by the data subjects to withdraw their consent;

- **Parental Consent Form** - a document used by FSS to obtain consent from the parent/legal guardian/representative of a minor to process personal data for a specific purpose;
- **Parental Consent Withdrawal Form** - a document used by the parent/legal guardian/representative of a minor to withdraw the consent from processing personal data for a specific purpose;
- **Data Subject Access Request Procedure** – a document to set up the process by which FSS answers to data subjects requests;
- **Data Protection Impact Assessment Methodology** – a document that describes how to assess the necessity and proportionality of a certain processing activity and provide measures to mitigate potential risks to the rights and freedoms of data subjects;
- **DPIA Register** – a document used by FSS to document the DPIA process. It includes the Threshold questionnaire and the DPIA questionnaire;
- **Cross Border Data Transfer Procedure** – a document for establishing the conditions under which a cross border data transfer may be carried out;
- **Standard Contractual Clauses** – model clauses issued by the EU Commission to provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.
- **Processor GDPR Compliance Questionnaire** – a questionnaire meant to assess supplier's compliance with GDPR;
- **Supplier Data Processing Agreement** – a contractual document meant to establish the limits and conditions under which a supplier (processor) can process personal data on behalf of FSS (controller);
- **IT Security Policy** – describes basic security rules for all employees;
- **Access Control Policy** – defines the management and governance process for the approval of access rights to particular users of information systems in FSS;
- **Information Security Management Policy** – describes security rules that need to be adhered to for the use of FSS and SCOTS IT infrastructure;
- **Electronic Communication Policy** – describes security rules for using laptops, mobile phones, social media channels and other devices outside of the FSS premises;

- **Clear Desk and Clear Screen Policy** – defines how to protect the information that is located in the workplace and on computer screens;
- **Government Information Security Classification Policy** – defines how to classify data according to confidentiality, and how to protect the data accordingly;
- **Anonymization and Pseudonymization Policy** – defines how to use these techniques in order to protect the personal data processing;
- **Policy on the Use of Encryption** – defines how to use cryptographic controls and keys to protect the confidentiality and integrity of the data;
- **Disaster Recovery Plan** – defines how to recover the infrastructure and the data after a disrupting incident;
- **Internal Audit Procedure** – defines how to test, assess and evaluate the organizational and technical safeguards in a company;
- **Data Breach Response and Notification Procedure** – a procedure that establishes FSS' obligations in case of a personal data breach;
- **Data Breach Register** – FSS' internal register of data breaches;
- **Data Breach Notification to the Supervisory Authority** – the document to be used in case of a data breach
- **Data Breach Notification to the Data Subjects**– the document to be used in case of a data breach

### 3.3 GDPR Implementation Events/Activities

The following events and activities will serve as an awareness-raising mechanism and to monitor compliance with GDPR across all FSS business areas :

GDPR Implementation Events/Activities	Proposed Timescale
Production and Circulation of GDPR Compliance Questionnaire	18 <sup>th</sup> December 2017
GDPR Myth Busting Seminar	14 <sup>th</sup> December 2017
Report on GDPR Compliance Questionnaire + Review of Contracts, Information Sharing Agreements and Data Protection Impact Assessments etc.	January 2018 to May 2018
Appointment of a Data Protection Officer (DPO)	31 January 2018
FSS GDPR Readiness Audit and Awareness workshop/Seminar (Delivered by external GDPR consultant )	30 March 2018

GDPR Implementation Events/Activities	Proposed Timescale
GDPR Documentation Framework Implementation – Focus on key Mandatory Documentation	January 2018 to May 2018
GDPR Readiness Update Seminar	May 2018
GDPR Documentation Framework Effectiveness Evaluation	June 2018 to August 2018
GDPR Workshop	August/September 2018
GDPR eLearning Module Development	June 2018 to December 2018

### 3.4 Project Organisation

#### 3.4.1 Project Sponsor

Garry Mournian, Head of Corporate Services who does not actively participate in the project but must be regularly briefed by the project manager about the project status, and intervene if the project is halted or delayed.

#### 3.4.2 Project Manager

The role of the project manager is to ensure resources necessary for project implementation, to coordinate the project, to inform the sponsor of the progress, and to carry out administrative work related to the project. The project manager's authority should ensure uninterrupted project implementation within set deadlines.

Tigan Daspan – Records Manager has been appointed project manager.

#### 3.4.3 Project Team

The role of the project team is to assist in various aspects of project implementation, to perform tasks as specified in the project, and to make decisions about various issues that require a multidisciplinary approach. The project team meets each time before the final version of 3-5 documents from section 3.2 of this Project Plan is completed, and in all other cases when the project manager deems it necessary.

**Table of participants in the project**

<b>Name</b>	<b>Branch</b>	<b>Job title</b>
Tigan Daspan	Corporate Services	Records Manager
Gordon Munn	Corporate Services	IT Projects Business Partner
Deepika Garg (HR Representative )	Corporate Services	HR Coordinator
Communication Representative	Communication & Marketing	Digital Marketing Manager
Private Office Representative	Private Office	Executive Officer

**3.5 Major Project Risks**

The main risks in the implementation of the project are the following:

- Extension of deadlines
- Performing activities that incur unnecessary costs and waste time
- Shortage or lack of competent employees (e.g. a DPO)

**3.6 Tools for Project Implementation, Reporting**

A shared file including all documents produced during the project will be created on eRDM. All members of the project team will have access to these documents. Only the project manager [and members of the project team] will be authorized to make changes and delete files.

**4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT**

<b>Record Name</b>	<b>Storage Location</b>	<b>Person Responsible for Storage</b>	<b>Control for Record Protection</b>	<b>Retention Time</b>
GDPR Action Plan	Shared file for project related activities in eRDM	Project Manager	Only the project manager and project team are authorised to edit data	All relevant records produced or captured during the GDPR implementation will be stored for a period of 5 years

**5. VALIDITY AND DOCUMENT MANAGEMENT**

This document is valid as of 19<sup>th</sup> February 2018



Owner of this document is Records Manager

Records Manager

A handwritten signature in black ink, appearing to read 'TIGAN DASPAN', written over a horizontal line.

TIGAN DASPAN

## ANNEX C - Development and update of GDPR policies, processes and procedures

Steps	Completed	Completed /Ongoing Update	In Progress	Not Started
1. Awareness	<ul style="list-style-type: none"> <li>- FSS IAOs Trained + IA Staff Awareness Sessions</li> <li>- <a href="#">GDPR – Action Plan</a> + <a href="#">Readiness Questionnaire</a></li> </ul>	<ul style="list-style-type: none"> <li>- <a href="#">Staff Awareness Sessions</a> - (4 x + 1-1++)</li> <li>- Weekly GDPR update – Geoff's Weekly Update</li> <li>- For the Field Monthly Update</li> </ul>		
2. Information you hold	<ul style="list-style-type: none"> <li>- External Audit – Union Data</li> <li>- FSS information assets registered on SG IAR</li> </ul>	<ul style="list-style-type: none"> <li>- <a href="#">GDPR Personal Data Processing Register</a></li> </ul>		
3. Communicating Privacy Information	<ul style="list-style-type: none"> <li>- <a href="#">Privacy Notice Guidance</a></li> </ul>	<ul style="list-style-type: none"> <li>- <a href="#">Privacy notices - Options</a></li> </ul>	<ul style="list-style-type: none"> <li>- GDPR Policy</li> </ul>	
4. Individual's rights	<ul style="list-style-type: none"> <li>- <a href="#">GDPR – Readiness Assessment Matrix</a></li> </ul>	<ul style="list-style-type: none"> <li>- <a href="#">GDPR Personal Data Processing Register</a></li> </ul>	<ul style="list-style-type: none"> <li>- GDPR Policy</li> </ul>	
5. Subject access requests	<ul style="list-style-type: none"> <li>- <a href="#">Data Subject Access Request Flowchart</a></li> <li>- Data Subject Access Request (DSAR) Form</li> <li>- GDPR – Personal Data Disclosure Form</li> </ul>			
6. Lawful basis for processing personal data		<ul style="list-style-type: none"> <li>- <a href="#">GDPR Personal Data Processing Register</a></li> <li>- <a href="#">Stakeholder List - Consolidation Exercise</a></li> <li>- <a href="#">Privacy Impact Plan</a> &amp; Data Sharing Agreements</li> <li>- Review of Contracts and agreements</li> </ul>		
7. Consent	<ul style="list-style-type: none"> <li>- <a href="#">Privacy Notice Guidance</a></li> </ul>	<ul style="list-style-type: none"> <li>- <a href="#">GDPR Personal Data Processing Register</a></li> <li>- Review of Contracts and Agreements</li> <li>- <a href="#">Stakeholder List - Consolidation Exercise</a></li> </ul>		
8. Children				<ul style="list-style-type: none"> <li>- Parental Consent form</li> <li>- Parental Consent Withdrawal Form</li> </ul>
9. Data breaches	<ul style="list-style-type: none"> <li>- <a href="#">Personal Data Breach Reporting Form</a></li> </ul>		<ul style="list-style-type: none"> <li>- Personal Data Breach Guidance</li> <li>- Personal Data Breach Register</li> </ul>	
10. Data Protection by Design & Default & Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> <li>- <a href="#">Privacy Approach Briefing</a></li> <li>- <a href="#">Privacy Impact Plan</a></li> <li>- <a href="#">Privacy Impact Screen</a></li> <li>- <a href="#">Privacy Impact Guide</a></li> <li>- <a href="#">Privacy Impact Register</a></li> </ul>			



<b>11. Data Protection Officer</b>	- Garry Mournian - Head Corporate Services (DPO)			
<b>12. International</b>	- Lead Data Protection Supervisory Authority – Information Commissioner’s Office (ICO)			- Cross Border Data Transfer Procedure - Standard Contractual Clauses