Data Protection Policy in line with GDPR

Dun Laoghaire Rathdown
Outreach Project

Last Review date: 16 October 2020

Revision date: September 2022

1.Responsibility for approval of policy	Governance & Human Resources Subcommittee
2.Responsibility for implementation	Manager
3.Responsibility for ensuring review	Manager
4. Version	V1OCTAC2020

Policy Statement

1.1. Dun Laoghaire Rathdown Outreach Project (DROP) recognises its responsibilities as a data controller under General Data Protection Regulations. DROP works to ensure data is processed in line with statutory requirements. The organization is committed to processing data in a manner consistent with the issued guidelines of the Data Protection Commissioner.

2. Purpose

2.1. To set out DROP's processes and procedures in respect of the General Data Protection Regulations (GDPR).

2.2. To provide a framework within which data protection can be managed, such that DROP is compliant with its statutory obligations

3. Glossary of Terms and Definitions

3.1. ***Data*** means information in a form which can be processed. It includes both automated (computerised) and manual data

3.2. ***Processing*** means performing any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment

3.3. ***Personal Data*** means data that relates to or can identify a living person, either by itself or together with other available information. Examples of personal data include a person's name, phone number, bank details and medical history.

3.4. ***Special categories of data*** *(which can only be processed under special circumstances as outlined in Article 9 of the Regulations)* relates to specific categories of data defined as data relating to a person's race or ethnic origins; political opinions; religious or philosophical beliefs; membership of a trade union; physical or mental health; sexual life and/or sexual orientation; criminal convictions or the alleged commission of an offence and genetic or biometric data.

3.5. ***Data Subject*** is an individual who is the subject of personal data ie Service User or Staff Member.

3.6. ***Data Controllers*** are the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data; where the purposes and means of such processing are determined by law.

3.7. ***Data Processor*** is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4. Scope

4.1 This policy applies to all personal data including special categories of data created or received in the course of DROP's business in all formats and of any age. It applies to all locations where personal data is held by DROP (including remote access to data) and is concerned with the responsibilities of DROP as a data controller. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone. It applies to all data in the organisation and to all staff members, volunteers and student placements who have access to data.

4.2 This policy should be read in conjunction with DROP's

5. Legislation and relevant documents

5.1 The Data Protection Act 1988

5.2 The Data Protection (Amendment) Act 2003

5.3 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) & Data Protection Act 2018

5.4. The Freedom of Information Act 1997
5.5. The Freedom of Information (Amendment) Act 2003
5.6. National Protocols and Common Assessment Guidelines to accompany the National Drugs Rehabilitation Framework
5.7. DROP Service User Confidentiality Policy
5.8. DROP Case Notes, Written Records & Correspondence Policy

6. Principles

6.1 Principles are an important part of data protection law, and are, in fact, at the core of the General Data Protection Regulations (GDPR). DROP undertakes to perform it responsibilities under the legislation in accordance with Article 5 of the GDPR as follows:

6.1.1 Obtain and process information lawfully, fairly and in a transparent manner DROP obtains and processes personal data fairly and in accordance with its statutory and other legal obligations

6.1.2 Keep it only for one or more specified, explicit and lawful purposes DROP keeps personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner that is compatible with these purposes

6.1.3 Use and disclosure only in ways compatible with these purposes DROP only uses and discloses personal data in circumstances that are necessary for the purposes for which it collects and keeps the data.

6.1.4 Keep it safe and secure DROP takes appropriate security measures against unauthorized access to, or alteration, disclosure, or destruction of data and against accidental loss or destruction

6.1.5 Keep it accurate, complete and up to date DROP operates procedures that ensure high levels of data accuracy, completeness and consistency

6.1.6 Ensure it is adequate, relevant, and not excessive Personal data held by DROP are adequate, relevant and not excessive in data retention terms

6.1.7 Retain for no longer than is necessary DROP has a set guidelines, contained within this policy regarding retention periods for personal data

7. Lawfulness of Processing

7.1 Each processing operation involving personal data needs to be based on one or more lawful basis. There are six available bases for processing personal data under Article 6. It is important to note that no single basis is more important than the others but more so the purpose and relationship to the data subject will determine the lawful basis for processing personal data.

The lawful basis for DROP are:

- **Consent:** DROP has an individual's freely given, specific, informed and unambiguous consent and indication of the data subject's wishes
- **Contract:** the processing is necessary for a contract DROP has with the data subject, or because they have asked DROP to take specific steps before entering into contract
- **Legal obligation:** the processing is necessary for DROP to comply with the law (not including contractual obligations)
- **Vital interests:** the processing is necessary in the protection of the data subject
- **Legitimate interest:** the processing is necessary for DROP's legitimate interests or the legitimate interest of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

DROP will decide which lawful basis applies depending on the specific purposes and the context of the processing. More than one basis may apply, however no one basis should be viewed as being better, safer or more important than the others; there are no hierarchy in order within GDPR.

8. Rights of Data Subjects

DROP's Service User Privacy Statement, which highlights the rights of the data subject is publically displayed both within the premises at 45 Upper Georges Street and on the organisation's website. Individuals have the following rights over the way DROP processes their personal data:

- **Right to access by the Data Subject** Individuals have the right to request a copy of their personal data DROP is processing about them and to exercise that right easily and at reasonable intervals. DROP has procedures in place to ensure that data subjects can exercise their rights under GDPR.
- **Right to rectification** individuals have the right to have their personal data deleted where DROP no longer has any justification for retaining it, subject to legal obligations or exemptions such as the use of pseudonymised data for statistical recording
- **Right to restriction of processing** individuals have the right to request the restriction or suppression of their personal data processing. This is not an absolute right and only applies in certain circumstances. When processing is restricted, DROP is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and DROP must respond within one calendar month.
- **Right to data portability** where it is technically feasible, individuals have the right to have a readily accessible machine readable copy of their personal data transferred or moved to another data controller where DROP are processing their data based on their consent and if that processing is carried out by automated means.
- **Right to Object** Individuals have the right to object to processing or restrict the processing of their personal data if:
  - ✓ The processing is based on public interest; or in order to pursue a legitimate interest of the controller or third party
  - ✓ The personal data was processed unlawfully
  - ✓ The personal data cannot be deleted in order to comply with a legal obligation
- **Right not to be subject to automated individual decision-making, including profiling** in certain circumstances individuals can object to profiling and automated decision making

9. Roles and Responsibilities

9.1 The Manager, as the designated Data Protection Officer, is the person with responsibility for data protection issues in the organisation and is responsible for:

9.1.1 addressing all queries in relation to data protection

9.1.2 ensuring that this policy is kept up to date in line with current legislation and best practice

9.1.3 overall implementation of this policy

9.2 Line managers are responsible for ensuring that staff members have read, understood and signed off on this policy, and other relevant policy documents, such as those on confidentiality. Record keeping and data protection requirements and responsibilities will form part of the induction process for new staff.

9.3 All staff members are responsible for ensuring that the management of personal data in the organisation is consistent with the practices outlined in this policy. All staff members should report any data breaches to the Manager immediately.

10 Storing Manual Data

10.1 Any manual data kept by the organisation should be kept in a manner consistent with good data retention:

10.1.1 All personal data should be kept in a locked filing cabinet, with the key being accessible only to relevant staff members

10.1.2 All records should be written legibly and indelibly. Records should be clear, unambiguous and accurate including the date (Day/Month/Year), and the printed name and signature of the person completing the record.

10.1.3 Alterations are made by scoring out with a single line followed by the initialled and dated correct entry. The use of correction fluid such as 'Tipp-ex' is not permitted.

10.1.4 Records are not to include jargon, subjective statements or abbreviations other than those in common organisational use. All records should be written in a way that is easy to understand

10.1.5 Records must be objective and factual and describe what is observed. If for some reason a more subjective statement needs to be made, the recorder should acknowledge this as a subjective opinion.

10.1.6 Records should include only essential and relevant details.

11 **Storing Automated Data**

11.1 The principles for manual data also apply to automated data. In addition:

11.1.1 Staff must ensure that computerised records are not left unattended, and that all computerised systems are logged off or locked appropriately.

9.1.2 All computerised systems which hold personal data must be password protected.

9.1.3 Staff should ensure that passwords are kept safe and not shared among colleagues.

11.2 All computerised records must be backed up regularly on an appropriate data storage backup system.

11.3 Personal data must never be downloaded onto an external system. Where it is required to carry personal data outside the organisation staff members need approval from line managers and at all times must be secure and password protected.

12 **Retention and Review of Data**

12.1 Precautions should be taken to protect written copies from damages due to fire and water.

12.2 Precautions should be taken to protect all electronic data from viruses or technical failure.

12.3 Data management systems need to be regularly monitored. The Manager will do spot checks on quality of documentation and record keeping.

12.4 The Manager will do a review every year to ensure that personal data is not being kept for any longer than is needed in line with the below retention period guidelines below. In the event of unspecified data, a blanket period of six years will apply in respect of retention. Data related to ongoing legal and investigative actions should not be destroyed.

12.5 Care should be taken to ensure that data are disposed of correctly and securely. All documents which contain personal information must be shredded.

12.6 Retention period guideline table:

Type of Data	**Lawful Purpose**	**Retention Period**
Employee Applications and CVs	Legal Obligation	1 Year for unsuccessful candidates and for the duration of employment plus 6 years from the date of termination of employment
Employee offer letters and other documentation regarding the hiring, promotion, demotion, transfer, termination or selection for training	Contract	6 years from date of making record or action involved
Records relating to background checks on employees	Contract	6 years from when the background check was conducted

Employee contracts; employment and termination agreements	Contract	6 years from the date of contract expiry or termination of agreement
Employee records with information on pay rate or weekly compensation	Contract, Consent	3 Years
Job descriptions, performance goals and reviews	Legal obligation, contract	For the duration of employment plus 6 years from the date of termination of employment
Salary Schedules & ranges for each job description	Legitimate interest, legal obligation	2 years
Personnel Records	Contract, Legal obligation	6 years after employment ceases
Tax Forms/Records	Legal Obligation	6 Years following date of hire
Records relating to workplace accidents	Legitimate Interest, Legal Obligation	6 years following the end of the calendar year that the records cover
Pension Records	Legitimate Interest, Legal obligation	Permanent
Details that include PPSNs, bank details	Consent, vital interest	3 years from end of contract
Payroll registers	Legitimate interest, legal obligation	7 years
Accounting Records	Legitimate interest, legal obligation	7 years
Statutory Maternity and Paternity Records	Contract, legal obligation	3 years after the end of the tax year in which the maternity period ends
Statutory Sick Leave records	Contract, legal obligation	3 years after the end of the tax year in which the sick leave period ends
Holidays, public holidays, and rest periods	Contract, legal obligation	3 years after the end of the tax year in which the holiday period ends
Service User contact details, correspondence and record keeping	Legitimate interest	For duration of service delivery and 3 years following end of service engagement
Participant CE records	Contract	6 years following termination of contract
Redundancy details	Legal Obligation	6 years after employment ceases
Time cards	Legal Obligation	3 years after audit
Trade Union Agreement		10 years after ceasing to be effective
Articles of Incorporation and companies seal	Legal obligation, legitimate interest	Permanent
Annual Corporate filings and reports to the attorney general	Legal obligation, legitimate interest	Permanent
Board policies, resolutions, meeting minutes, AGM meetings & Committee meetings	Legal obligation, legitimate interest	Permanent
Business related email	Legal obligation, legitimate interest	3 years
Fixed Asset records	Legal obligation, legitimate interest	Permanent
Resolutions	Legal obligation,	Permanent

	legitimate interest	
Insurance contracts and policies, insurance claims and applications	Legal obligation	Permanent
Leases and real estate documents	Legal obligation, legitimate interest	Permanent

13 **Access Controls**

13.1 Access to data containing personal information is strictly limited to a "need to know" basis. However, for an effective team response to the needs of Service Users, all staff members involved in an individual's care will "need to know" relevant personal information. This should be explained clearly to Service Users at the outset of their relationship with the organisation.

13.2 Personal data will not be shared between separate teams, unless valid consent exists, or the data is shared in accordance with DROP's Confidentiality policy.

14 **Access for Data Subjects**

14.1 An individual has the right to receive confirmation that their data is being processed and that they have the right to this data.

14.2 We must provide an individual with a copy of the information they request, free of charge, without delay and within one month receipt of an access request form. The data cannot be altered in any way other than mentioned in 14.2.3 below following an access request. On receipt of a data subject access request The Manager should:

- 14.2.1 Contact the data subject, acknowledging receipt of the access request and date that the access was received; confirm the specific information they wish to access. If the person does not wish to disclose their reason for wishing to access their file they are still entitled to full access.
- 14.2.2 Make an appointment to meet the person with their records no later than one month from the date of receipt of access request. Personal information should only be given to the individual concerned (or someone acting on his or her behalf and with their pre-arranged written authority).
- 14.2.3 Collate a copy of the records, removing all information relating to other people. When providing people with access to personal data, care must be taken to ensure the confidentiality of other individuals identified. If other names are mentioned on the documentation, these should be blacked out by a permanent pen.
- 14.2.4 Present the records to the person and offer to take them through it. When necessary, explain how the different records are used and be prepared to answer any questions the person may have.
- 14.2.5 Inform the person that they are entitled to receive copies of files, but that all original documentation will remain on their file in a secured location unless there is a written request for the deletion of all personal data.

14.3 The Manager and Line Managers should ensure that they are familiar with current Data Protection and Freedom of Information Legislation.

15 **Personal Data Security Breaches**

A data security breach is any event that has the potential to affect the confidentiality, integrity or availability of data held by DROP in any format. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Under the GDPR, where DROP is in control of why and how personal data sets are processed, as data controllers we are required to report relevant personal data breaches concerning those data sets to the Data Protection Commission within 72 hours of becoming

aware of the breach. This reporting is done through the manager as the Data Protection Officer. For further details please review DROP's Data Breach Procedure which should be read in conjunction with this policy.

16 **Complaints**

16.1 In the event that a Service User or staff member is unhappy with the way they have been treated in respect of the management of your private data, they should be supported to make a complaint, or institute a grievance in line with DROP's Complaints policy.

16.2 Service Users and staff members are also encouraged to contact the Data Protection Commissioner for further information on how to make a complaint to the Office of the Data Protection Commissioner:
http://www.dataprotection.ie
1890 252 231
Info@dataprotection.ie
Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois

16.3 The organisation will publically display this policy and the Reporting a Data Breach Incident Policy & Procedure on our website. This will allow ease of access for data subjects to inform themselves on what they can expect should their data become compromised as a result of a breach.

Appendix 1 – DROP Data Subject Access Request Form

A copy of photographic identification must accompany this request form when submitting to the DPO of DROP. Please note that this request does not incur a fee.

SECTION A – please complete this section completely

Full Name	
Are you a current or Former Service User of DROP (please state which one)	
Are you a current or Former Employee of DROP (please state which one)	
If neither a service user of employee of DROP please state the relationship with the organisation including dates	
Current Address	
Contact Telephone	
Contact Email	

SECTION B – Please complete this section with as much detail as possible

I, _____ wish to have access to personal data that I believe the organisation has processed about me as outlined below.

_____

_____

_____

_____

_____

_____

_____

Signed: _____ Date: _____

Please return this form to:
Anthea Carry, PRIVATE & CONFIDENTIAL, Data Protection Officer, Dun Laoghaire Rathdown Outreach Project, 45 Upper Georges Street, Dun Laoghaire, Co Dublin **or** via email to manager@drop.ie