Data Subject Right Request

Version date: March 2020

Next review due: June 2021

Data Subject Right Request

Contents

Lacrosse Scotland, Caledonia House, South Gyle, Edinburgh, EH12 9DQ
w. www.lacrossescotland.com e. admin@lacrossescotland.com
Registered Company SC282483

Data Subject Right Request

FOREWORD

Lacrosse Scotland is committed to complying with data protection law and to respecting the privacy rights of individuals. One of the key areas under the General Data Protection Regulation (GDPR) are the data subject rights, henceforth as **Rights**, where data subjects (individuals to whom the relevant personal data relates) can evoke a greater set of rights against businesses and organisations that process their personal data.

This document sets out procedures that shall be followed in case of data subject executing one of their rights.

References in this document to "us", "we", "ourselves" and "our" are to Lacrosse Scotland, whilst references to "you", "yourself" and "your" are to person dealing with or involved in facilitating data subject right request.

Data subject rights

Under data protection laws data subject have certain rights in relation to their own personal data. In summary these are:

1. The rights to access their personal data, usually referred to as a **subject access request**;
2. The right to have their personal data rectified;
3. The right to have their personal data erased, usually referred to as **the right to be forgotten**;
4. The right to restrict processing of their personal data;
5. The right to object to receiving direct marketing materials;
6. The right to portability of their personal data;
7. The right to object to processing of their personal data; and
8. The right to not be subject to a decision made solely by automated data processing.

Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances.

Data subject right request

If you receive a verbal request in relation to a Right (as per above), or believe you have a verbal request for the exercise of a Right, you should:

1. pass the call or person to your supervisor/manager if possible (unless you are a supervisor/manager). The supervisor/manager should make a written record of all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to our DPO/ Chairperson. If it is not possible to transfer the individual over then make a written record of the request and contact details for individual making the request; and
2. inform our DPO/ Chairperson of the request and pass them any written records relating to the request.

If a letter or fax exercising a Right is received by you then you should:

1. pass the letter to your supervisor/manager;
2. the supervisor/manager must log the receipt of the letter with our DPO/ Chairperson and send a copy of it to them; and
3. our DPO/ Chairperson will then respond to the individual on our behalf.

If an email exercising a Right is received by you then you should:

1. pass the email to your supervisor/manager;
2. the supervisor/manager must log the receipt of the email with our DPO/ Chairperson and send a copy of it to them; and
3. our DPO/ Chairperson will then respond to the individual on our behalf.

Our DPO/ Chairperson will co-ordinate our response which may include written material provided by our external legal advisors. The action taken will depend upon the nature of the request and the Right. DPO/

Chairperson will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from our DPO/ Chairperson should suffice in most cases.

Our DPO/ Chairperson will inform the relevant management line of any action that must be taken to legally comply with any exercise of rights. Our DPO/ Chairperson will also co-ordinate any additional activity required to meet the exercise of any of the Rights.

The manager/senior manager who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

Our DPO/ Chairperson reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by our external legal advisors.

How to locate information for data subject right requests and requests for the right to be forgotten

If you are responsible for carrying out or co-ordinating any searches for personal data then this section will assist you in how you should approach carrying out the searches.

The personal data we need to provide in response to a subject access request, "right to be forgotten" or any other exercise of data subject rights may be located in several filing and/or network systems, so it is important to identify at the outset the type of information requested to enable a focused search.

However you should note that the individual is not obliged to clarify the scope of what we will need to search for, so whilst we can ask, we may not receive a useful clarification or any response at all. In this case we still have to comply with the original request.

If the data subject is our member - the request should be forwarded on to our data processor (membership database provider), whom will follow their procedures to execute the data subject right.

Despite the above, depending on the type of information requested, you may need to search all or some of the following:

1. electronic systems (e.g. office databases, networked and non-networked computers, servers, member records, human resources records system, email data, CCTV);
2. manual/paper filing systems (but only if they are 'structured filing systems', on which see below); and
3. any other data systems held externally by our data processors.

If you are not authorised to access the relevant system or files that need to be searched, then you will not be able to carry out the search in those systems or files. In this case you will need to delegate those aspects of the search to a person who is authorised to access the relevant system or files.

You should conduct a reasonable search of the relevant systems using the individual's name, employee or membership number, address, national insurance number, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different, and you should check with our DPO/ Chairperson before commencing any search.

If information is not part of a structured filing system, it does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

To be a structured filing system, the system must:

1. contain information relating in some way to individuals. Usually, there would be more than one file in the system or a group of information referenced by a common theme (e.g. an absence spreadsheet).

The files need not be located in the same geographical location, but could be dispersed over different locations;

2. be structured by reference to individuals (e.g. by name or employee or account number) or by reference to information relating to individuals (e.g. type of job or location, address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held; and
3. be structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced so as to easily indicate whether and where in the file data about the individual is located.

Therefore, a structured filing system which is subject to the data protection laws must have an external and internal structure which allows personal data about an individual to be located relatively easily without having to conduct a manual search of the entire file. If you have to thumb through the whole file to find specific information, the file is not a structured filing system.

It might help to apply the 'temp test' to determine if a system is a relevant filing system. Ask yourself if a temp with no specialist knowledge of our internal processes and procedures could, if asked to retrieve information about a specified individual, identify that the system might hold such information and where in that system the information would be. If so it will be a structured filing system.

You should liaise with our DPO/ Chairperson in relation to the searches to be carried out. Usually you will be required to carry out searches of any physical files or records.

Right of Access

This paragraph contains the specific procedure to be followed where an individual exercises their right of access (also known as a data subject access request). The request need not refer to the Right, for instance, it might simply request 'a copy of all the information that you have about me'.

There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

The data protection laws gives individuals the right to obtain:

1. confirmation that their personal data is being processed;
2. access to their personal data; and
3. access to other supplementary information.

The individual is entitled to receive a description of the following:

1. the purposes for which we process the data;
2. the categories of personal data we process about them;
3. the recipients to whom we may disclose the data;
4. the duration for which the personal data may be stored;
5. the rights of the data subject under the data protection laws;
6. any information available regarding the source of the data were not collected from the data subject direct;
7. the right of the data subject to make a complaint to the supervisory authority for data protection;
8. the logic behind any automated decision we have taken about him or her (see below), the significance and consequences of this automated processing.

Plus we must also provide the information constituting the individual's personal data which is within the scope of their request. We must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically we can, unless the data subject specifies otherwise, also provide the information in electronic form.

If the individual requests details on automatic decisions made about him, we must provide appropriate information, but in a format that does not compromise any trade secrets.

We may:

1. ask for additional information to confirm the identity of the individual making the request;
2. request that the scope of the request is narrowed in order to ease the searches to be undertaken (but the individual does not have to agree to such a request from us); and
3. where requests are manifestly unfounded or excessive, because they are repetitive: (a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or (b) or refuse to respond. Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Where we process a large quantity of information about an individual, the data protection laws permit us to ask the individual to specify the information the request relates to. The legislation does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

We should verify the identity of the person making the request, using "reasonable means" if we are not sure about their identity.

Redactions

1.1. Where we are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. They are not entitled to see information which relates to other individuals or to other people, e.g. to a company.

1.2. In these cases we would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

Disclosing personal data relating to other individuals

Sometimes information that is determined to be personal data about one individual might include information identifying personal data about another person (e.g. an email between two people might contain personal information relating to both the sender and the recipient) and in some cases it is not possible to redact the information about the other person. There are additional steps to consider in relation to whether we disclose this information.

We must consider whether the other person has consented to the disclosure of their information or whether it would be reasonable to comply with the request without the other person's consent.

Where the other person has consented, their information can be disclosed.

Where the other person has not consented, whether it would be reasonable to disclose that person's information will depend upon all the circumstances and you must assess these on a case by case basis.

We would consider whether:

1. The other person has refused their consent;
2. The other person's consent cannot be obtained (e.g. because they are incapable of giving it due to illness or incapacity);
3. Asking for consent might reveal the identity of the individual making the request;
4. We owe the other person a duty of confidentiality;
5. We have taken any steps to obtain the consent of the other person;
6. The other person is a recipient or one of a class of recipients who might act on the data to the individual's disadvantage;

7. The other person is the source of the information;
8. The information is generally known by the individual; and
9. The individual has a legitimate interest in the disclosure of the other person's information which they have made known to us.

If you decide that the other person's information should be withheld (usually it should be), we still have to provide as much of the information requested as we can. Therefore, we should protect the other person's identity by redacting as much of this information and other identifiable particulars.

Always keep a record of what you have decided to do and your reasons for doing it.

Exemptions to the right of subject access

In certain circumstances we might be exempt from providing personal data in response to a subject access request. These exemptions are described below and should only be applied on a case by case basis after a careful consideration of all the facts.

Crime detection and prevention

We do not have to disclose personal data that we process for the purposes of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting any tax or duty, if and to the extent that giving subject access would be likely to prejudice any of these purposes.

Confidential references

We do not have to disclose certain confidential references that we have given to third parties, but might have to disclose confidential references that we receive from third parties. Bear in mind that references received from third parties may contain personal data of another person, so you must consider the rules regarding disclosure of other party's personal data set out above.

Legal professional privilege

We do not have to disclose any personal data that is legally privileged. The following would be legally privileged:

1. confidential communications between us and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice; and
2. confidential communications between us or our lawyers and a third party (e.g. a witness) where the dominant purpose of the communication is to give or seek legal advice in respect of current or potential legal proceedings. This claim to legal privilege would end as soon as the case has been decided and, at that moment, the documents in the file might be disclosable if a subject access request is received.

Management forecasting

We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any organisation or any other activity (e.g. staff relocations, redundancies, succession planning, promotions and demotions) if and to the extent that disclosing the personal data would be likely to prejudice the conduct of that organisation or activity.

Negotiations

We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

In any cases of doubt then speak to our DPO/ Chair of Charity Trustees and it may be that external legal advice is necessary in relation to whether or not an exemption can be applied in a particular case.

Right to Erasure, also known as "the right to be forgotten"

The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

1. where their personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
2. when the individual withdraws consent (but only to the extent that consent is the only basis for processing their personal data);
3. when the individual objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing;
4. where their personal data was unlawfully processed;
5. where their personal data has to be erased in order to comply with a legal obligation; and
6. where their personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request:

1. to exercise the right of freedom of expression and information;
2. to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
3. for public health purposes in the public interest;
4. archiving purposes in the public interest, scientific research historical research or statistical purposes; or
5. the exercise or defence of legal claims.

If we have disclosed the personal data to be erased to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Right to rectification

An individual has the right to ask us to:

1. correct inaccurate personal data;
2. complete information if it is incomplete; and
3. delete personal data which is irrelevant or no longer required for our purposes.

If we have disclosed the personal data in question to third parties, we must inform them of the rectification request where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

If data is factually correct and we are justified in keeping it, i.e. it is relevant to the lawful purpose we are holding it for then we do not have to change or delete it, but the individual may make a request for erasure, i.e. the right to be forgotten, and in that case we would have to analyse the personal data and whether we can retain it based on that Right.

Where we are not taking any action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority (usually the ICO) and to seek a remedy from the Courts.

Right to Restrict Processing

An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

We will be required to restrict the processing of personal data in the following circumstances:

1. where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;
2. where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual;
3. when processing is unlawful and the individual opposes erasure and requests restriction instead; and
4. if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Previously given consent for processing can be revoked at any time by the individual, therefore we cannot justify continued processing of data as a result of a previous consent.

The individual does not have this right if the individual has entered into a contract with us and the processing is necessary for the fulfilment of that contract.

We must inform individuals when we decide to lift a restriction on processing (for example, if an individual contested our right to process their personal data on legitimate interest grounds and we subsequently found that our processing was justified on these grounds).

If we have disclosed the restricted personal data to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

The right to data portability only applies:

1. to personal data an individual has provided to a data controller;
2. where the processing is based on the individual's consent or for the performance of a contract; and
3. when processing is carried out by automated means.

We must provide the personal data in a structured, commonly used and machine- readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

It is not expected that this right will impact upon as we do not process personal data by automated means.

Right to Object

Individuals have the right to object to:

1. processing based on legitimate interests;
2. the performance of a task in the public interest/exercise of official authority (including profiling);
3. direct marketing (including profiling); and
4. processing for purposes of scientific/historical research and statistics.

If we process personal data on the basis of our legitimate interests or the performance of a task in the public interest/exercise of official authority:

1. individuals must have an objection on "grounds relating to his or her particular situation"; and
2. we must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

If we process personal data for direct marketing purposes:

1. we must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse;
2. we must deal with an objection to processing for direct marketing at any time and free of charge; and
3. we must nevertheless comply with the terms of the Privacy and Electronic Communication Regulations and the e-Privacy Regulation which replaces it.

If we process personal data for research purposes:

1. individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes; and
2. If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

If our processing activities fall into any of the above categories and are carried out online, we must offer a way for individuals to object online.

We must inform individuals of their right to object "at the point of first communication" and in our privacy notices. This right must be "explicitly brought to the attention of the data subject and is to be presented clearly and separately from any other information".

Automated decision making and profiling

The privacy legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

We do not currently undertake any automated decision making. We must identify any of our subsequent processing operations that constitute automated decision making.

Individuals have the right not to be subject to a decision when:

1. it is based on automated processing; and
2. it produces a legal effect or a similarly significant effect on the individual.

We must ensure that individuals are able to:

1. obtain human intervention;
2. express their point of view; and
3. obtain an explanation of the decision and challenge it.

The right to obtain human intervention does not apply if the automated decision is:

1. necessary for entering into or performance of a contract between us and the individual;
2. authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or
3. based on explicit consent (but bear in mind that any consent can be withdrawn).

The data protection laws define profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

1. performance at work;
2. economic situation;
3. Health;
4. personal preferences;
5. Reliability;
6. Behaviour;
7. location; or
8. Movements.

When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place. We must:

1. ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;
2. use appropriate mathematical or statistical procedures for the profiling;
3. implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
4. secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes must not concern a child. Automated decisions must not involve or be based on the processing of special categories of data or criminal history records (previously sensitive personal data) unless:

1. we have the explicit consent of the individual; or
2. the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual; and
3. (in each case) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Enforcement

If an individual disagrees that we have properly complied with a Right or we fail to respond they may apply to a Court for an order or complain to the ICO in each case requiring us to properly perform the Right.

If the Court or the ICO agrees with the individual it can:

1. order us to properly carry out the Right and what steps are needed to do this; and
2. order us to notify third parties who we have passed the data onto of the Right;

A court can also award compensation to the individual for any damage they have suffered as a result of our non-compliance. The ICO can also impose a civil fine upon us. These fines can be very substantial.

Deleting personal data in the normal course

We are only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

What we cannot do is amend or delete data because we do not want to supply it or because of the exercise of a Right.