

## St John Ambulance Ireland

# General Data Protection Regulation Policy

### 1. Introduction

St John Ambulance Ireland (SJAI) collects and uses data for a variety of purposes about its staff, officers, members/volunteers, examination candidates, patients and other individuals who come in contact with the organisation.

The General Data Protection Regulation (GDPR) was brought into force in 25 May 2018 and supersedes the previous Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

### 2. Purpose of this Policy

This policy is a statement of SJAI's commitment to protect the rights and privacy of individuals in accordance with the General Data Protection Regulation.

### 3. Definitions used in GDPR Policy

- Data means automated and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system.
- Data Controller means a body that, either alone or with others, controls the contents and use of personal data.

- Data Processor means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.
- Data Subject means an individual who is the subject of personal data. This includes patient data.
- Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
- Processing means performing any operation or set of operations on the information or data, whether or not by automatic means, including:
  - a) Obtaining, recording or keeping the information, or
  - b) Collecting, recording organising, storing, altering or adapting the information or data,
  - c) Retrieving, consulting or using the information or data
  - d) Disclosing the information or data by transmitting, disseminating or otherwise making them available, or
  - e) Aligning, combining, blocking, erasing or destroying the information or data.

Relevant Filing System means any set of information relating to individuals to the extent that, while not computerised, is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data means personal data, which relate to specific categories defined as:

- a) The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
- b) Trade union membership
- c) The physical or mental health or condition or sexual life of the data subject
- d) The commission or alleged commission of any offence by the data subject, or
- e) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.



#### 4. Responsibilities under the GDPR Policy

SJAI have certain **key responsibilities** in relation to the information which we keep on computer or in a structured manual file about individuals. These are summarised in terms of eight "Rules" which are listed below;

- **Obtain** and process the information fairly
- **Keep** it only for one or more specified and lawful purposes
- **Process** it only in ways compatible with the purposes for which it was given to you initially
- Keep it **safe and secure**
- Keep it **accurate and up-to-date**
- Ensure that it is **adequate, relevant and not excessive**
- Retain it **no longer than is necessary** for the specified purpose or purposes
- **Give a copy of his/her personal data** to any individual, on request.

#### 4. Responsibility

SJA has overall responsibility for ensuring compliance with the General Data Protection Regulation. However, all employees and members/volunteers of the organisation who collect and/or control the contents and use of personal data are also responsible for compliance with GDPR. The organisation will provide support, assistance, advice and training to all sections, offices, staff, members/volunteers to ensure it is in a position to comply with GDPR.

It will be the responsibility of the Commissioner to develop and encourage good data handling practice within the organisation.

While SJAI is the Data Controller under the GDPR Policy and is therefore ultimately responsible for the implementation, in order to handle day-to-day matters, the organisation has appointed a Data Protection Officer (DPO) and a Data Information Officer (DIO) to assist the organisation and its members with compliance with the GDPR Policy.

Each Superintendent, Officer & Member in Charge (MIC) must ensure that the DPO is informed of any changes in uses of personal data that might affect SJAI's compliance with the GDPR Policy.



Patient data is an important element of the GDPR policy and all members must be fully aware of the responsibilities in this matter and how they receive and store patient data. Please make sure to adhere to the GDPR policy at all times when handling patient data.

## **6. Procedures and Guidelines**

This policy supports the provision of a structure to assist in the organisation's compliance with the GDPR Policy, providing guidelines to comply with GDPR and support in the event of a data breach.

## **7. Status of this Policy**

This policy has been approved by the Commissioner and applies to all members of the organisation. All members of SJA must read, understand and adhere to this policy.

Any breach of this policy will be taken seriously and may result in disciplinary proceedings.

Any member of the organisation who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the SJA Data Protection Officer immediately, email [dpo@stjohn.ie](mailto:dpo@stjohn.ie).

## **8. Review**

This Policy will be reviewed in light of any legislative or other relevant indicators in line with the General Data Protection Policy Regulation 2018 as set out by the Data Protection Commission.