

Anxiety UK

Anxiety UK – Employee Privacy Notice

Introduction

This privacy notice describes how we process your personal data as your employer or when you are applying for employment with us.

These are our reasons for collecting it, what we do with it and what your rights are under the UK's data protection laws (the Data Protection Act 2018, UK GDPR).

Who we are

Anxiety UK is the country's largest anxiety, stress and anxiety-based depression charity dedicated to helping anyone affected by such conditions.

Anxiety UK is a registered charity (1113403), and a company limited by guarantee (company no. 5551121).

Our registered address is: Anxiety UK, Nunes House, 447 Chester Road, Old Trafford, Manchester M16 9HA.

We are the data controller for the processing described in this notice and are registered with the Information Commissioner's Office – reference number [Z6130270](#).

We have appointed a Data Protection Officer who can be contacted at the above address, or via privacy@anxietyuk.org.uk .

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way,
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you,
- only use it in the way that we have told you about,
- ensure it is correct and up to date,
- keep your data for only as long as we need it,
- keep your data secure.

Purpose of processing personal data & our lawful basis for doing so

We must have a lawful basis for processing personal data. As your employer we will process your personal data:

- in order to carry out our legal obligations, and
- in order to perform the employment contract that we are both party to, or to take the necessary steps to enter into a new employment contract

We need to process your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance are correctly paid,
- ensuring student loan payments are made,
- carrying out checks in relation to your right to work in the UK,
- making reasonable adjustments for disabled employees,
- recording accidents at work

We also process data so that we can carry out activities which are associated with the contract of employment we have with you, or will have with you if your application is successful, such as:

- making decisions about who to offer initial employment to, and subsequent internal appointments and promotions,
- making decisions about salary and other benefits,
- providing contractual benefits to you,
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises,
- offering a method of recourse for you against decisions made about you via a grievance procedure,
- assessing training needs,
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments ,
- gaining expert medical opinion when making decisions about your fitness for work,
- managing statutory leave and pay systems such as maternity leave and pay,
- business planning and restructuring exercises,
- dealing with legal claims made against us,
- preventing fraud,
- ensuring our administrative and IT systems are secure and robust against unauthorised access.

What Personal Data do we process?

We process the following categories of personal data relating to you:

- your basic personal details including your name, address, date of birth, email address, phone numbers,
- gender,
- marital status,
- next of kin and their contact numbers,

- medical or health information including whether or not you have a disability to help us make reasonable adjustments and to support you,
- information included on your CV including references, education history and employment history,
- documentation relating to your right to work in the UK where appropriate,
- driving licence details if you drive for work purposes,
- bank details,
- tax codes,
- National Insurance number,
- Student loan details,
- Accident at work records,
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us,
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings,
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms,
- leave records including annual leave, family leave, and sickness absence,
- training details,
- your account details for the company's IT systems.

Special categories of data

Special categories of data are defined by the GDPR and include data relating to:

- health, biometrics, religious or political beliefs, ethnicity and sexuality

As your employer we will most likely be processing data related to health.

We will use some special category data:

- in our sickness absence management procedures,
- to maintain records of statutory sick pay or maternity pay,
- to determine reasonable adjustments ,

We process special categories of personal data in order to carry out our legal obligations, exercise specific rights under employment law and provide access to occupational healthcare.

Occasionally we may process special category data with your explicit consent, for example when we ask for any special dietary requirements in the context of planning a company event.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, it may also be collected during your employment. For example we may

need to process details of driving convictions if your role requires driving, or details of criminal convictions via a DBS (Disclosure & Barring Service) check if your role is eligible.

We rely on the lawful basis of legal obligation to process this data where the role requires us to do so, or your consent where checks are not legally mandated.

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references, and membership of appropriate professional bodies required for the role.

Personal data is kept in personnel files and within the company's IT systems.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information e.g. confirming your right to work in the UK.

Sharing your personal data

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you.

We share your data with third parties in order to manage HR records, payroll, benefits, recruitment, professional body certifications, and other specific role related needs which may arise from time to time and for which you will be fully informed.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

We may disclose your personal data if we receive a valid request from the Police or if we receive a court order compelling us.

We use a number of third party systems providers to deliver our services, some of which are cloud-based packages. Where we are using such third party systems we ensure that we

have a data processing agreement in place to protect your rights and comply with data protection laws.

How long do we keep your personal data for?

We aim to retain personal data for no longer than is necessary, which is a core principle of UK data protection legislation.

We will retain your personal data for up to 7 years from the end of your employment unless we have a legal obligation to retain it for longer.

Where we are processing personal data relating to an unsuccessful application for employment, trustee position or voluntary position, we will hold your personal data for a much shorter period, normally 1 year, unless we have your consent to retain it for longer.

How we keep your personal data secure

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

The following key measures help keep us keep your personal data secure:

- Where possible, suitable encryption is used for data at rest
- We use multi-factor authentication where available
- We conduct regular security assessments and penetration testing
- We assess the security practices of our suppliers and partners
- We use encrypted email services where appropriate
- We password protect sensitive documents
- We limit access to personal data to only those members of staff who need it
- All members of staff have confidentiality clauses in their contracts of employment
- We provide regular security training for our staff, volunteers and associates
- We ensure that any paper files are kept in locked cabinets
- Our premises are protected by CCTV

International transfers of personal data

We primarily process data in the UK, our Microsoft Office 365 environment is also hosted in the UK.

However we do use a number of cloud based tools which are based outside the UK, including the USA.

We ensure that we have a lawful basis for such international transfers which most often means that we have Standard Contractual Clauses (SCCs) in place with each provider. These SCCs are mandated by the Information Commissioner's Office (ICO) and aim to safeguard your rights when your personal data are transferred to any nation which lacks an agreement to uphold UK resident's data protection rights by default.

Your Rights

You have the right to:

- **Request access to your personal data** (commonly known as a “data subject access request”). This enables you to receive a copy of the applicable personal data we hold about you and to check that we are lawfully processing it. We will provide copies of applicable personal data, however we are not obliged to provide all personal data which relates to you (for example we can withhold information subject to legal privilege, or information which compromises the privacy of other individuals such as employment references).
- **Request correction of the personal data** that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure of your personal data**. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing of your personal data** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Request restriction of processing of your personal data**. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - If you want us to establish the data's accuracy.
 - Where our use of the data is unlawful but you do not want us to erase it.
 - Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
 - You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer of your personal data to you or to a third party**. 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 automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time where we are relying on consent to process your personal data**. 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. We will advise you if this is the case at the time you withdraw your consent.
- **The right not to be subject to any automated decision-making and profiling**. You have a right not to be subject to automated decision making in any way that significantly impacts you or has legal effects on you. This right does not apply when we are processing data in accordance with a contract with you, however you do have the right to have the methods and logic of the automated system explained to you.

- We do not currently deploy any automated decision making which impacts our employees or potential employees and will tell you should that change,**
- **the right to complain** to us or the supervisory authority if you believe your rights have been infringed.

Please note, some of these rights only apply in certain circumstances and we may not be able to fulfil every request and there may be some circumstances where Anxiety UK is allowed to withhold information from you.

Please contact us using the details in “Who we are” to make any request in relation to your rights under data protection law.

If you have a complaint

If you would like to lodge a complaint with us regarding the processing of your personal data then please contact us using the above details (see “Who we are”).

You also have the right to complain to the Information Commissioner’s Office (ICO). You can contact the ICO on their helpline 0303 123 1113 or online at www.ico.org.uk. If you should contact the ICO they will normally ask you to contact us first.

Review of this privacy notice

We keep this privacy notice under regular review. This privacy notice was last updated in February 2022.