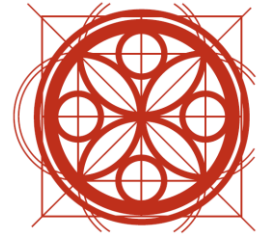




By Appointment To HM The Queen
Building Façade Restoration
and Conservation
PAYE Stonework & Restoration Ltd
London



PAYE

GDPR POLICY STATEMENT

SUBJECT ACCESS REQUEST

A Subject Access Request is a request for personal information that an organisation may hold about an individual. If an individual – or another individual authorised to do so on their behalf – wishes to exercise a subject access right, the request must be made in writing.

Although from time to time an individual may request details of some elements of their personal data held by telephone – formal SARs must be submitted in writing, either electronically, or by post.

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Acts (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- The reasons why their data is being processed;
- The description of the personal data concerning them;
- Anyone who has received or will receive their personal data; and
- Details of the origin of their data if it was not collected from them.
- Erase of personal data

SAR HANDLING – APPOINTMENT OF A DESIGNATED PERSON

In order to ensure SARs are responded to in a timely and effective manner, responsibility for identification and management of all requests will be assigned to a Designated Person (DP). In PAYE the DP is Joanna Curtis. In the event where the DP is unavailable for any extended period of time, the organisation will delegate responsibility to a deputy.

RESPONSE TIME

Under the GDPR, we must respond to SARs **within 30 days of receipt**. This deadline can be extended by a further two months where there are a number of requests or the request is complex, but **you must contact the individual within the initial 30 days of receipt**, explaining why the extension is necessary, and when the information will be made available.

PROVISION OF INFORMATION

Individuals can make a formal SAR electronically/by email or in writing.

When a data subject makes the request by email, the response also should be provided in email format unless otherwise requested by the data subject.

In all cases the **individual's identity must be verified** prior to granting access to information. Where insufficient information is provided to verify the identity of the individual and their right to access the personal data, the individual should be contacted in writing, or by phone if appropriate, to request the additional information necessary.



SAR TRACKING & RESPONSE

- 1) On receipt of an SAR through any of the above channels, the request must be copied and forwarded to the Designated Person, where it will be recorded on file.
- 2) Where staff have personal e-mail accounts where a SAR could be made to, these should be monitored when the member of staff is out of the office to ensure that SARs are dealt with quickly. Remember – we only have up to one month to respond, so we need to ensure the relevant information is collated and returned on time.
- 3) On receipt of the SAR, the Senior Manager or designated person will log the nature of the SAR request and allocate responsibility for preparation and return of the response.
- 4) Where the required information cannot be provided within the designated one-month timeframe, a letter of explanation must be issued with details of the reason for the delay, and confirmation as to the expected date when the information will be supplied.
- 5) On issue of the formal response letter, the date of issue will be logged, and a copy of the material sent stored on file for future reference.

RIGHT TO WITHHOLD PERSONAL DATA

Under the GDPR, organisations can withhold personal data if disclosing it would '*adversely affect the rights and freedoms of others.*' This is not likely to be the case with the majority of SARs being received, but if in doubt, cross check with the Senior Manager of the service, or the Data Protection Officer.

FEES

Under the GDPR, a request for personal information is free unless the request is 'manifestly unfounded or excessive'. In which case the organisation can charge a 'reasonable fee' for multiple requests. This would include both multiple requests, or requests for additional copies of the information.

As with all matters arising with respect to Data Privacy and/or the GDPR, if in doubt with regards to any aspect of a Subject Access Request - refer any questions or concerns to either the Senior Manager or the Designated Person.

ERASE OF DATA

If requested for erase of personal data, any data identifying that individual must be erased permanently from the data base and a copy of receipt sent to the individual confirming their data has been erased.

Request's must be made through SAR by email or writing, verbal communication shall not be accepted.

DATA BREACHES

Under the GDPR if PAYE are subject of a data breach, they must notify the Information Commissioner's Office within 72 hours of the breach.

This can be reported online or either by telephone.

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

The following information need to be given to the ICO:

- Brief description of what has happen
- How did you find out about the breach and how long has it been
- Who has been affected
- What are we doing as a result of the breach



PROCESSING INDIVIDUALS DATA

Individuals data shall not be processed without the consent of the owner, staff's data is only processed when security clearance & training courses are required, unless the DP is required to do so by Union or Member State Law.

MjKember.

Matt Kember
Managing Director

January 2020