Data Subject Access Request Policy

Date - 16 March 2023
Version - 3

Contents

1 Definitions and interpretation

1.1 Definitions

In this Policy:

CWL	Castle Water Limited (registered number SC475583) having its registered office at 1 Boat Brae, Blairgowrie PH10 7BH;
CWL Group	means CWL and each Group Company;
Group Company	means CWL and any of its subsidiaries, holding companies or any subsidiaries of such holding company;

2 Introduction

2.1 The CWL Group holds personal data (or information) about job applicants, employees, clients, customers, suppliers, business contacts and other individuals for a variety of business purposes.

2.2 Under Retained Regulation (EU) 2016/679, UK General Data Protection Regulation (UK GDPR), individuals (known as 'data subjects') have a general right to find out whether we hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that we are undertaking.

2.3 Our data protection officer, Euan Mitchell, General Counsel (euan.mitchell@castlewater.co.uk) is responsible for ensuring:

2.3.1 that all data subject access requests are dealt with in accordance with the UK GDPR and other relevant legislation and guidance; and

2.3.2 that all staff have an understanding of the UK GDPR and other relevant legislation and guidance in relation to data subject access requests and their personal responsibilities in complying with the relevant aspects of the UK GDPR and other relevant legislation and guidance.

2.4 This policy provides guidance for staff members on how data subject access requests should be handled and is intended for internal use. It is not a privacy policy or statement and is not to be made routinely available to third parties.

2.5 This policy applies to all staff but much of it is aimed primarily at those members of staff who are authorised to handle data subject access requests. These sections are identified by the words '(authorised staff)' appearing in the section title. For other staff members, it provides guidance on:

2.5.1 what to do if you receive a data subject access request (see paragraph 3 below); and

2.5.2 how to decide whether a request for information is a data subject access request (see paragraph 2 below).

2.6 Failure to comply with the right of access under the UK GDPR puts both staff and the CWL Group at potentially significant risk, and so the CWL Group takes compliance with this policy very seriously. For further information on the consequences of failure to comply, see paragraph 15 below.

2.7 If you have any questions regarding this policy, please contact the data protection officer on dpo@castlewater.co.uk .

3 How to recognise a data subject access request (all staff)

3.1 A data subject access request is a request from an individual (or from someone acting with their authority, e.g., a relative or solicitor) for the information the individual is entitled to ask for under the UK GDPR, namely:

3.1.1 for confirmation as to whether we process personal data about the individual and, if so

3.1.2 for access to that personal data; and

3.1.3 certain other supplementary information

3.2 Such a request will typically be made in writing but may be made orally (eg during a telephone conversation). The request may refer to the UK GDPR, the 'GDPR' and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

3.3 All data subject access requests should be immediately directed to the data protection officer in accordance with paragraph 3 below.

4 What to do when you receive a data subject access request (all staff)

4.1 If you receive a data subject access request and you are not authorised to handle it, you must immediately take the steps set out in paragraphs 3.4 (request received by email), 3.5 (request received by letter) or 3.6 (request received orally). 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 Information Commissioner's Office (ICO) and/or legal action by the affected individual.

4.2 The timescales referred to in this policy must be calculated from the day we receive a request (whether it is a working day or not) until the corresponding calendar date in the next month, for example if a request is received on 1 September, information must be provided in accordance with paragraph 8.1 by 1 October.

4.3 For information on what amounts to a data subject access request, see paragraph 2 above. If you are in any way unsure as to whether a request for information is a data subject access request, please contact the data protection officer on dpo@castlewater.co.uk.

4.4 If you receive a data subject access request by email, you must immediately forward the request to the data protection officer at this email address: dpo@castlewater.co.uk, ensuring that you

provide a copy of any relevant documentation and attachments that are available to you at the time of the request (even in those circumstances where you do not have all the information).

4.5 If you receive a data subject access request by letter you must:

4.5.1 scan the letter;

4.5.2 send the original to the data protection officer at this address: Castle Water Limited, 1 Boat Brae, Blairgowrie, PH10 7BH for the attention of Euan Mitchell, Data Protection Officer; and

4.5.3 send a scanned copy of the letter to this email address: dpo@castlewater.co.uk.

4.6 If you receive a data subject access request orally, you must:

4.6.1 note the date of the request;

4.6.2 take the full name and contact details of the individual (please note that the name and contact details must be specific to an individual. E.g., cannot be “customer” or “info@” email address);

4.6.3 obtain as much information as possible about the individual’s request; and

4.6.4 immediately email the data protection officer at this email address: dpo@castlewater.co.uk and provide the individual’s contact details and details of the oral request and the date on which it was received.

4.7 If you receive a request via social media, you must:

4.7.1 take a screenshot or other copy of the request and immediately send it by email to the data protection officer at this address: dpo@castlewater.co.uk.

4.7.2 when sending over a social media request, do not send a link only as links can break, or the underlying social media request may be deleted.

4.8 You must not take any other action in relation to the data subject access request unless the data protection officer has authorised you to do so in advance and in writing.

5 Conditions for responding to a valid request (authorised staff)

5.1 Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

5.2 While it is not a requirement under Retained Regulation (EU) 2016/679, UK GDPR that an individual must make a DSAR in writing, it is helpful for the CWL Group if they do so. Individuals should therefore be encouraged to put requests in writing via email or letter.

5.3 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

5.3.1 that is manifestly unfounded or excessive, eg repetitive; or

5.3.2 for further copies of the same information.

6 Identifying the data subject (authorised staff)

6.1 Before responding to a data subject access request, we will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.

6.2 We will not retain personal data, e.g. relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

6.3 If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm their identity. Typically we will request a copy of the individual's driving licence or passport to enable us to establish their identity and signature (which should be compared to the signature on the data subject access request and any signature we already hold for the individual). We may also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

6.4 If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request (see paragraph 7 below).

7 Refusing to respond to a request (authorised staff)

7.1 We may refuse to act on a data subject access request where:

7.1.1 even after requesting additional information in accordance with paragraph 6.2, we are not in a position to identify the individual making the data subject access request;

7.1.2 requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character or if the information has already been provided.

7.2 If we intend to refuse to act on a data subject access request, we will inform the individual, within one month of receiving the individual's request:

7.2.1 of the reason(s) why we are not taking action; and

7.2.2 that they have the right to complain to the ICO and seek a judicial remedy.

8 Time limit for responding to a request (authorised staff)

8.1 Once a data subject access request is received, the CWL Group must provide the information requested without delay and at the latest within one month of receiving the request. You should therefore make a note of when request was received and when the time limit will end.

8.2 If a data subject access request is complex or the data subject has made numerous requests, the CWL Group:

8.2.1 may extend the period of compliance by a further two months; and

8.2.2 must inform the individual of the extension within one month of the receipt of the request and explain why the extension is necessary.

9 Information to be provided in response to a request (authorised staff)

9.1 The individual is entitled to receive access to the personal data we process about the individual and the following information:

9.1.1 the purposes for which we process the data;

9.1.2 the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

9.1.3 where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

9.1.4 the fact that the individual has the right:

9.1.4.1 to request that the CWL Group rectifies, erases, or restricts the processing of the individual's personal data; or

9.1.4.2 to object to its processing;

9.1.4.3 to lodge a complaint with the ICO;

9.1.5 where the personal data has not been collected from the individual, any information available regarding the source of the data;

9.2 The information referred to in paragraph 9.1 should be provided:

9.2.1 in a way that is concise, transparent, easy to understand and easy to access;

9.2.2 using clear and plain language, with any technical terms, abbreviations or codes explained;

9.2.3 in writing, if the data subject access request was made in writing; and

9.2.4 in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual.

10 How to locate information (authorised staff)

10.1 The personal data we need to provide in response to a data subject access request may be located in several of our electronic and manual filing systems or on those of our data processors or other third parties. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

10.2 Depending on the type of information requested, you may need to search all or some of the following:

10.2.1 electronic systems, including:

10.2.1.1 billing systems such as Velocity or Edge or TEIP;

10.2.1.2 customer relationship management systems such as Zoho, Velocity or CSM

10.2.1.3 telephony systems such as Amazon Connect;

10.2.1.4 all databases including shared drives, networked and non-networked computers and servers,

10.2.1.5 human resources system,

10.2.1.6 email data,

10.2.1.7 back up data,

10.2.1.8 CCTV;

10.3 manual filing systems in which personal data are accessible according to specific criteria, eg chronologically ordered sets of manual records containing personal data; and

10.4 data systems held externally by our data processors such as our external payroll provider Cascade;

10.5 You should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

11 What is personal data? (authorised staff)

11.1 Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to access to information which constitutes the individual's personal data.

11.2 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, eg their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (eg key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

12 Requests made by third parties on behalf of the individual (authorised staff)

Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that the agent is authorised to act on behalf of the individual.

13 Exemptions to the right of subject access (authorised staff)

In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

13.1 **Crime detection and prevention:** We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that they are being

investigated for an illegal activity (ie by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

13.2 **Protection of rights of others:** We do not have to disclose personal data to the extent that doing so would involve disclosing information which identifies another individual, unless:

13.2.1 that other individual has consented to the disclosure of the information to the individual making the request; or

13.2.2 it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

13.2.2.1 the type of information that would be disclosed;

13.2.2.2 any duty of confidentiality owed to the other individual;

13.2.2.3 any steps taken by the controller with a view to seeking the consent of the other individual;

13.2.2.4 whether the other individual is capable of giving consent; and

13.2.2.5 any express refusal of consent by the other individual.

13.3 **Confidential references:** We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

13.3.1 education, training or employment of the individual;

13.3.2 appointment of the individual to any office; or

13.3.3 provision by the individual of any service

13.4 This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (ie the person giving the reference), which means you must consider the rules regarding disclosure of third-party data set out in paragraph 12 before disclosing the reference.

13.5 **Legal professional privilege:** We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

13.5.1 'legal advice privilege', which covers confidential communications between any CWL Group Company and its professional legal advisers for the purpose of seeking or obtaining legal advice;

13.5.2 'litigation privilege', which covers confidential communications between any CWL Group Company and its professional legal advisers or a third party where litigation is contemplated or in progress.

13.6 **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 business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions, and demotions. This

exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

13.7 **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. For example, if the HR department is negotiating with an employee in order to agree the terms of a redundancy package and the employee makes a data subject access request, the HR department can legitimately withhold giving access to information which would prejudice those redundancy negotiations. The HR department must, however, disclose all other personal data relating to the individual unless those other personal data are also exempt from disclosure.

14 Deleting personal data in the normal course of business (authorised staff)

14.1 The information that we are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received. However, as we have one month in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

14.2 We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a data subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

15 Consequences of failing to comply with this policy (all staff)

15.1 The CWL Group takes compliance with this policy very seriously. If we fail to comply with a subject access request or fail to provide access to all the personal data requested or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

15.2 it may put at risk the individual(s) whose personal information is being processed;

15.3 the individual may complain to the ICO and this may lead the ICO to investigate the complaint. If we are found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for the CWL Group and, in some circumstances, for the individual responsible for the breach;

15.4 if an individual has suffered damage, or damage and distress, as a result of our breach of the UK GDPR or other relevant legislation, the individual may take us to court and claim damages from us; and

15.5 a court may order us to comply with the subject access request if we are found not to have complied with our obligations under the UK GDPR and other relevant legislation.

15.6 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

16 Contacts and responsibilities (all staff)

16.1 This Policy will be reviewed annually by the data protection officer.

16.2 Any questions regarding this Policy should be addressed to the data protection officer.