Provincial Grand Lodge of Somerset

Data Protection Act Subject Access Requests (SARs)

The following is provided by way of general advice.

Subject Access Request (SAR)

When a person requests a copy of all their personal data from the Provincial Grand Lodge of Somerset, they are in effect making a Subject Access Request (SAR) under the European Union's Data Protection Regulation (the "GDPR") and enactment within UK Law, which provides rules as to how an SAR must be complied with. As the regulations apply to both the United Grand Lodge of England (UGLE) and the Provincial Grand Lodge of Somerset, both must comply with SAR's and separate requests may be required.

The regulations allow an organisation to charge a maximum £10 Subject Access Fee to process an SAR request. As the Provincial Grand Lodge of Somerset is a not for profit charitable fraternity and thus in order to cover some of the administrative costs, this is the fee which the Provincial Grand Lodge of Somerset charges.

A request for an SAR should be made in writing wherever possible and the deadline for compliance is 30 days commencing from, the later of, receipt of an SAR or receipt of the Subject Access Fee.

(It is important to note that the DPA rules do not apply to individuals collecting information solely for their own domestic and household affairs e.g. an address book or solely for research, journalistic, artistic or literary purposes and also that the subject will not be requesting information under the Freedom of Information Act (FOI) (which they may sometimes believe): the FOI applies to Public Authorities and does not apply to UGLE or the Provincial Grand Lodge of Somerset).

The Provincial Grand Secretary is responsible for receiving and processing all SAR requests.

1. Upon receipt of an SAR request
If a verbal request for an SAR is received, the Provincial Grand Secretary will require this to be submitted in writing (letter by email will suffice) and for the subject to provide any other information in order to verify identity. The initial request will be dealt with as soon as possible and normally within five days of receiving the initial query.

The following example letter can be used in order to respond to a request and which can be amended according to what is required in each circumstance:

Dear (insert name),

Re: Subject Access Request (SAR) – European Union's Data Protection Regulation (the "GDPR") and enactment within UK Law

Further to your request under the Data Protection Act regarding personal data about you held by the Provincial Grand Lodge of Somerset, can you please send us the following:

1. *Your request in writing*
2. *Copies of your passport or photo driving licence; and copy recent utility bill in order to verify your identity;*
3. *The Provincial Grand Lodge of Somerset reserve the right to charge a £10 Subject Access Fee (Please make cheques payable to 'Provincial Grand Lodge of Somerset' and send to the address provided below).*

By way of reassurance, once we have received the fee, we will process your request as soon as possible and in any event, within 30 days thereafter, as required by the GDPR.

Yours sincerely,

2. Responding to an SAR

The 30 day period – including weekends – starts from the SAR is received. The final day of the 30 day period represents the deadline by which time the SAR must be received by the applicant. Allowance must therefore be made for compilation of the reply and delivery delay. Special Delivery 'next day' may be required.

3. Compliance with SAR

For more detailed information/Advice please visit ico.org.uk.

The ICO also operate a helpline which you can use to ask about general information/questions (you do not have to identify yourself or the Provincial Grand Lodge of Somerset). The following is a brief guide only.

(a) What is personal data?

An SAR only applies to 'personal data'. This is any information held about the subject whereby the subject can be identified from the information. Names, addresses or specific roles are obvious ways of identifying individuals but they can also be identified in photos or CCTV images.

(b) What kind of records does data protection apply to?

The rules apply particularly to computer or automated records (including email) but can also apply to manual records which enable information about a particular individual to be easily retrieved e.g. filed by the name or role. Please note the rules only apply to information actually held and about living individuals: it may be that certain information has been destroyed/deleted locally as should be normal practice. Examples of automated records include:

- Computer files - files stored on hard file or floppy discs, CD-ROMs, DVDs, hard disks, back-up files, emails
- Audio/Video - CCTV, webcam images,
- Digitalised images - scanned photos, digital camera

Examples of manual records include:

- Files - on employees, volunteers, non-members
- Index systems - names, addresses, other details
- Microfiche records – containing personal data

Under the rules, an individual is entitled only to their own personal data and not to information relating to other people. Therefore, when disclosing personal data to subjects it is important not to inadvertently disclose personal data about third parties in the process i.e. you have to be careful not to breach the data protection rights of third parties. Information pertaining to third-parties must be withheld, including details of the author.
All papers/documents sent to the applicant will need to be checked very carefully and any personal data relating to third parties 'redacted' i.e. deleted/Crossed out - to the extent that it is not visible to others. Following redaction the original should be photocopied and the checked photocopy sent to the applicant. The original un-redacted copies should be retained. See Annex 1.

It is important to note that whole documents should not be withheld just because they contain the details of third parties. In that instance, these details will need to be redacted so as to ensure that they cannot be identified. However, where even after redaction, the identity of third parties is still ascertainable it may be necessary to withhold the whole document. This decision will need to be taken with great care. If in any doubt, you should check matters with ico.org.uk.

(c) What data can be withheld and how?

There are exemptions to disclosure but, in the main, these are very specific and tend to apply to particular cases e.g. confidentiality of police investigation or HR records. It is quite rare for exemptions to apply more generally and decisions must be made on a carefully considered discretionary basis, which can be justified. Also, when they do apply this does not necessarily mean that a whole document is exempt e.g. the exemption could apply to a part or parts of a document too. Please see the ico.org.uk website for further explanation and to see whether any of these may apply.

Annex 1

Some basic rules to apply when redacting:

1. The information disclosed should relate to the data subject making the request - do not include irrelevant information.

2. Particular care should be taken when redacting to ensure that the personal data of other individuals is not released - that is any data which would allow you to identify the people from the data combined with other information held.

3. The following general rules should be applied – although there may be specific incidents when they would not:

a. redact all names other than that of the person making the request

b. redact job titles

c. redact e-mail addresses

d. redact addresses

e. redact phone numbers

f. redact references to an individual's gender if that would lead to them being identified

g. redact personal descriptions which may lead to a person being identified, so a description of someone as a brown haired man is unlikely to identify someone but a red haired man with a beard may

h. redact any other narrative data that would lead to an individual being identified

i. think about the combination of information sets that taken together would lead to an individual being identified

4. When taking out personal details from email headers, leave in the date and title line unless the title line conflicts with the above.

February 2018