Verification of readily accessible records

Policy Number	32
Version	6
Policy Contact	Matthew Betteridge
Date Issued	1st November 2017
Reviewed	06th May 2025
Next Review Date	06th May 2026
Target Audience	Agency Workers
Approved by	OneCall24 Policy Team

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the UK GDPR and Data Protection Act 2018. The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

As a recruitment business, One Call 24 Limited (OneCall24) collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how OneCall24 implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

Application of this policy

All staff, volunteers, contractors and consultants etc must comply with this policy, in their conduct of official business for OneCall24. This policy applies to records in all formats, including electronic records.

Records as a resource

OneCall24 recognises that records are a vital asset to:

- facilitate information accessibility, and enhance business operations by supporting program delivery, management and administration
- deliver customer services in an efficient, fair and equitable manner
- provide evidence of actions and decisions and precedents for future decision making, and a small percentage of OneCall24 records will become archived

Records Management Program

A records management program is a planned, coordinated set of policies, procedures, people, systems and activities that are required to manage records.

One Call 24 Records Management Program seeks to ensure that:

- it has the records it needs to support and enhance ongoing business and customer service, meet accountability requirements
- these records are managed efficiently and can be easily accessed and used for as long as they are required
- records are stored as cost-effectively as possible and when no longer required they are disposed of in a timely and efficient manner

A goal of particular note is that the organisation is committed, through its Records Management Program, to maintaining digital and other technology dependent records in authentic and accessible form for as long as they are required.

Storage

All current hardcopy records must be stored in designated, secure storage areas that are appropriate for active use and subject to access restrictions. These areas must be clearly marked and managed to ensure that only authorised personnel can access the records. This helps maintain confidentiality, integrity, and availability of personal data in accordance with the UK GDPR.

Records that are no longer in regular use but are still required for legal, operational, or audit purposes should be securely transferred to the custody of the Head of GDPR, Susanna Caddeo. This includes records that must be retained under statutory obligations or internal policy requirements. The transfer process must be documented to ensure traceability and accountability.

Electronic records should be stored using secure, scalable digital systems. These may include encrypted servers or approved cloud-based platforms that meet the organisation's information security standards. Outdated storage media such as CDs, DVDs, and magnetic disks should be phased out in favour of more secure and sustainable formats. All electronic storage must ensure that records remain accessible, authentic, and intact for as long as they are required.

OneCall24 maintains a formal Retention Schedule, which outlines the required storage periods for all categories of personal data. This schedule is based on statutory requirements, business needs, and guidance from the Information Commissioner's Office (ICO). It is reviewed regularly to ensure compliance with the storage limitation principle under Article 5(1)(e) of the UK GDPR, which requires that personal data be kept no longer than necessary for the purposes for which it was collected.

Records of short-term value are reviewed periodically and securely disposed of at appropriate intervals. Disposal decisions must be documented and carried out in a manner that ensures the data cannot be reconstructed or retrieved. Records of long-term or archival value should be retained in

formats that ensure continued accessibility and usability, with appropriate metadata and version control where applicable.

Maintenance and monitoring

OneCall24 is committed to ensuring that all records, whether physical or digital, are properly maintained and monitored throughout their lifecycle. To support this, the location and status of each record must be documented and updated whenever the record is accessed, moved, or transferred. This ensures that records remain traceable, secure, and accountable at all times, in accordance with the UK GDPR's accountability principle.

For electronic records, maintenance may involve the migration of data between systems or formats to preserve accessibility and usability over time. Any such migration must be authorised by the Head of GDPR, Susanna Caddeo, and must be carried out in a way that guarantees the authenticity, completeness, and integrity of the data. Migration processes should be documented and include appropriate validation checks to confirm that no data is lost, altered, or rendered inaccessible.

All record movements and data migrations must also be documented within the OneCall24's Record of Processing Activities (ROPA), in accordance with Article 30 of the UK GDPR. This ensures full traceability of processing operations and supports the OneCall24's broader accountability obligations, including audit readiness and compliance with the ICO's 2024 Data Protection Audit Framework.

These measures form part of the OneCall24's commitment to digital continuity, ensuring that records remain reliable and usable for as long as they are required, regardless of changes in technology or systems.

Access

Records must be available to all authorised staff that require access to them for business purposes.

All access to OneCall24 records by members of the public, including Freedom of Information requests, will be in accordance with:

- The Access to Health Records Act (1990)
- The Data Protection Act (2018)
- Freedom of Information Scotland Act (2002)
- Public Records Act (Scotland) 2011
- Regulation 29 of the Conduct Regulations and Data Protection

Regulation 29

At all times, OneCall24 agrees to abide by the clauses/terms as set out within regulation 29 of the Conduct Regulations and Data Protection as detailed below (Guidance taken from https://www.legislation.gov.uk/uksi/2003/3319/regulation/29):

29.—(1) Subject to paragraph (6), every agency and every employment business shall keep records which are sufficient to show whether the provisions of the Act and these Regulations are being complied with including (subject to paragraph (3))—

(a)the particulars specified in Schedule 4, in relation to every application received by the agency or employment business from a work-seeker;

(b)the particulars specified in Schedule 5, in relation to every application received by the agency or employment business from a hirer; and

(c) the particulars specified in Schedule 6 relating to dealings with other agencies and employment businesses.

(2) The records mentioned in paragraph (1) shall be kept for at least one year from the date of their creation, and in the case of the particulars referred to in sub-paragraphs (a) and (b) of paragraph (1), at least one year after the date on which the agency or employment business last provides services in the course of its business as an agency or an employment business to the applicant to whom they relate.

(3) Neither an agency nor an employment business is required to keep the particulars referred to in paragraphs (1)(a) or (1)(b) in respect of applications on which the agency or employment business takes no action.

(4) The records mentioned in paragraph (1) may be kept by an agency or employment business, either at any premises it uses for or in connection with the carrying on of an agency or employment business, or elsewhere. If they are kept elsewhere, the agency or employment business shall ensure that they are readily accessible by it and that it is reasonably practicable for any person employed by the agency or employment business at any premises it uses for or in connection with the carrying on of an agency or employment business to arrange for them to be delivered no later than the end of the second business day following the day on which a request under section 9 of the Act(**1**) for them is made, to the premises at which that person is employed.

(5) The records an agency or employment business is required to keep pursuant to this regulation may be kept in electronic form, provided that the information so recorded is capable of being reproduced in legible form.

(6) This regulation does not apply to any records which an agency is required to preserve in accordance with paragraph 12 of Schedule 2.

Definitions and Key Terms

In this policy the following terms have the following meanings:

'*consent*' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the *processing* of persona data relating to him or her;

'*data controller*' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the *processing* of *personal data*;

'*data processor*' means an individual or organisation which processes *personal data* on behalf of the *data controller*;

'personal data'* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;

'*processing*' means any operation or set of operations performed on *personal data*, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

'*profiling*' means any form of automated *processing* of *personal data* consisting of the use of *personal data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'*pseudonymisation*' means the *processing* of *personal data* in such a manner that the *personal data* can no longer be attributed to an individual without the use of additional information, provided that

such additional information is kept separately and is subject to technical and organisational measures to ensure that the *personal data* are not attributed to an identified or identifiable individual;

'*sensitive personal data*'* means *personal data* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the *processing* of genetic data, biometric data, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

'*Supervisory authority*' means an independent public authority which is responsible for monitoring the application of data protection. In the UK the *supervisory authority* is the Information Commissioner's Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

OneCall24 processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws. OneCall24 has registered with the ICO and its registration number i**s ZA136295.**

OneCall24 may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations
- Accounts and records;
- Administration and processing of work-seekers' personal data for the purposes of providing work-finding services, including processing using software solution providers and back office support
- Administration and processing of clients' personal data for the purposes of supplying/introducing work-seekers.

The data protection principles

The Data Protection Laws require OneCall24 acting as either *data controller* or *data processor* to process data in accordance with the principles of data protection. These require that *personal data* is:

1. Processed lawfully, fairly and in a transparent manner;

2. Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that *personal data* that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
6. Processed in a manner that ensures appropriate security of the *personal data*, including protection against unauthorised or unlawful *processing* and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
7. The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

Legal bases for processing

OneCall24 will only process *personal data* where it has a legal basis for doing so (see Annex A). Where OneCall24 does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

OneCall24 will review the *personal data* it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date.

Before transferring *personal data* to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), OneCall24y will establish that it has a legal reason for making the transfer.

Privacy by design and by default

OneCall24 has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all *processing* activities. This includes implementing measures such as:

- data minimisation (i.e. not keeping data for longer than is necessary);
- *pseudonymisation*;
- anonymization;
- cyber security

For further information please refer to OneCall24's Information Security Policy.

OneCall24 shall provide any information relating to data *processing* to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. OneCall24 may provide this information orally if requested to do so by the individual.

Privacy notices

Where OneCall24 collects *personal data* from the individual, OneCall24 will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where OneCall24 collects *personal data* other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the *personal data*, but at the latest within one month. If OneCall24 intends to disclose the *personal data* to a third party then the privacy notice will be issued when the *personal data* are first disclosed (if not issued sooner).

Where OneCall24 intends to further process the *personal data* for a purpose other than that for which the data was initially collected, OneCall24 will give the individual information on that other purpose and any relevant further information before it does the further *processing*.

Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

Rectification

The individual or another *data controller* at the individual's request, has the right to ask the OneCall24 to rectify any inaccurate or incomplete *personal data* concerning an individual.

If OneCall24 has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the *personal data* unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however OneCall24 will not be in a position to audit those third parties to ensure that the rectification has occurred.

Erasure

The individual or another *data controller* at the individual's request, has the right to ask OneCall24 to erase an individual's *personal data.*

If OneCall24 receives a request to erase it will ask the individual if s/he wants his *personal data* to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). OneCall24 cannot keep a record of individuals whose data it has erased so the individual may be contacted again by OneCall24 should OneCall24 come into possession of the individual's *personal data* at a later date.

If OneCall24 has made the data public, it shall take reasonable steps to inform other *data controllers* and *data processors processing* the *personal data* to erase the *personal data*, taking into account available technology and the cost of implementation.

If OneCall24 has given the *personal data* to any third parties it will tell those third parties that it has received a request to erase the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however OneCall24 will not be in a position to audit those third parties to ensure that the rectification has occurred.

Restriction of processing

The individual or a *data controller* at the individual's request, has the right to ask OneCall24 to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful, and the individual opposes its erasure;
- OneCall24 no longer needs the *personal data* for the purposes of the *processing*, but the *personal data* is required for the establishment, exercise or defence of legal claims; or
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of OneCall24 override those of the individual.

If OneCall24 has given the *personal data* to any third parties it will tell those third parties that it has received a request to restrict the *personal data*, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the *personal data* they hold - however OneCall24 will not be in a position to audit those third parties to ensure that the rectification has occurred.

Data portability

The individual shall have the right to receive *personal data* concerning him or her, which he or she has provided to OneCall24, in a structured, commonly used and machine-readable format and have the right to transmit those data to another *data controller* in circumstances where:

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, OneCall24 will send the *personal data* to a named third party on the individual's request.

Object to processing

The individual has the right to object to their *personal data* being processed based on a public interest or a legitimate interest. The individual will also be able to object to the *profiling* of their data based on a public interest or a legitimate interest.

OneCall24 shall cease *processing* unless it has compelling legitimate grounds to continue to process the *personal data* which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their *personal data* for direct marketing. Please refer to OneCall24's Marketing Policy for further information.

Enforcement of rights

All requests regarding individual rights should be sent to gdpr@onecall24.co.uk

OneCall24 shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision making processes or profiling within one month of receipt of the request. OneCall24 may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where OneCall24 considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature OneCall24 either may refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

Automated decision making

OneCall24 will not subject individuals to decisions based on automated *processing* that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

OneCall24 will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

Reporting personal data breaches

All data breaches should be referred to gdpr@onecall24.co.uk.

Personal data breaches where OneCall24 is the data controller:

Where OneCall24 establishes that a *personal data breach* has taken place, OneCall24 will take steps to contain and recover the breach. Where a *personal data breach* is likely to result in a risk to the rights and freedoms of any individual OneCall24 will notify the ICO.

Where the *personal data breach* happens outside the UK, OneCall24 shall alert the relevant *supervisory authority* for data breaches in the effected jurisdiction.

Personal data breaches where OneCall24 is the data processor:

OneCall24 will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

Communicating personal data breaches to individuals

Where OneCall24 has identified a *personal data breach* resulting in a high risk to the rights and freedoms of any individual, OneCall24 shall tell all affected individuals without undue delay.

OneCall24 will not be required to tell individuals about the *personal data breach* where:

- OneCall24 has implemented appropriate technical and organisational protection measures to the *personal data* affected by the breach, in particular to make the *personal data* unintelligible to any person who is not authorised to access it, such as encryption.
- OneCall24 has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, OneCall24 shall make a public communication or similar measure to tell all affected individuals. All

individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with *personal data* these should be respected at all times:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

If you have a complaint or suggestion about OneCall24's handling of personal data then please contact gdpr@onecall24.co.uk.

Alternatively, you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

The people responsible for are Susanna Caddeo, Head of GDPR and Matthew Betteridge Data Protection Officer.

- adding, amending or deleting *personal data*;
- responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision making processes and profiling

Reporting data breaches/dealing with complaints

The lawfulness of *processing* conditions for *personal data* are:

1. Consent of the individual for one or more specific purposes.
2. Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
3. Processing is necessary for compliance with a legal obligation that the controller is subject to.
4. Processing is necessary to protect the vital interests of the individual or another person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

The lawfulness of *processing* conditions for *sensitive personal data* are:

1. Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
2. *Processing* is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
3. *Processing* is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving *consent*.
4. In the course of its legitimate activities, *processing* is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the *processing* relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the *consent* of the individual.
5. *Processing* relates to *personal data* which are manifestly made public by the individual.
6. *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. *Processing* is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
8. *Processing* is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee , medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
9. *Processing* is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
10. *Processing* is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.