

Contents

1.0. Introduction	1
2.0. Our Details	1
3.0. How we receive personal data	1
4.0. The data we collect about you	2
5.0. Why we need to collect this data	2
6.0. Legal basis for using your personal data	2
7.0. Disclosure of your data	3
8.0. Data security	3
9.0. Data retention	3
10.0. Your legal rights	3
11.0. Making a complaint	5

1.0. Introduction

The purpose of this document is to explain how Alert Health Ltd manages your personal information when you contact us or use one of our services, and your rights under current Data Protection Law.

2.0. Our Details

We are registered with the Information Commissioner's Office, reference number ZA057422. Our contact details in relation to data protection are:

Data Protection

Alert Health Ltd

Ground Floor

Aurora House

8 Inverness Campus

Inverness, IV2 5NA

Tel: 01463 710 441

Email: dataprotection@alerthealth.co.uk

Alert Health is the Data Controller for the personal information we process, unless otherwise stated.

3.0. How we receive personal data

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- you have enquired about, booked or engaged in at least one of our services,
- your company has a contract with us and you are acting as their representative,
- your company provides services to us, and you are acting as their representative
- you have applied for a job with us.

We also receive personal information indirectly, in the following scenarios:

Once PRINTED, this is an UNCONTROLLED DOCUMENT

- a third-party occupational health service provider has enquired about or booked at least one of our services on behalf of your employer,
- you are engaged in our service provision and with your consent, an external health professional has provided us with information in relation to your health.

Where you engage with our services, your medical records and related data will be securely managed within Meddbase, our cloud-based medical record management platform.

4.0. The data we collect about you

The types of **personal data** we may collect and process include:

- name
- address
- date of birth
- telephone number
- email address
- details of your current and previous occupations
- GP practice

The types of **special category data** (also known as sensitive data) we collect and process include:

- relevant medical history
- biometrics (body measurements and calculations)
- outcomes of clinical examinations and assessments
- information provided by an external health professional

5.0. Why we need to collect this data

- to book an appointment
- to inform our health assessments
- to enter your details onto medical certificates and reports for purpose of identification
- to ensure we can make contact with you
- to notify your GP of any relevant medical information

6.0. Legal basis for using your personal data

We will only use your personal data when the law allows us to, and where at least one of the following conditions applies:

- a) we have your consent
- b) processing is necessary to fulfil a contract we have with you (*Article 6 (1) (f) of Data Protection Act 2018 – see *definition below*)
- c) processing is necessary to carry out occupational health assessments of fitness for work or monitoring of health at work (*Article 9 (2) (h) of Data Protection Act 2018 – see **definition below*)
- d) where anonymous data is used to protect and promote workplace health through audit or research

Once PRINTED, this is an UNCONTROLLED DOCUMENT

**Article 6 (1) (f): processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party.*

***Article 9 (2) (h): processing is necessary for the purposes of preventive or occupational medicine, for the assessment of 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 or services...”.*

7.0. Disclosure of your data

We will only share your data in the following circumstances:

- where we have your explicit written consent
- where there is a legal obligation to disclose e.g. under court order
- where the Health and Safety Executive has rights under Health & Safety at Work etc. Act 1974
- where it can be justified in the public interest without consent
- with Meddbase, our appointed data processor, solely for the purpose of securely managing medical records and enabling our service delivery. Meddbase only processes your personal data on our documented instructions and is bound by strict contractual and legal obligations of confidentiality and data protection.

We will never share your data for marketing purposes.

8.0. Data security

We understand that the security of your information is important to you. We have put in place appropriate security measures to prevent your personal data from being: accidentally lost; used or accessed in an unauthorised way; altered; or disclosed. We use industry standard physical and procedural security measures to protect information from the point of collection to the point of destruction. This includes: encryption; firewalls; access controls; policies; and other procedures, to protect information from unauthorised access.

Where data processing is carried out on our behalf by a third party, we take steps to ensure that appropriate security measures are in place to prevent unauthorised disclosure of personal data. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

In addition to our own technical and organisational safeguards, your information may be stored and processed on Meddbase's secure platform. Meddbase adheres to the National Cyber Security Centre's (NCSC) Cloud Security Principles and implements industry-standard controls including encryption in transit and at rest, robust access controls, continuous monitoring, and regular security testing. Further details of Meddbase's security posture can be found [here](#).

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9.0. Data retention

As data controller we will keep your information either electronically or on paper, securely, for as long as there is a good reason for retention. Timescales for destruction of data are in accordance with the relevant law, or best practice. Specific examples include:

- occupational health records – retained for 6 years after you leave employer, or until you reach age 75, whichever is sooner
- email enquiries – retained for 1 year
- job enquiries/ CVs – retained for 1 year, unless otherwise requested

Where your data is stored within Meddbase, retention periods remain aligned to statutory and best practice requirements (e.g., occupational health records retained for 6 years after leaving employment or until age 75, whichever is sooner). Meddbase applies secure deletion procedures in line with our policies.

Where we act as data processor, your data will only be held by us as long as it is required to perform the service. The data controller (i.e. third party occupational health provider) will hold the medical record.

10.0. Your legal rights

These rights apply where Alert Health Ltd is the Data Controller. To exercise any of these rights, email dataprotection@alerthealth.co.uk.

Where your personal data is processed within Meddbase, we will facilitate your rights of access, correction, erasure, portability, and objection by working with Meddbase as our data processor.

Where Alert Health is acting as Data Processor on behalf of a third party, Alert Health will provide you with contact details for the Data Controller so you can redirect your request to them.

10.1. Request access to your data

You have a right to know what information is being held about you and to ask for a copy. Requests should be made in writing to the Data Controller. There is generally no charge for this, but a fee may be charged for repeated requests or for multiple copies.

In rare situations where access would damage your physical or mental health or that of another person, or where it would reveal the identity of a third party who does not consent to be identified, a request may legitimately be denied.

10.2. Ask for your data to be corrected

You have the right to ask the Data Controller to correct any factually inaccurate personal data. In the case of occupational health medical records, clinicians will always be ready to correct errors of fact. If there is disagreement about diagnosis or the clinician's opinion, a supplementary clarifying statement can be added to the records so that they are completely accurate.

10.3. Limit processing

You can limit the way we use your personal data if you are concerned about the accuracy of the data or how it is being used. However, should the data be required: for legal claims; to protect another person's rights; or for reasons of important public interest, your request might not be accepted.

Where we are relying on consent to process your personal data, you can withdraw your consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. You would be advised of this at the time you request to withdraw your consent.

10.4. Object to processing

In some circumstances you can object to the processing of your personal data, and we will stop using your data for that purpose unless we provide you with a legitimate reason not to. You can only object to us processing your data when the data is being used for: a task carried out in the public interest; our legitimate interests or statistical purposes.

10.5. Ask for erasure

You can also request erasure of personal data ("the right to be forgotten") where: the information is no longer necessary; you have withdrawn consent; the controller bases the processing on Article 6 (1) (f) but does not have legitimate grounds for processing the data; the data have been unlawfully processed.

Personal sensitive data held in medical records will not always be deleted on request because they fall within Article 9 (2) (h) and because they may be needed to defend the health professional or the employer if a claim is made.

10.6. Request transfer of your data

At your request, we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to data we have collected.

11.0. Making a complaint

If you are concerned about the way your data is used please contact the Data Controller at dataprotection@alerthealth.co.uk. Alternatively you have a right to complain to the Information Commissioner's Office – see ico.org.uk.