

COMHAIRLE CHONTAE LAOISE
LAOIS COUNTY COUNCIL



Data Subject Access Request (SAR) Policy
Including
Rectification, Erasure and Restriction of
Data

Version:	Version 1.2
Prepared by:	Irene Delaney
Date:	10 th September 2019
Amended:	11 th February 2020
Details of Amendment	Inclusion of additional text under Part 6
Issued to:	
Agreed by: Management Team on 18th February 2020	
Circulated to:	

Laois County Council reserves the right to amend or revoke policy at any time without notice and in any manner in which the Council sees fit at the absolute discretion of the Council.

TABLE OF CONTENTS

1.	Introduction.....	4
2.	Purpose.....	4
3.	Personal Information.....	4
4.	Right of Access by a Data Subject.....	5
5.	Making a Subject Access Request	5
6.	Subject Access Request - Exemptions and Refusals.....	6
7.	Right to Rectification of Personal Data.....	9
8.	Right of Erasure of Personal Data.....	9
9.	Right of Restriction of Personal Data.....	10
10.	Right to Object.....	11
11.	Right to Data Portability.....	11
12.	Rights relating to Automated Decision-making including profiling...	12
13.	Data Transfers to External Persons/Bodies or Third Party Processers	12
14.	Complaints to the Office of the Data Protection Commission.....	13

Appendix 1 Glossary of Terms

1. Introduction

Data Protection is the safeguarding of the privacy rights of individuals (Data Subjects) in relation to the processing of personal data in paper and electronic format. The Data Protection Acts 1988 to 2018 and the General Data Protection Regulation (GDPR), effective from 25th May 2018, lay down strict rules about the way in which personal data and special categories of data are collected, processed, stored, disclosed and destroyed.

The legislation also gives Data Subjects the right to access their personal data on request and have their personal data amended if found to be incorrect.

As a Data Controller and processor of personal information, Laois County Council (the Council) complies with the basic principles of the GDPR to make sure that personal data is:

- Collected and processed lawfully, fairly and in a transparent manner
- Processed for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and up to date
- Retained for no longer than is necessary
- Safe and secure.

A glossary of terms used in this policy and other related policies is available in Appendix 1 of the Council's Data Protection Policy.

2. Purpose

As Laois County Council processes personal information regarding Data Subjects, it is legally obligated to provide any information (with limited exceptions) retained in relation to that Data Subject which is kept on computer or in any manual filing system on receipt of a Subject Access Request (SAR) from them.

This document outlines the Council's policy for responding to Subject Access Requests for personal data and details the responsibilities of the Council and the rights of the individual. It also outlines the process for Data Subjects when making a Subject Access Request which may include CCTV recordings and footage.

3. Personal Information

Personal information is defined, in the GDPR, as

“Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

4. Right of Access by the Data Subject

The Data Subject has the right to obtain from Laois County Council confirmation as to whether or not personal data concerning him or her is being processed, together with the following information:

- the purposes and legal basis of the processing,
- the categories of personal data concerned,
- the recipients or categories of recipient to whom the personal data have been or will be disclosed; in particular, recipients in third countries or international organizations,
- where possible, the retention period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,
- the existence of the right to request from the Council: rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing,
- the right to lodge a complaint with the Office of the Data Protection Commission,
- where the personal data is not collected from the Data Subject, any available information as to its source,
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The GDPR states that the right to obtain a copy of your personal data must not adversely affect the rights and freedoms of others. This means that the right cannot be used to access the personal data of other persons, i.e. third parties.

There are also a number of other restrictions to the right of access, provided for by sections 56 - 61 of the Data Protection Act 2018.

5. Making a Subject Access Request

A Subject Access Request may be made in writing or electronically **by e-mail** to the:

Data Protection Officer,
Laois County Council,
County Hall,
Portlaoise,
Co. Laois. ;

Email: dataprotection@laois.ie

Telephone: 057 8664095.

When a request is made electronically, the response will be provided in a commonly used electronic format unless otherwise requested in writing. Usually this means that a photocopy or printout of the personal data will be provided.

Requestors must provide the identification outlined on the Subject Access Request (SAR) form at Appendix 2 to ensure the information is only given to the person entitled to it.

If there is insufficient information provided to process the SAR, the Council will contact the Data Subject for further specific details or clarifications.

The request must also not be excessive or disproportionate.

While the Council will provide the information requested free of charge, further copies requested may incur a charge to cover administrative costs. The Council aims to provide the requested information as soon as possible, but within a maximum of one month from the date the request is received.

However, where the retrieval or provision of information is particularly complex or subject to a valid delay, the period may be extended by a further two months and the Data Subject will be informed in writing as to why the extension is necessary.

6. Subject Access Request - Exemptions and Refusals

Data Protection legislation and the GDPR contain certain exemptions from the requirement to provide personal information. If one or more of these exemptions apply to a request, the Council will inform the Data Subject at the earliest convenience, or at the latest, within one month of receipt of the request. These exemptions are set out in Section 59, 60 and 61 of the Data Protection Act 2018 and gives further effect to Article 23 of the GDPR to restrict the rights afforded by the GDPR under Articles 12 - 22 and Article 34.

The exemptions also include where the request would involve disproportionate effort or is considered to be unfounded or excessive.

In this regard, Laois County Council may be exempt from providing you with your personal data if a restriction of your right of access is necessary:

- For the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- For the administration of any tax, duty or other money due or owing to the State or a local authority
- In contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out of court procedure.
- For the enforcement of civil law claims, including matters relating to any liability of an organization in respect of damages, compensation or other liabilities or debts related to the claims or
- For the purpose of estimating the amount of the liability or an organization on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation in any case in which the application of those rights or obligations would be likely to prejudice the interests of the organization in relation to the claim,
- To safeguard Cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State.

Laois County Council will not normally disclose the following types of information in response to a Subject Access Request:

- Information about other people

A Subject Access Request may cover information which relates to one or more people other than the Data Subject. The information about other people may be personal data about that person to which the usual data protection rules under the Acts, including the restrictions on disclosure apply. In such circumstances the Council will not grant access to the information in question unless the other person has consented to the disclosure of their data to the Data Subject.

- Information given in confidence

Where the Council holds personal data about a Data Subject in the form of an opinion given in confidence and on the understanding that it would be treated as confidential, the Council will not be required to disclose such opinions in response to a Subject Access Request.

➤ Repeat Requests

The Data Protection Acts provide an exception for repeat requests where an identical or similar request has been complied with in relation to the same Data Subject within a reasonable prior period. Laois County Council will consider that if a further request is made within a period of six months of the original request and where there has been no significant change in the personal data held in relation to the individual, it will be treated as a repeat request. Accordingly where personal data has recently been provided to the Data Subject or his/her legal representative, the Council will not normally provide a further copy of the same data in response to subsequent a Subject Access Request.

➤ Reasons for Refusal

When Laois County Council refuses a Subject Access Request, it will do so in writing and will set out the reasons for refusal. Any person who is not satisfied with the response of the Council has the right to make a complaint to the Office of the Data Protection Commission.

The Council may also refuse a Subject Access Request where the identity of the Data Subject cannot be verified, or where requests are unfounded or excessive.

Data Subject Access rights as set out above do not apply to:

- (a) Personal data processed for the purpose of seeking, receiving or giving of legal advice,
- (b) Personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings, including personal data consisting of communications between a client and his or her legal advisers or between advisers or
- (c) Where the exercise of such rights or performance of such obligations would constitute a contempt of court.
- (d) The Data Protection (Access Modification) (Health) Regulations 1989 (S. I. No. 82 of 1989) and the Data Protection (Access Modification) (Social Work) Regulations 1989 (S. I. No. 83/1989) provide that health data and data obtained during the course of carrying out social work relating to an individual should not be made available to the individual in response to a Data Subject Access Request if it would be likely to cause serious harm to the physical or mental health of a Data Subject. In the event that these Regulations apply, the data in question will not be provided to the Data Subject but will however be furnished to the Data Subject's own medical practitioner.

All requests will be channeled through the Data Protection Officer who will maintain a Register of all requests received. An acknowledgement will issue within 7 days and the request will be referred by the Data Protection Officer to the relevant Department(s)/Data Controller for a response within one month from the date of receipt of the request. The Data Protection Officer will issue the decision. However, this period can be extended where the request is complex and the Data Subject will be informed why the extension is necessary.

7. Right to Rectification of Personal Data

The legislation also includes an individual's right to have inaccurate or incomplete data rectified. If your personal data is inaccurate, you have the right to have the data rectified by the Controller, without undue delay. If your personal data is incomplete, you have the right to have data completed, including by means of providing supplementary information.

The Council will respond within a month from the date the request was received. However, this period can be extended where the request is complex and the Data Subject will be informed why the extension is necessary.

8. Right to Erasure of Personal Data (Right to be forgotten)

Data Subjects have the right to have their personal data erased if:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the Data Subject withdraws consent on which the processing is based and there is no other lawful basis for processing the data,
- the Data Subject objects on the basis that there is no overriding legitimate basis for continuing the processing
- Where personal data are being processed for direct marketing purposes
- the personal data has been unlawfully processed
- the personal data must be erased for compliance with a legal obligation

If personal data has been disclosed to others the Council will inform each recipient of the erasure unless this proves impossible or involves disproportionate effort. If asked to, the Council will inform Data Subjects about these recipients. The Council will also take reasonable steps to inform other controllers who are processing personal data that the Data Subject has requested the erasure by them of any links to or copies of the data. (Reasonable steps mean taking account of available technology and the cost of implementation including technical measures.)

The right of erasure does not apply if processing is necessary for the following reasons:

- For exercising the right of freedom of expression and information
- For compliance with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as erasure is likely to render impossible or seriously impair the achievement of the objectives of that archiving
- For the establishment, exercise or defence of legal claims.

The right of erasure is also restricted in certain circumstances under the Data Protection Act 2018.

The Council will respond within a month from the date the request was received. However, this period can be extended where the request is complex and the Data Subject will be informed why the extension is necessary.

9. Right to Restriction of Personal Data

Data Subjects have a limited right of restriction of processing of their personal data by a Data Controller. When processing is restricted, the Council will store the personal data, but not use it. Other processing actions such as deletion will require the consent of the Data Subject.

The right to restrict processing applies in the following circumstances:

- The Data Subject contests the accuracy of their personal data and the Data Controller is verifying the accuracy of the data
- The data has been unlawfully processed and the Data Subject opposes erasure and requests restriction instead
- The Council no longer needs the personal data but the Data Subject needs the Council to keep it to establish, exercise or defend a legal claim
- The Data Subject has objected to the processing of their data and the Council is considering whether legitimate grounds override those of the Data Subject.

The Council reserves the right to refuse to comply with a request for restriction where the request is unfounded, excessive or repetitive. If personal data has been disclosed to others the Council will inform each recipient of the restriction unless this proves impossible or involves disproportionate effort. If asked to, the Council will inform Data Subjects about these recipients.

Where a Data Subject has obtained a restriction of processing of their data, the data controller must inform the Data Subject before lifting the restriction.

The Council will respond within a month from the date the request was received. However, this period can be extended where the request is complex and the Data Subject will be informed why the extension is necessary.

10. Right to Object

Data Subjects have the right to object on grounds relating to his or her particular situation to certain types of processing of personal data in particular situations including:

- Processing based on legitimate interests, the performance of a task in the public interest and/or the exercise of official authority.

Data Subjects have a stronger right to object to processing of personal data where the processing relates to direct marketing including profiling.

In cases where processing is based on legitimate interest, the Council must stop processing the personal data unless

- The Council can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims.

In cases where processing of personal data is for direct marketing purposes the Council must stop as soon as an objection is received. There are no exemptions or grounds to refuse.

In cases where processing of personal data is for conducting scientific, historical or statistical research necessary for the performance of a public interest task, the Council is not required to comply with an objection to the processing.

11. Right to Data Portability

A Data Subject may be entitled to obtain personal data in a format that makes it easier to reuse the information in another context, and to transmit this data

to another data controller without hindrance. This is referred to as the right to data portability.

The right to data portability only applies:

- To personal data a Data Subject has provided to the Council
- Where the processing is based on the Data Subject's consent or for the performance of a contract
- When processing is carried out by automated means.

This right only applies to the extent that it does not affect the rights and freedoms of others.

The right allows Data Subjects to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The personal data will be provided in a structured, commonly used and machine-readable format, free of charge and within one month of the request.

12. Rights relating to Automated Decision-Making including profiling

The GDPR includes provisions on:

- Automated individual decision-making (making decisions solely by automated means without any human involvement)
- Profiling (automated processing of personal data to evaluate certain things about an individual).

Profiling can be part of an automated decision-making process. The Council does not currently undertake processing which falls under automated decision-making or profiling.

13. Data Transfer to External persons/Bodies or Third Party Processers

Laois County Council engages a number of Data Processers to process personal data on its behalf. Any transfer of data to a third party which contains personal data must have a formal written contract in place with that Processer which clearly sets out:

1. Their obligations with regard to the personal data.
2. The specific purpose for which the data may be used,
3. Requiring the Processer to process the data in compliance with the Data Protection Acts and the GDPR
4. The method which will be used to dispose of the data.

14. Complaints to Data Protection Commissioner

If a Data Subject is not satisfied with the outcome of a Subject Access Request, they are entitled to make a complaint to the Data Protection Commissioner at:

Postal Address: Data Protection Commissioner,
Canal House,
Station Road,
Portarlinton R32 AP23
Co. Laois.
Telephone: + 353 57 8684800
E-mail info@dataprotection.ie

Appendix 1 - Glossary of Terms

Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Data Subject an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Protection Commission - The "Data Protection Commission" was established by the Data Protection Acts 1988 to 2018 ('the Data Protection Acts'). Under the GDPR and the Data Protection Acts, the Commission is responsible for monitoring the application of the GDPR in order to protect the rights and freedoms of individuals in relation to processing. The tasks of the Commission include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing; handling complaints lodged by Data Subjects; and cooperating with (which includes sharing information with) other data protection authorities in other EU member states.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Personal data: any information relating to an identified or unidentifiable natural person (Data Subject): an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specified to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data: personal data revealing: the racial or ethnic origin of the Data Subject, the political opinions or the religious or philosophical beliefs of the Data Subject, or whether the Data Subject is a member of a trade union, genetic data, biometric data for the purposes of uniquely identifying an individual, data concerning health or personal data concerning an individual's sex life or sexual orientation. The processing of these special categories is prohibited, except in limited circumstances set out in Article 9 of the GDPR.

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 transmitted, stored or otherwise processed. 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. **Examples include** access to personal information by an unauthorised third party; deliberate or accidental action (or inaction) by a controller or processor; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; and loss of availability of personal data.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Processing means 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, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Supervisory authority means an independent public authority which is established by a member state pursuant to Article 51. In the case of Ireland, the supervisory authority is the Office of the Data Protection Commission.