Colleague Guidance – Individual Rights Requests

1) What rights do individuals have under UK law[1]?

The GDPR provides the following rights for individuals:

1. **The right to be informed** (a Privacy Notice)
2. **The right of access** (a Subject Access Request)
3. **The right to rectification** (a request to amend their personal data)
4. **The right to erasure** (a request to have their personal data removed)
5. **The right to restrict processing** (a request to ask us to temporarily cease processing their personal data)
6. **The right to data portability** (a request to have their personal data transferred to another data controller, e.g. a new energy supplier, or children nursery, or co-operative society)
7. **The right to object** (a request to ask us to stop processing their personal data)
8. **Rights in relation to automated decision making and profiling** (i.e. where processing is solely effected by automated means, without any human involvement).

2) Who can exercise these rights?

Any individual whose personal data is collected and processed by the Society e.g. colleagues, customers, members, contractors, directors or third parties, such as suppliers or agency staff.

In certain circumstances, we might receive requests from public bodies such as the Police, HMRC or a Regulator[2] wanting to know what information we hold about an

[1] The General Data Protection Regulation 2016 (GDPR) will continue to apply in the UK until the Brexit process has completed, and likely to continue to apply even after that, embodied in UK legislation. Currently, the GDPR became law in the UK as the Data Protection Act 2018.
[2] For example Ofgem, Ofsted, Ofcom, ABTA etc.

individual – usually to help them with their enquiries or criminal investigations. See below on how to respond to such requests.

3) What do these rights mean, in more detail?

See **Appendix 1**, which contains more detail in relation to each individual right.

4) How will we know, when a request is being made under these rights?

Colleagues must be able to recognise and deal with a request from an individual to exercise their rights under the GDPR, and to ensure requests are dealt with in accordance with the Society's processes. The most common type of request is the Subject Access Request (see more details below), but people may also ask for their personal details to be deleted, or to stop sending them marketing communications.

Requests can be made in writing, including email, and verbally. They don't need to have legal jargon in them to be individual rights requests.

5) What do we do when a request is received?

If you receive a request of any type, whether made by an individual or any public body in relation to the processing of personal data, this needs to be forwarded to your Data Protection Champion (DPC) without delay. You can find a list of the Society's DPCs on Colleagues Connect. If you are unsure, you should contact the Society's DPM[3].

6) How long do we have to comply?

All requests must be dealt with promptly, and at the latest **within 30 days**.

In limited circumstances, the period may be extended by a further two months, where necessary, taking into account the complexity and number of the requests received from the same individual eg. a large number of databases or documents that need to be searched.

In such cases, the Society's DPM, liaising with the relevant DPC, will let the individual know, within one month of receiving their request, explaining why an extension of time is necessary.

7) What about requests made on behalf of the individual?

[3] The GDPR introduced the obligation for certain organisations to formally appoint a Data Protection Officer (DPO). Within the Society, this requirement applies to our Healthcare and Energy businesses. The DPO role is covered by the Society's Data Protection Manager.

Usually, an individual would make a request in respect of their own personal data.

Occasionally, requests are made by people on behalf of others, for example a family member, a solicitor or a carer may log a request on behalf of an individual. In these cases, it is important to make sure the person making the request is authorised by the individual to do so, otherwise we might be disclosing information to someone unlawfully (ie. without their knowledge and consent), which is a breach of the law.

Any such requests should be forwarded to your DPC without delay, and they will decide whether it is a valid request, whether the person making the request has written authority, and whether confirmation of identity or any further validation is required to process the request.

If challenged, you should contact the Society's DPM who, liaising with the relevant DPC, may contact the person making the request to explain why the additional evidence is required to process the request, or whether we are unable to process it altogether.

8) Do all requests need to be complied with?

Yes, but - individual rights are not exercisable in all circumstances. There may be circumstances where the Society can refuse to respond to a request.

Decisions about whether we should refuse to comply with a request must be made by the Society's DPM who will respond to the individual and inform them of their right to complain to the ICO if they aren't happy with the response.

9) Can we charge a fee?

Under the GDPR, an individual will not have to pay a fee to access their personal data (or to exercise any of their other rights). However, the law says we may charge a reasonable fee if, for example, the request for access is clearly unfounded or excessive.

The Society's DPM, liaising with the relevant DPC, will make an assessment and decide, on a case-by-case basis, whether a fee can, or should, be charged.

10) A Subject Access Request has been received: what do we do now?

All Subject Access Requests ("SARs") must be forwarded without delay to your DPC, who will liaise with the Society's DPM as necessary, and if there are any doubts or difficulties in completing the request, the Society's DPM will contact the individual making the request to advise them accordingly.

Particular care must be taken where the information to be provided includes personal data about people other than the individual who has logged the request. The Society has a responsibility to protect all personal data it processes, and must not disclose individuals' personal data in response to a SAR without their consent. For example, it might be necessary, in certain cases, to edit a CCTV footage to digitally mask other people appearing in it before it can be released to the individual who made the request.

11) What about other requests we receive eg. for erasure ("right to be forgotten"), amendment or objection to processing?

Similarly to SARs, when a request is received from an individual exercising their legal rights in relation to their personal data, it must be forwarded to your DPC without delay; they will liaise with the Society's DPM to ensure the request is carried out correctly and in a consistent manner to that of other business groups.

12) We have heard a lot about the "right to be forgotten": when does this right apply?

See **Appendix 1** for further details.

13) Do we need to tell other organisations if we receive a request from an individual exercising their legal rights in respect of their personal data?

Yes, in certain cases - if you have shared someone's personal data with a third party (a data processor), you will need to let them know that a request has been made, as they may need to take action to enable us to respond to the request, for example collating any information they may hold about that person at their end.

Similarly, if any of our third-party processors receives an individual request, they will need to inform the relevant DPC/business group, in order that the request can be actioned without delay.

14) Does the right to data portability apply to us?

Yes - the right to data portability allows individuals to obtain, and reuse, their personal data for their own purposes across different services.

With the Society, the right might be exercised, for example, by Energy customers switching to a different energy provider, by members taking up membership with a different co-operative society, by Healthcare customers changing their GP, or by parents moving their children to a different childcare provider.

For more information, see **Appendix 1**.

15) How do we comply with a data portability request?

As per other types of requests, you must firstly forward the request to your DPC, who will liaise with the Society's DPM to assess the validity and feasibility of the request, and carry it out as necessary.

You must ensure your business group has the technical capability to provide the requested personal data in a structured, commonly used and **machine-readable form**. Open formats include, for example, CSV files. Machine-readable means that the information is structured so that software can extract specific elements of the data, enabling the receiving organisation to re-use the data (eg. Word, Excel, etc. A PDF document, or a screenshot, would not be valid formats).

An individual is free to choose whether the requested personal data should be sent back to them, or transmitted directly to another organisation (if technically feasible).

16) What does automated decision-making mean, and do we need to worry about profiling?

Automated individual decision-making means making a decision solely by automated means, without any human involvement eg. automated selection of candidates based on set word criteria in job applications.

It includes profiling, which relates to the automated processing of personal data to evaluate certain things about an individual eg. a database of customers which automatically extracts data based on postcode information to target defined groups of customers with direct marketing.

This type of processing can only be carried out if any of the following applies:

- it is necessary for the entry into or performance of a contract
- it is authorised by law
- it is based on the individual's explicit consent.

The Society does not routinely carry out automated processing or profiling of personal data, however there may be instances when some profiling is carried out, but it would always be supported and complemented by a fair amount of human intervention from colleagues, for example in a direct marketing promotional campaign targeting customers living in a set geographical area, or from a specific age/gender group.

17) Need more information?

The Society has put in place guidance for colleagues and policies on data protection matters, which are available on Colleagues Connect.

If you need more information, or have any questions, you should contact in the first instance **your business group's DPC** (the list of the Society's DPCs is available on Colleagues Connect).

Alternatively, you can also contact the **Society's DPM**, based at Co-operative House, The Midcounties Co-operative, Warwick Technology Park, Warwick CV34 6DA) – Andrew Stride, Head of Legal, Secretariat Group, Tel: 01926 516 064 (direct); Email: data-protection@midcounties.coop.

- **To access Colleagues Connect**: https://colleaguesconnect.midcounties.coop/working-here/data-protection/
- **Appendix 1** contains more details about each individual right.
- **Appendix 2** contains a checklist, to help you assess your business group's readiness to comply with individual rights' requests, in line with the Society's guidance.

APPENDIX 1

1. The right to be informed

The DPA says that, in order to comply with the first Principle (processing personal data lawfully, fairly and in a transparent manner), the Society must provide individuals with certain prescribed information at the point when their personal data is collected. This is known as a privacy notice, or privacy policy.

The information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

The Society's privacy notices/policies contain the requisite information.

2. The right of access

Individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other information, such as that which should be provided in a privacy notice.

The Society must verify the identity of the person making the request.

A copy of the information should be provided free of charge. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Information must be provided without delay and at the latest within 30 days. The period for compliance may be extended by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request, and explain why the extension is necessary.

If the request is made electronically, the information should be provided in a commonly used electronic format; likewise, if the request is made by post, the information should be provided in hard copies.

Where we process a large quantity of information about an individual, the DPA permits us to ask the individual to specify the information the request relates to. The DPA does not include 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.

3. The right to rectification

The DPA includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification either verbally or in writing, and we have one calendar month to respond to a request. In certain circumstances, we may refuse a request for rectification.

This right is closely linked to the Society's obligations under the accuracy principle of the DPA.

4. The right to erasure (also known as 'the right to be forgotten')

Individuals can make a request for erasure either verbally or in writing, and we have one month to respond to a request.

This right is not absolute, and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- their personal data is no longer necessary for the purpose which we originally collected or processed it
- we are relying on consent as our lawful basis for holding the data, and the individual has withdrawn their consent
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and we have no overriding legitimate interest to continue the processing
- we are processing the personal data for direct marketing purposes, and the individual objects to that processing
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement).

The right to erasure does not apply if processing data is necessary for certain reasons, for example to comply with a legal obligation, in relation to legal claims or for health purposes.

5. The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is a temporary alternative to requesting the permanent erasure of their data, and may be requested because they have issues with the content of the information we hold, or with the way we have processed their data.

This is not an absolute right, and only applies in certain circumstances.

When processing is restricted, we are permitted to store the personal data, but not use it.

An individual can make a request for restriction either verbally or in writing, and we have one calendar month to respond to a request.

We can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

6. The right to data portability

The right to data portability allows individuals to request that their personal data be transferred to another person, or organisation.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means (i.e. does not apply to paper file systems).

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 (for example, Word, Excel, etc. A PDF document, or a screenshot, would not be valid formats). This enables other organisations to use the data.

The information must be provided free of charge.

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.

7. The right to object

Individuals have the right to object to processing in certain situations:

- when processing is based on legitimate interests
- when personal data is used for direct marketing purposes (including profiling).

We must stop processing personal data based on legitimate interests, unless we can demonstrate compelling grounds for the processing, which override the interests, rights and freedoms of the individual.

We must also stop processing personal data for direct marketing purposes, as soon as we receive an objection. There are no exemptions, or grounds to refuse.

8. Rights in relation to automated decision making

The DPA has provisions on data controllers taking significant decisions based solely on automated processing of individuals' personal data. We can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by law; or
- based on the individual's explicit consent.

We must also make sure that:

- We give individuals information about the processing;
- We introduce simple ways for them to request human intervention, or challenge a decision;
- We carry out regular checks, to make sure our systems are working as intended.

APPENDIX 2

Checklist – Assess your business group's readiness to comply with individual rights' requests

☐	We are aware of the different rights that an individual has
☐	We know how to recognise an individual rights' request and understand when these rights apply
☐	We understand how to report individual rights' requests we receive to the Society's DPM
☐	We understand when requests can be refused and are aware of the Society's obligation to explain our decision
☐	We have internal processes in place to ensure that we are ready to respond to a request without undue delay and within one month of receipt
☐	We have appropriate system capability to access, rectify, update, delete and transfer personal data
☐	We understand any relevant third party processor need to be advised when a request is received
☐	We are aware of the time limit for responding to requests and the circumstances when the time limit can be extended