An Roinn Cosanta
Department of Defence

CIVIL DEFENCE
Cosaint Shibhialta

Policy on Data Management

Policy Number	POL GEN 004
Policy Owner	AP – Business Management & Procurement
Revision date	March 2026
Approved by	Head of Branch
Further info	civildefence@defence.ie
Review by	March 2027*
Policy Summary	This policy sets out the controls in place to ensure the security of data in all Civil Defence business processes
Changes Made	New policy

**As a new policy, and in the context of potential system changes in 2026/27, this policy should be reviewed after one year. Thereafter, every two years or as required by changes in legislation*

Contents

1. Purpose

The purpose of this policy is to clearly outline the end-to-end data management and protection processes that are employed within Department of Defence Civil Defence Branch, including any shared management with other Data Controllers or Processors

2. Introduction/Background

Civil Defence (Cosaint Shibhiálta) is a statutory volunteer-based organisation with a nationwide footprint, established in 1951. In central Government terms, responsibility for the organisation falls under the aegis of the Department of Defence/Civil Defence Branch. The Department has responsibility for setting the strategic direction and policymaking for the national civil defence organisation, and for a number of other processes including garda vetting, central training and central procurement of key fleet and equipment.

At a local level, Civil Defence is managed by Civil Defence Officers employed by each local authority. The local authorities fall under the ambit of the Department of Housing, Planning & Local Government. Local authorities have responsibility for the operational management of their respective units.

There are approximately 2,000 Civil Defence volunteers registered with 28 Civil Defence Units across the 26 Local Authorities. The management of these volunteers is affected through the Volunteer and Equipment Management System (VEMS) which is operated under a Joint Data Controller Agreement between the Department of Defence and each Local Authority.

In addition to the management of VEMS, the respective organisations have defined Data Management and Protection procedures as set out in Sections 2 and 3 below.

2. Department of Defence Data Protection and Data Management Procedures

As a Branch of the Department of Defence, Civil Defence Branch is governed by Department of Defence Data Protection and Management Procedures.

The Department of Defence has a Data Governance unit which has overall responsibility for the following:

- Archives
- Corporate Data
- Data Protection
- Freedom of Information
- Irish Language Awareness
- Records Management

Policies relating to all of the above are available on the Department of Defence DNet. Noelle Clancy is the Department of Defence Data Protection Officer. The Department of Defence Data Protection Policy last updated May 2018. This Policy is published on The Departments DNET and can be accessed at https://defence.cloud.gov.ie/KnowledgeBase/DATAPROTECTION/Shared%20Documents/Data%20Protection%20Policy

The policy covers the following

1. Introduction
2. Purpose
3. Scope
4. Data protection principles
5. Rights of data subjects
6. Responsibility for this policy
7. Responsibilities of the Department of Defence
8. Responsibilities of the Data Protection Officer
9. Responsibilities of staff

10. Queries about the data protection policy

Data Protection Training is mandatory for all Department of Defence Staff and is available on the Department's eLearning portal. This training is updated every 2 years with the latest module released in January 2026 to cover Data Protection 2026 to 2028.

The Department of Defence Records Management Policy was last updated May 2018. This Policy is published on The Departments DNET and can be accessed at https://defence.cloud.gov.ie/Shared%20Documents/Records%20Management/Records%20Management%20Policy

The policy covers the following

1.0 Introduction

2.0 Policy Aims and Objectives

3.0 Scope

4.0 Roles and Responsibilities

5.0 Records Management Principles

6.0 Training

7.0 Failure to Comply with the Records Management Policy

8.0 Review Period

Records Management Training is mandatory for all Department of Defence Staff and is available on eLearning.

Within **Civil Defence Branch**, the Business Management Section has responsibility for the Branch management of the above processes. The Branch has a Data Governance Steward Eileen Joyce and an Alternate Data Governance Steward Merena Doran. They are members of the Data Governance Working Group which meets 4 times each year to discuss all matters Data Governance related.

3. Local Government Management Association/Local Authority Data Protection and Data Management Procedures

The LGMA have the following privacy statement on their website which is linked to their Data Protection policy

LGMA Privacy Statement

This website is maintained by the Local Government Management Agency. The Agency respects your right to privacy and will not collect any personal information about you on this website without your clear permission. Any personal information which you volunteer will be treated with the highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts, 1988 – 2018.

This website does not collect any personal data, apart from information that you volunteer. (For example, when providing feedback or asking a question). Any information you provide in this way is used only for the purpose you provide it.

Local Authority Data Management and Protection processes are designed to ensure that personal data is managed securely. Key procedures include appointing a Data Protection Officer, publishing privacy notices, conducting DPIAs as required, handing access requests and reporting data breaches.

An example of the very detailed Kilkenny County Council Data Protection protocol can be viewed at the following link: https://kilkennycoco.ie/eng/your_council/data-protection/#:~:text=Right%20of%20Rectification%20or%20Erasure,locate%20the%20personal%20data%20involved.

4. Specific information – Civil Defence processes

4.1 Joint Controller Agreement between Department of Defence/Civil Defence and each Local Authority & the Volunteer & Equipment Management System

Civil Defence Branch has a Joint Controller Agreement with each Local Authority in relation to the operation of the Volunteer and Equipment Management System. This agreement sets out the respective roles and responsibilities of the data controllers, who have jointly determined the purposes and means of processing and the arrangement between the Parties inherent to the operation of Civil Defence.

It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other. It is signed by the Principal Officer in Civil Defence Branch and Data Protection Officer in the Local Authority on Behalf of the Chief Executive Officer of the Local Authority.

Civil Defence hosts the Volunteer and Equipment Management System, which records all data necessary to manage volunteers and duties. The information recorded includes Volunteer Personal Information, their training, vaccinations, and events that they have attended with Civil Defence.

Within Civil Defence Branch, the system is used to record garda vetting, training, uniforms and equipment. Within each Civil Defence Unit, a small number of designated employees have access to the VEMS system for the purpose of recording certain elements of training, and for recording the assignment of volunteers to duties.

The system restricts access according to agreed roles, and is further security controlled using multi-factor authentication.

Volunteers also have very restricted (and password protected) access through the Volunteer Portal

Each Role is restricted to the area that the person is working in. Data can only be seen on a need-to-know basis.

4.2 Learning Support Platform

Civil Defence College utilises a Moodle Learning Support Platform for the purposes of sharing College & Course related information and tracking completion of certain key self-paced learning.

This system is also password protected, with access to different areas of the system linked to the user access role.

Volunteers can access the following data protection information on the Learning Support Platform: https://www.civildefence.ie/wp-content/uploads/2023/03/1.2.5-Civil-Defence-College-Data-Protection-Policy-4-2022.pdf

4.3 Management of hard copy records that contain personal data

All Civil Defence training for Volunteers at PHECC responder and practitioner level includes the importance of data protection in respect of patient care records and patient information.

Local Authority Civil Defence Officers follow the Local Authority GDPR record management processes, including in respect of the storage of completed Patient Care Records.

The management of patient care records is audited by the Governance Validation Framework Working Group, in the course of their on-site audits.

4.4 Annual reviews – Record of processing activities (ROPA) and Security reviews

Each year, the Department of Defence requires that all Branches complete a ROPA Review and a Security Review to ensure that all processing activities are kept under constant review and are appropriate, and to ensure that the security of records is appropriate and maintained.

4.5 Use of Unmanned Aircraft Systems and footage transmission

Civil Defence operates an Unmanned Aircraft System (UAS) service, also called a Drone Service. in support of the Principal Response Agencies (PRAs). Civil Defence Remote Pilots are trained and certified by the Irish Aviation Authority (IAA) to operate in the 'Open Category'.
The main drone activity is searching for missing persons in coastal areas, rivers, lakes and countryside. Other services provided by Civil Defence in the context of the UAS service include:

- Mapping of areas of land and water
- Surveys for local authorities
- Photography and videography for other State bodies
- Photography and videography of operations and training events

Once an activation request is received by the local Civil Defence Officer from a PRA, the drone team can respond. Appropriate warning signage is erected around the drone operator advising members of the public that drone activity is taking place.

For Missing Person Searches:

1) VIDEOING - Videography/photography is only engaged when the UAS is flown over the allocated Search Area. All recording is disabled while traversing the landing/take-off area to the Search Area.
2) DOWNLOAD - Once the flight operation is completed, the SD card on which the imagery data is recorded is taken from the craft and reviewed on a computer to ensure that nothing was missed during the operational flight. If nothing of relevance to the operation appears on the SD card then it is formatted (wiped) and returned for the next flight. If an item of interest is identified, the pilot is notified, and the images are handed as potential evidence to Án Garda Siochána (AGS) under a Civil Defence Data Sharing Agreement.
3) DELETING - Any footage not needed as evidence is erased.

For other services:

When supporting the local authority or other state bodies with UAS systems for other roles particularly for emergency management, all images and video are handed over to the relevant section, e.g. Fire & Rescue

SONAR:

Civil Defence operates a SONAR service in support of the Principal Response Agencies (PRAs). The primary sonar activity is searching for missing persons in bodies of water, although Civil Defence will occasionally engage in sub-surface surveys for local authorities. Sonar images and scans are revied by the sonar operators for anomalies and these are handed over to the relevant tasking agency e.g. AGS for missing person searches.

Annex

Joint Controller Agreement

between

The Department of Defence

and

XXXXXXX County Council

In respect of Civil Defence

November 2023

VERSION CONTROL

Document Title	Joint Controller Agreement between the Department of Defence and individual LAs in respect of Civil Defence.
Document Reference/Version Number	1.1
Purpose of Document	This Agreement sets out the respective roles and responsibilities of the data controllers who have jointly determined the purposes and means of processing and the arrangement between the Parties inherent to the operation of Civil Defence. It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.
Document Author	Civil Defence Branch, Department of Defence
Authorised By	Principal Officer, Civil Defence Branch ? on behalf of the Local Authority.
Effective Date	tbc
Proposed Review Date	To be reviewed every 5 years or whenever there is a significant change to the administrative arrangements put in place for the effective delivery of the schemes.
Responsibility for Review	Civil Defence Branch, Department of Defence ? on behalf of the Local Authorities
Contact Details	Civil Defence Branch, Department of Defence, Benamore, Roscrea, Co. Tipperary. 0505-25310

Version	Date Issued	Summary of Changes
1.0	5/09/2023	First Draft prepared by A. Dillon
1.1	22/09/2023	Second draft incorporating suggestions from the Departments DPO
1.2	3/10/2024	Third draft incorporating suggestions from the LGMA DPO committee

THIS AGREEMENT is made on [ ]

BETWEEN:

(1) The Minister for Defence, whose principal place of business is at Department of Defence, Station Road, Newbridge, Co. Kildare ("the Minister")

And;

(2) The Local Authority ("Local Authority") [insert details, address etc]

(each a "Party" and together "the Parties").

WHEREAS:

A. The Civil Defence Act, 2023 provides for the functions of the Minister for Defence relating to Civil Defence and also provides for the responsibilities of Local Authorities relating to Civil Defence.

B. The Civil Defence Act, 2023 also provides for the establishment and maintenance of a register to be known as the Register of Civil Defence Volunteers.

C. Details of the personal data processed by the Minister, and the Local Authority, is set out in Appendix 2.

D. The Minister and the Local Authority are joint controllers as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council, 27 April 2016 (the "GDPR").

E. The Minister and the Local Authority are required, as joint controllers, pursuant to Article 26 of the GDPR to prepare an Agreement setting out their respective responsibilities for compliance with their obligations under the GDPR and to make available to data subjects, as defined in the GDPR, the essence of that Agreement (the "Agreement").

F. The Minister and the Local Authority have entered into the Agreement on the date of this Agreement and the essence of this Agreement is available to Data Subjects by means of notification at www.Defence.ie and the Local Authority website at www.xxxcoco.ie.

INTERPRETATION

1. The following definitions apply in this Agreement:

"Act" means the Civil Defence Act 2023:

"Agreed Purpose" has the meaning set out in clauses 6 - 10;

"Agreement" means this Agreement and the provisions in Appendix 1;

"Anonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject.

"**Data Controller"** has the meaning given under the Data Protection Laws;

"Data Processor" has the meaning given under the Data Protection Laws;

"Data Protection Laws" means all applicable national and EU data protection laws, regulations and guidelines, including but not limited to the Data Protection Acts 1988 to 2018 and Regulation (EU) 2016/679 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 (the "General Data Protection Regulation"), and any guidelines and codes of practice issued by the Office of the Data Protection Commission or other supervisory Authority for data protection in Ireland.

"Data Subject" has the meaning given under the Data Protection Laws;

"Data Subject Access Request" means a request made by a Data Subject in accordance with rights granted under the Data Protection Laws to access his or her personal data;

"Department" means the Department of Defence;

"Personal data" has the meaning given under Data Protection Laws;

"Personal data breach" has the meaning given to it by Article 4 of the GDPR

"Processing" has the meaning given under the Data Protection Laws.

2. Except as expressly provided for in this Agreement, terms defined and used in this Agreement shall have the same meaning as those terms defined and used in the Arrangement as attached as Appendix 1 hereto.

3. The Parties agree to abide by the terms of this Agreement.

4. This Agreement shall in all aspects be governed by and construed in accordance with the laws of Ireland and the Parties hereby further agrees that the courts of Ireland have exclusive jurisdiction to hear and determine any disputes arising out of or in connection with this Agreement.

5. This Agreement does not purport to alter the respective responsibilities which each Party has under the relevant Data Protection Laws but rather seeks to clarify how their responsibilities may be met where personal data collected and processed by the Local Authority is made available to the Minister for the purposes set out in clause 9 below.

PURPOSE OF AGREEMENT

6. This Agreement sets out the respective roles and responsibilities of the data controllers who have jointly determined the purposes and means of processing and the arrangement between the Parties. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

7. This Agreement shall be amended by the Parties should it be found appropriate to set out further procedures for the sharing/processing of Personal data.

8. The Local Authority collects personal data in order to comply with its responsibilities under the Act including the following;

   (a) The establishment and maintenance of its Civil Defence Unit in accordance with Section 4 of the Act.
   (b) The appointment of Civil Defence Officers in accordance with Section 5 of the Act.
   (c) The recruitment, management, deployment and training of Civil Defence Volunteers in accordance with Section 6 of the Act.
   (d) The establishment and maintenance of a register of Civil Defence Volunteers in accordance with Section 7 of the Act.

9. The Minister processes Personal data relating to Civil Defence, including for the following purposes;
   (a) Assisting with the maintenance of the Register of Civil Defence Volunteers, in accordance with Section 7 of the Act,
   (b) Assisting with the training of Civil Defence Volunteers, including the certification of such training,
   (c) Assisting with the Garda Vetting of Civil Defence Volunteers, as provided for under Section 6(2) (d)(iv) of the Act; and to
   (d) Discharge the Minister's governance and oversight responsibilities for the funding of Civil Defence, in accordance with Section 9 of the Act.

10. Article 6(1)(e) of the General Data Protection Regulation (EU) 2016/679 (GDPR) allows for processing of personal data to be carried out "in the performance of a task carried out in the public interest". Article 9(2)(h) of the General Data Protection Regulation provides for the processing of medical information for the assessment of the working capacity of an individual.

ROLES & RESPONSIBILITIES OF THE LOCAL AUTHORITY IN RELATION TO THIS AGREEMENT

11. The Local Authority confirms that it will only process the Personal data the subject of this Agreement in accordance with law and that the Local Authority has a legal basis for processing the data.

12. The Local Authority collects the Personal data in accordance with the relevant legislation, which is required for the operation of Civil Defence in the area of that Local Authority.

13. The Local Authority shall include details of the Personal data it collects in respect of Civil Defence in its data privacy notices.

14. The Local Authority shall not transfer onwards the Personal data the subject of this Agreement unless required to do so by law; in such a case the Local Authority shall inform the Minister of the requirement and will be responsible for including details in its privacy notices.

ROLES & RESPONSIBILITIES OF THE MINISTER IN RELATION TO THIS AGREEMENT

15. The Minister confirms that he/she will only process the Personal data the subject of this Agreement in accordance with law and that the Minister has a legal basis for processing the data.

16. The Minister shall, in the privacy notice available on www.Defence.ie, provide information on the Personal data processed by the Department in relation to Civil Defence.

17. The Minister shall not transfer onwards the Personal data to which he/she has been given access unless required to do so by law; in such a case the Minister shall inform the Local Authority of the requirement and he/she will be responsible for including details in its privacy notice.

18. Where the Minister receives queries directly from members of the Civil Defence organisation or members of public regarding their own personal data, and or from public representatives as per section 40 of the Data Protection Act 2018, personal information may be requested from the Local Authority to respond appropriately to these queries.

USE OF PROCESSORS AND DATA TRANSFERS

19. The Parties are entitled to use data processors and sub-processors in connection with the Agreed Purpose as defined in this Agreement.

20. If any data processors and-sub-processors are used, each Party is responsible for compliance with the requirements of Article 28 of the GDPR. Each Party is obliged, inter alia, to:

    a use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Laws and ensure the protection of the rights of the data subject;

b ensure that a valid data processing agreement has been made between the Party and the data processor; and

c ensure that a valid sub-processing agreement has been made between the data processor and any sub-processor.

21. The data processors used by both Parties in connection with the processing are detailed at Appendix 3. If either Party intends to use data processors in connection with the processing other than those detailed at Appendix 3, the Party in question must inform the other Party.

22. Neither Party will authorise the disclosure, transfer or further processing of personal data with a third Party outside of the EEA without (i) ensuring that such disclosure/transfer is permitted under the Data Protection Laws and (ii) informing the other Party of the planned disclosure, transfer or further processing.

23. If either Party processes the Personal data for any purpose other than the Agreed Purpose as defined in this Agreement, that Party shall do so as an independent Data Controller in respect of that processing and shall be solely responsible for that processing under the Data Protection Laws.

SECURITY ARRANGEMENTS

24. The Local Authority confirms that it has in place the necessary technical and organisational measures to keep the personal data the subject of this Agreement secure.

25. The Local Authority shall ensure that members of its staff who have access to the personal data have an appropriate level of awareness of the security measures in place and that they comply with the security measures.

26. The Local Authority shall ensure that only staff designated in writing by the Chief Executive may access the Register of Civil Defence Volunteers, in accordance with Section 7(5)(b) and 7 (6)(a) of the Act.

27. The Local Authority shall ensure that only Civil Defence Officers employed by the Local Authority may access and process the medical information referred to in Section 7(4)(i) of the Act.

28. The Minister confirms that he/she has in place the necessary technical and organisational measures to keep the personal data the subject of this Agreement secure.

29. The Minister shall ensure that Department of Defence staff who have access to the personal data have an appropriate level of awareness of the security measures in place and that they comply with the security measures.

30. The Minister shall ensure that only such officers as the Minister may designate in writing may access or amend the Register of Civil Defence Volunteers, in accordance with Section 7(5)(c) and 7(6)(b) of the Act.

DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

31. Each of the Parties is responsible for compliance with the requirement in Article 35 of the GDPR on data protection impact assessments. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the joint controllers must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

32. Where a DPIA is to be undertaken by the Local Authority, the Minister shall be consulted on identifying potential risks and the various measures designed to treat risks and to protect the rights of the data subjects.

33. Where a DPIA is to be undertaken by the Minister, the Local Authority shall be consulted on identifying potential risks and the various measures designed to treat risks and to protect the rights of the data subjects.

34. The joint controllers are obliged to comply with the requirement in Article 36 of the GDPR on prior consultation of the supervisory Authority when this is relevant.

AUDITS AND COOPERATION WITH THE SUPERVISORY AUTHORITY

33. Each of the Parties is responsible for cooperation with the Supervisory Authority. The Parties agree that they will assist each other, where required, with any requests for information from the Supervisory Authority.

34. The Parties agree that upon request from the Supervisory Authority, they will submit their data processing facilities for an audit and, if required, will cooperate with each other in relation to the audit.

DATA BREACHES

35. The Local Authority and the Minister shall each inform the other immediately (but no later than 24 hours) after it comes to their attention that a Personal data Breach likely to result in a risk to the rights and freedoms of natural persons has occurred.

36. In the case of any doubt about whether a breach is likely to result in a high risk to the rights and freedoms of natural persons, the Parties shall consult each other and carry out a joint risk assessment to decide on the remedial and preventative action that may be required.

37. In the case of a Personal data breach within the Local Authority and/or its agents and processors that is likely to result in a risk to the rights and freedoms of natural persons, the Local Authority will be responsible for notifying the Data Subjects and the Data Protection Commission in line with requirements in Art 33 and 34 of the GDPR. The Local Authority's Data Controller will provide such assistance that the Minister's Data Controller may need in order to fully comply with the Data Protection Laws.

38. In the case of a Personal data breach by the Department that is likely to result in a risk to the rights and freedoms of natural persons, the Department will be responsible for notifying the Data Subjects and the Data Protection Commission in line with requirements in Art 33 and 34 of the GDPR. The Minister's Data Controller will provide such assistance that the Local Authority's Data Controller may need in order to fully comply with Applicable Data Protection Law.

RIGHTS OF DATA SUBJECTS

39. The Local Authority shall, in principle, be responsible for responding to requests from Data Subjects for the exercise of their rights in connection with the processing of the personal data,
e.g. requests for confirmation of processing, access, copies of the data, rectification, erasure, and restriction of processing and to any objection raised to processing of the data, the subject of this Agreement.

40. Data Subjects shall be notified of this in the information provided to them by the Local Authority when the data is collected. Where a Data Subject makes a request of the Department, the Department shall refer the Data Subject to the Local Authority if the request concerns the Local Authority processing of the personal data but the Department shall respond to the request if it concerns the Department's processing of the personal data.

41. The Parties agree to assist each other and provide whatever technical assistance is required to allow the other to respond to a Data Subject request.

42. The Local Authority intends to retain the personal data processed in respect of their responsibilities under the Act as outlined in the Local Authority's data retention policy.

43. The Department intends to retain the personal data made available to it by the Local Authority pursuant to the Agreed Purpose for a period of as outlined in the Department's data retention policy.

REVIEW OF THE AGREEMENT

44. Each Party commits to giving a minimum of 90 days-notice of its intention to review this Joint Controller Agreement.

45. The Agreement should also be reviewed where there is a significant change to the administrative arrangements put in place for Civil Defence.

46. The Agreement will be terminated where it can be shown that a Joint Controller relationship no longer exists between the Parties.

SIGNATURES

Both parties agree that the officer who signs this Agreement shall take responsibility for the adherence to terms and conditions of this agreement.

Signed:

_____

XXXX – Post held in LA

For and on behalf of the Chief Executive Officer

Xxx County Council

Date:

_____

Principal Officer

For and on behalf of the Minister for Defence:

Appendix 1 – Arrangement between the Minister and xxx Local Authority

1. The parties to this arrangement are:
   a. The Minister for Defence and
   b. Xxx Local Authority

2. The parties are entering into this arrangement for the purposes of Article 26 of the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and the Council, 27 April 2016.

3. The Local Authority collects personal data in order to comply with its responsibilities under the Civil Defence Act 2023, including the following:
   (a) The establishment and maintenance of its Civil Defence Unit in accordance with Section 4 of the Act.
   (b) The appointment of Civil Defence Officers in accordance with Section 5 of the Act.
   (c) The recruitment, management, deployment and training of Civil Defence Volunteers in accordance with Section 6 of the Act.
   (d) The establishment and maintenance of a register of Civil Defence Volunteers in accordance with Section 7 of the Act.

4. The responsibilities of XXX Local Authority in relation to the Civil Defence, as agreed in this Agreement, are as follows:
   (a) xxx Local Authority is responsible to the data subjects as regards any rights they wish to assert under the General Data Protection Regulation, and the Data Protection Act 2018, including right of access and rectification.

(b) xxx local authority is responsible for providing information on the processing of personal data within their Civil Defence Unit in a transparent manner in accordance with Articles, 12, 13 and 14 of GDPR.

5. Legal basis for processing:
   Pursuant to the Civil Defence Act 2023 XXXX Local Authority is authorised to process data for the purposes of complying with its responsibilities in relation to Civil Defence.

6. In meeting, its statutory obligation in respect of Civil Defence, the Local Authority may require the following personal data:
   (a) the volunteer's name;
   (b) the volunteer's home address, email address and telephone number;
   (c) the volunteer's date of birth;

(d) the date on which the volunteer was registered by the Local Authority concerned;

(e) records of the volunteer's training for the purposes of carrying out duties as a civil defence volunteer;

(f) records of the volunteer's qualifications for the purposes of carrying out duties as a civil defence volunteer;

(g) records of the volunteer's attendance at, and carrying out of, duties as a civil defence volunteer;

(h) a unique number assigned to the volunteer which shall be used to identify the volunteer;

(i) medical information, only insofar as such information is required to assess the capability of the person to carry out duties as a civil defence volunteer in respect of which such medical information is required;

(j) details of the volunteer's driving licence;

(k) the most recent date of a vetting disclosure made in respect of the volunteer by the National Vetting Bureau of the Garda Síochána under section 14 of the Act of 2012 for the purposes of carrying out duties as a civil defence volunteer;

(l) details of equipment and clothing issued to the volunteer for the purpose of carrying out duties as a civil defence volunteer

The information is maintained by the Local Authority in line with the Local Authority data retention policy which is available at www.xxxCOCO.ie

Any information in respect of Civil Defence volunteers held by the Department of Defence will be maintained in line with the Department of Defence data retention policy which is available at www.defence.ie.

7. Subject Access Requests, including postal queries, are dealt with by the Data Protection Officer {Insert LA + address of LA, **email:** DPO@xxxCOCO.ie.

8. Further, if the Minister is in receipt of a subject access request then same is passed on to dataprotection@defence.ie

9. Xxx Local Authority's Privacy Notice and further information is available at www.xxxCOCO.ie or by contacting XXXX Local Authority at DPO@xxxCOCO.ie or by post or by writing to Data Protection Officer, xxxx Local Authority.

Appendix 2 – Details of the personal data processed by the Local Authority and the Minister

Personal data processed by the Local Authority:

The **Local Authority** is the primary collector of personal data in respect of Civil Defence. Data collected from data subjects (including via application forms) includes the following;

(a) the volunteer's name;

(b) the volunteer's home address, email address and telephone number;

(c) the volunteer's date of birth;

(d) the date on which the volunteer was registered by the Local Authority concerned;

(e) records of the volunteer's training for the purposes of carrying out duties as a civil defence volunteer;

(f) records of the volunteer's qualifications for the purposes of carrying out duties as a civil defence volunteer;

(g) records of the volunteer's attendance at, and carrying out of, duties as a civil defence volunteer; (h) a unique number assigned to the volunteer which shall be used to identify the volunteer;

(i) medical information, only insofar as such information is required to assess the capability of the person to carry out duties as a civil defence volunteer in respect of which such medical information is required;

(j) details of the volunteer's driving licence;

(k) the most recent date of a vetting disclosure made in respect of the volunteer by the National Vetting Bureau of the Garda Síochána under section 14 of the Act of 2012 for the purposes of carrying out duties as a civil defence volunteer;

(l) details of equipment and clothing issued to the volunteer for the purpose of carrying out duties as a civil defence volunteer.

Personal data processed by the Minister

This data is generally entered onto the on-line Register of Civil Defence Volunteers, known as the Volunteer and Equipment Management System (VEMS). The VEMS system is maintained by the Department of Defence. Department of Defence officials, designated in writing by the Minister, can access all information on VEMS. Designated officials in each Local Authority can only access information on VEMS in relation to their own Local Authority.

Periodic Garda Vetting is required for all Civil Defence Volunteers. Vetting applications are processed centrally by the Department of Defence. Vetting is not done via the VEMS system. However the date of the most recent vetting is entered onto VEMS for the purposes of ensuring prompt re-vetting is carried out (currently every 5 years).

Appendix 3 - Data Processors, in Ireland, the European Economic Area (EEA) and third countries outside the EEA, engaged by the Parties in connection with the joint processing

List of Data Processors used by the Minister

Processor Name	Location (Country)	Service Provided
Codec	Ireland	Codec are the VEMS system implementers. They provide a managed service for support and maintenance.

List of Data Processors used by the Local Authority

Processor Name	Location (Country)	Service Provided