

DATA PROTECTION (UKGDPR) POLICY

CONTENTS

QUICK OVERVIEW	3
1.0 INTRODUCTION	4
2.0 PURPOSE	4
3.0 SCOPE	4
4.0 ROLES AND RESPONSIBILITIES	4
5.0 DATA STORAGE	5
6.0 EMPLOYEE AND ASSOCIATE INFORMATION	6
7.0 CLIENT AND SALES INFORMATION	6
8.0 MEMBERS OF THE GENERAL PUBLIC	7
9.0 DATA SECURITY	7
10.0 INDIVIDUAL RIGHTS	8
11.0 SUBJECT ACCESS REQUESTS	8
12.0 DATA BREACHES	9
13.0 REFERENCES AND ASSOCIATED DOCUMENTATION	9
14.0 MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS	9

VERSION CONTROL

Version	Primary Editor	Reviewer	Changes made by reviewer	Approved by	Date
V1.01	Lauren Earl	Andrew Moore	Partner Review		09/04/20
V1.02	Lauren Earl	Madeleine Milligan	Updates following Partner Review		15/04/20
V2.0	Lauren Earl	Madeleine Milligan	Finalised	Andrew Moore	15/04/20
V2.01	Lauren Earl	Curtis Batterbee	Proofed		29/04/20
V2.02	Lauren Earl	Madeleine Milligan	Addition of Change Log clause	Liane Langdon	15/05/20
V2.03	Lauren Earl	Madeleine Milligan	Updated employee data retention periods	Andrew Moore	22/05/20
V2.04	Lauren Earl		Changes following migration to Microsoft 365		06/08/20
V2.05		Liane Langdon	Finalised		24/09/20
V2.06		Ed Taylor	Address and systems updated	Andrew Moore	16/05/22
V2.07		Liane Langdon	Alignment to DSPT requirements	Andrew Moore	19/01/23
V3.0		Lynne Smith	Formatting changes		19/01/23
V4.0		Lynne Smith	Renamed and Version Control	Andrew Moore	31/01/23
V4.01		Annabelle Armstrong	Reviewed and updated document to reflect new DPO details	Andrew Moore	24/08/23
V5.0		Nick Jones	Formatting Changes and version control.		25/08/23
V5.01		Marielle Walmsley	Address updated		16/11/23
V6.0		Nick Jones	Formatting and Version control		08/02/24
V7.00	Marielle Walmsley		Updated policy owner	Jane Williams	30/04/24
V7.01	Annabelle Armstrong		Annual Review and minor compliance enhancements: - Breach reporting timescale - SAR identify verification - International transfers - No automated decision-making Branding updated		28/04/26

V8.00	Dan Sly		Xero removed Reference added		15/07/26
-------	---------	--	---------------------------------	--	----------

QUICK OVERVIEW

For quick reference the guide below is a summary of the document. This does not negate the need for the document author and all members of staff to be aware of and follow the detail of this policy.

- This policy outlines the steps Clarity Consulting Associates Ltd take to ensure any data we collect, store, and process is protected and compliant with the UK General Data Protection Regulation.
- Clarity Consulting Associates Ltd take privacy of information seriously and ensure that we protect data collected and received from the clients we work with, our employees, our associates, and members of the general public that we interact with. This data is kept safely and securely and not shared with any third party unless through the explicit consent of the information's owner.
- Our Data Protection Officer is responsible for overseeing the implementation of this policy and ensuring our compliance with relevant laws and regulations.

1.0 INTRODUCTION

- 1.1 Clarity Consulting Associates Ltd (hereafter referred to as “Clarity”) take the privacy of information seriously and ensure that we protect data collected and received from the clients we work with, our employees, our associates and members of the general public that we interact with. This data is kept safely and securely and not shared with any third party unless through the explicit consent of the information’s owner.
- 1.2 Clarity is committed to compliance with all aspects of The UK General Data Protection Regulation (UKGDPR).
- 1.3 This policy is not contractual; Clarity therefore reserves the right to amend this policy as necessary to meet any changing requirements.

2.0 PURPOSE

- 2.1 The purpose of this policy is to document the processes in place that ensure Clarity is compliant with the UK General Data Protection Regulation (UKGDPR) and ensure the privacy of data held by the company.

3.0 SCOPE

- 3.1 This policy applies to all personal data collected, processed and stored by Clarity, its employees and associates.

4.0 ROLES AND RESPONSIBILITIES

- 4.1 George Harris is our Data Protection Officer (DPO) (non-statutory). This role is a leadership role, responsible for overseeing data protection strategy and implementation and to ensure compliance with the UK GDPR requirements. The specific responsibilities of this role include:

- To co-ordinate and process requests for data to be deleted and any data queries that are received by the organisation pertaining to data.

- To work with the organisation to ensure sufficient in-house training, local information audits and monitoring of data processes is conducted to ensure compliance with the legislation.

4.2 The DPO's minimum tasks are defined in Part 3, Chapter 4 of the Act:

- to inform and advise the controller, its employees and any associated processors about their obligations to comply with the UK GDPR and other relevant data protection laws such as Part 3 of the Act;
- to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

4.3 Chris Richmond, Senior Consultant, is the nominated Caldicott Guardian

4.4 Paul Sly, Partner, is the nominated Senior Information Responsible Owner (SIRO)

5.0 DATA STORAGE

5.1 Clarity collects and stores personal information. The types of information that we currently keep includes:

- Employee & Associate Information such as the information required to process payroll, make statutory returns (e.g. to HMRC), ensure accessibility/ dietary needs are met and for emergency and personal communication;
- Client Information such as contact details;
- Supplier Information such as contact details;
- Information on members of the general public such as contact information available in the public domain for experts in health and care, journalists and other stakeholders in our wider environment, and contact details of members of the public who sign up to our newsletters or other publications, events and networks.

5.2 All data that Clarity is in possession of is kept in encrypted storage with access controls in the UK.

5.3 Clarity's cloud storage is operated by Microsoft from servers based in the UK.

5.4 Clarity's website is hosted by Webflow on AWS servers. Webflow's DPA incorporates the new standard contractual clauses approved by the European Commission in June 2021 (which are considered by the European Commission to be offering an adequate level of protection for the personal information of EU Member State residents). The website provider has its own Privacy Policies, technical and operational mechanisms for security and data protection which are aligned with Clarity's IMS Policies.

- 5.5 Where personal data is transferred outside of the United Kingdom, Clarity ensures that appropriate safeguards are in place, including the use of the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses and that transfer risk assessments are completed where required.

6.0 EMPLOYEE AND ASSOCIATE INFORMATION

- 6.1 All employee information is stored on the company's document management system, Microsoft SharePoint. This is an online cloud based system which is password protected and uses role based access to ensure that data is only accessible by members of staff that require access for the purposes of management, payroll and in case of emergency. It has both encrypted storage and multi factor authentication role based access controls.
- 6.2 Information held on behalf of employees by Clarity includes:
- Recruitment information including contact details, qualifications, employment history, referees, ethnicity and disability details.
 - Payroll information including contact details, bank details, pension details and tax details.
 - Contractual information including annual leave, sick leave and performance information.
- 6.3 All data is held on a lawful basis for processing personal data under Article 6(1)(c) – legal obligations, Article 6(1)(b) – contractual obligations to maintain legal accuracy, and Article 9(2)(b) – employment obligations of the General Data Protection Regulation.
- 6.4 This data is shared as part of these obligations with authorities where necessary, including HMRC and pensions providers.
- 6.5 The retention schedule is as follows:
- Recruitment information – 6 years post-employment, 1 year for any unsuccessful applicants.
 - Payroll information – 6 years post-employment, with the exception of pension information which is 75 years post-employment.
 - Contractual information – 6 years post-employment.

7.0 CLIENT AND SALES INFORMATION

- 7.1 Client information is stored on the company's cloud storage (SharePoint for engagements, CMap for client relationship and engagement management)
- 7.2 Sales information and client information is gathered as part of our ongoing professional relationship with existing clients.
- 7.3 In addition, information is gathered by our website (www.ccal.co.uk) when clients opt in to mailing lists and direct marketing. This information is retained until twelve months beyond the end of the customer relationship.

- 7.4 Intellectual property developed during client engagements is retained and products returned to the client at the end of any given customer relationship. Copies of products and drafts are retained in secure storage by Clarity for a minimum of 12 months beyond the end of the customer relationship unless otherwise agreed with the client.

8.0 MEMBERS OF THE GENERAL PUBLIC

- 8.1 Members of the general public can sign up for marketing emails via our website (www.ccal.co.uk). This information is stored within GetForm.io and our Clarity document management system, Microsoft SharePoint.
- 8.2 All emails that are delivered using this service have an unsubscribe link within the email which enables the user to opt out from further communications. This process also erases their data from our database.
- 8.3 A Website Privacy Policy is available on our website to inform visitors of the information we collect when using and interacting with the site.

9.0 DATA SECURITY

- 9.1 Clarity commits to ensuring that personal data is stored securely using modern software that is kept up to date.
- 9.1.1. All employees are instructed to exclusively use our cloud storage and to ensure that no data or files are saved on computer hard drives.
 - 9.1.2. We discourage the use of memory sticks to transfer files. However, when there is no reasonable alternative an encrypted memory stick may be used to ensure data is secure in the event of loss or theft.
- 9.2 Access to personal data is limited to staff who need access and appropriate security is in place to avoid unauthorised sharing of information.
- 9.3 When personal data is deleted, it is done in a manner that ensures the data is irrecoverable.
- 9.3.1. A Change Log is maintained by the Business Manager and saved on SharePoint with restricted access. To ensure UKGDPR compliance, all instances of permanent removal of personal data or other storage/change compliance actions within SharePoint or CMap are documented on the Change Log, e.g. the deletion of a CMap contact, the removal of past employee HR files from SharePoint, or client data reaching record destruction date. If a previous backup needs to be reinstated, the Change Log can then be used to ensure all deleted content is removed from the backup. A hardcopy of the Change Log is also maintained to ensure continuity should any issues with SharePoint arise.

- 9.4 Back-up and data recovery procedures are in place as outlined in our Business Continuity Policy.

10.0 INDIVIDUAL RIGHTS

Clarity does not currently carry out automated decision-making or profiling that produces legal or similarly significant effects for individuals.

- 10.1 Clarity will ensure that the rights of the individual are preserved with respect to ownership of their information and recognise the following individual rights:
- The right to be informed;
 - The right of access;
 - The right to rectification;
 - The right to erasure;
 - The right to restrict processing;
 - The right to data portability;
 - The right to object; and
 - The right not to be subject to automated decision-making including profiling.

11.0 SUBJECT ACCESS REQUESTS

- 11.1 Clarity will process all subject access requests that are made to the company within one month of receiving them.
- 11.2 All subject access requests will be processed unless they are manifestly unfounded or excessive. In such cases, this will be clearly communicated with the individual concerned with the rationale provided. We will clearly state that the requestor has the right to complain to the Information Commissioner's Office or seek legal remedy.
- 11.3 Subject access requests can be made to Clarity via the data controller:
- datacontroller@ccal.co.uk
 - Alternatively, write to us at 5th Floor, Kings House, 174 Hammersmith Road, London W6 7JP
- 11.4 Before responding to a Subject Access Request, Clarity may request reasonable evidence to verify the identity of the individual making the request. This is to ensure that personal data is not disclosed to unauthorised persons.

12.0 DATA BREACHES

- 12.1 Clarity are committed to the protection of any data that we hold as a company, however in the unlikely event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, Clarity shall promptly assess the risk to people's rights and freedoms and, where required, notify the ICO within 72hrs of becoming aware of a notifiable personal data breach.

13.0 REFERENCES AND ASSOCIATED DOCUMENTATION UKGDPR

Relevant policies can be found in the [All Staff QMS Current Policies folder](#):

- Business Continuity Policy
- Website Privacy Policy

[Data protection Act 2018](#)

[Data \(Use and Access\) Act 2025](#)

14.0 MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS

This policy will be reviewed on a biannual basis by Clarity's senior team, or earlier if appropriate/required.