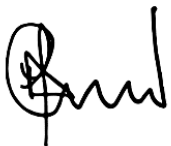


# Auxo Group Data Protection Policy

This document is approved and authorised for application within Auxo Group and all associated subsidiary companies.



**Ford Garrard, CEO**

Last Review Date: October 2024

## Contents

<b>Introduction .....</b>	<b>2</b>
<b>Definitions .....</b>	<b>2</b>
<b>Data Processing and Data Protection Laws .....</b>	<b>3</b>
<b>Data Protection Principles.....</b>	<b>3</b>
<b>Legal Bases for Processing .....</b>	<b>4</b>
<b>Privacy by Design and by Default .....</b>	<b>4</b>
<b>Rights of the Individual .....</b>	<b>4</b>
<b>Privacy Notices .....</b>	<b>4</b>
<b>Subject Access Requests .....</b>	<b>4</b>
<b>Retification .....</b>	<b>5</b>
<b>Erasure.....</b>	<b>5</b>
<b>Restrictions on Processing .....</b>	<b>5</b>
<b>Data Portability.....</b>	<b>6</b>
<b>Object to Processing .....</b>	<b>6</b>
<b>Enforcement of Rights.....</b>	<b>6</b>
<b>Automated Decision Making .....</b>	<b>6</b>
<b>Reporting Personal Data Breaches.....</b>	<b>6</b>
<b>Personal Data Breaches where we are the Data Controller .....</b>	<b>7</b>
<b>Personal Data Breaches where we are the Data Processor.....</b>	<b>7</b>
<b>Communicating Personal Data Breaches to Individuals .....</b>	<b>7</b>
<b>The Human Rights Act .....</b>	<b>7</b>
<b>Complaints.....</b>	<b>7</b>

## Introduction

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 2018 and the EU General Data Protection Regulation (together the ‘Data Protection Laws’). 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.

We collect and process both personal data and sensitive personal data and we are required to do so to comply with other legislation. We are also required to keep this data for different periods depending on the nature of the data.

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

## Definitions

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 personal 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.

“**pseudonymization**” 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.

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	2	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------

\* 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).

## Data Processing and Data Protection Laws

We process personal data in relation to our own staff, work-seekers and individual client contacts and we are a data controller for the purposes of the Data Protection Laws. All Auxo Group companies and associated businesses are registered with the ICO and registrations are renewed annually.

We 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

## Data Protection Principles

The Data Protection Laws require us, when 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:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
- Kept for no longer than is necessary for the purposes for which the personal data are processed
- 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
- The data controller shall be responsible for, and be able to demonstrate, compliance with the principles

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	3	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------

## Legal Bases for Processing

We will only process personal data where we have a legal basis for doing so (see Annex A). Where we do not have a legal reason for processing personal data, any processing would be a breach of the Data Protection Laws.

We will review the personal data we hold 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)), we will establish that we have a legal reason for making the transfer.

## Privacy by Design and by Default

We have implemented measures and procedures that adequately protect the privacy of individuals and ensure 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
- clear desk policy

## Rights of the Individual

We 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. We may provide this information orally if requested to do so by the individual.

## Privacy Notices

Where we collect personal data from an individual, we will give the individual a privacy notice at the time when it first obtains the personal data.

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

Where we intend to further process the personal data for a purpose other than that for which the data was initially collected, we 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.

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	4	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------

## Retification

The individual or another data controller at the individual's request, has the right to ask us to rectify any inaccurate

or incomplete personal data concerning an individual.

If we have given the personal data to any third parties, we 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 we 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 us to erase an individual's personal data.

If we receive a request to erase, we will ask the individual if they want their personal data to be removed entirely or whether they are 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). We cannot keep a record of individuals whose data it has erased so the individual may be contacted again by us should we come into possession of the individual's personal data at a later date.

If we have made the data public, we 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 we have given the personal data to any third parties, we 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 we will not be in a position to audit those third parties to ensure that the rectification has occurred.

## Restrictions on Processing

The individual or a data controller at the individual's request, has the right to ask us 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
- We no longer need the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims
- The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending verification as to whether our legitimate grounds override those of the individual

If we have given the personal data to any third parties, we 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 we will not be in a position to audit those third parties to ensure that the rectification has occurred.

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	5	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------

## Data Portability

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to us, 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
- The processing is carried out by automated means

Where feasible, we 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.

We 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.

## Enforcement of Rights

All requests regarding individual rights should be sent to our Data Protection Officer by email at [Auxo- dpo@peo.legal](mailto:Auxo-dpo@peo.legal)

We 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. We may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

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

## Automated Decision Making

We 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
- The individual has given their explicit consent

We 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 our Data Protection Officer by email at:

[Auxo-dpo@peo.legal](mailto:Auxo-dpo@peo.legal)

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	6	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------

## Personal Data Breaches where we are the Data Controller

Where we establish that a personal data breach has taken place, we 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, we will notify the ICO.

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

## Personal Data Breaches where we are the Data Processor

We will alert the relevant data controller as to the personal data breach as soon as we are aware of the breach.

## Communicating Personal Data Breaches to Individuals

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

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

- We have 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
- We have 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, we shall make a public communication or similar measure to tell all affected individuals

## The Human Rights Act

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)

## Complaints

If you have a complaint or suggestion regarding our handling of personal data, please contact our Data Protection Officer by email at [Auxo-dpo@peo.legal](mailto:Auxo-dpo@peo.legal)

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

Doc No:	POL03	Date:	Oct 2024	Version No:	1	Page No:	7	Owner:	Business Assurance	Uncontrolled when printed
---------	-------	-------	----------	-------------	---	----------	---	--------	--------------------	---------------------------