Job Applicant Privacy Notice

Last updated: April 2023

Chugai Pharma Europe Ltd - CPE (Company no. 03486599) and **Chugai Pharma UK Ltd - CPU** (Company no. 02814621), referred to in this notice as **the "organisation"** (which for the purpose of this notice shall be read depending on the company you have applied to work for), are committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you when you apply for a job with CPE or CPU, it also describes how long that information is kept for and the circumstances in which we might disclose it to a third party, in accordance with the General Data Protection Regulation (GDPR) and applicable data privacy law.

The organisation is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. We have appointed a data protection officer (**DPO**) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, please contact our appointed DPO using the details set out below.

How to contact the Data Protection Officer:

Email address:	dataprotection@chugai-pharm.co.uk
Postal address:	Mulliner House, Flanders Road, London W41 NN, United Kingdom
Telephone number:	+44 208 987 5600

The organisation collects and processes personal data relating to potential employees to manage their recruitment. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- Name, address, telephone number, email address
- Gender
- Date of birth
- Employment history, other relevant experience, achievements, skills and qualifications
- The notes and outcome of any interviews or tests which form part of the recruitment process
- Employment references and the results of any pre-employment screening
- Any other additional information provided by you in the context of the recruitment and selection process, such as:

    - information about your nationality and entitlement to work in the UK
    - information about your criminal record, if applicable
    - reports regarding any pre-employment psychometric assessments, where undertaken
    - information about medical or health conditions, including whether you have a

disability for which the organisation needs to make reasonable adjustments
- Any other correspondence relating to your recruitment

How does the organisation obtain and use your information?

The personal information we hold about you comes from the following places:

- your recruitment application and the supporting information you included with it (either directly or via a recruitment agency)
- pre-employment checks, vetting and references from external parties
- information created by the organisation during your recruitment application, such as correspondence with you, interview notes or assessment results

The organisation and the companies that process recruitment related information on our behalf will use your personal information to:

- Evaluate your application and assess your suitability for the role in question
- Make a decision about whether you should be selected for interview and appointment
- Conduct relevant pre-employment screening (e.g. carry out criminal record checks, verify your address, academic qualifications and work experience)
- Review and audit the recruitment process and its outcomes
- Carry out equalities monitoring activities
- With your consent, identify any future employment opportunities with CPE and/or CPU which may be of interest to you

Your personal information will only be accessed and processed by authorised personnel (i.e. recruiting line managers, HR professionals and occupational health professionals) who are involved in the management and administration of the recruitment process and have a legitimate need to access your personal information.

Why does the organisation process personal data?

Under privacy and data protection legislation, the organisation is only allowed to use personal information if we have a proper reason or 'legal basis' to do so. In the case of your recruitment application with the organisation, these 'legal grounds' are:

The organisation has a **legitimate interest** in processing your personal data for:
- running the recruitment process
- ensuring effective general HR and business administration
- responding to and defending against legal claims

Where you have given your **consent** to the organisation, for example:
- Where you agreed we can keep your information to identify any future employment opportunities in CPE or CPU which may be of interest to you

Sometimes we also need to collect or store information that is defined as 'special category personal data'. In the case of your recruitment application this is likely to consist of the following, where you choose to provide it:
- race and ethnic origin
- religion
- health (physical or mental)

- sexual orientation

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Applicants are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

In addition, UK privacy legislation has added information about criminal allegations, proceedings or convictions to the list of special categories compiled under EU law. As before, there are a number of 'legal grounds' we rely on when handling this kind of information, depending on the circumstances, which are:

- Where we have your explicit consent to do so for a particular purpose
- Where it's necessary for carrying out the obligations and exercising specific rights of the organisation or you in the field of employment law
- For the establishment, exercise or defence of legal claims
- Where it is necessary for equality of opportunity or treatment
- Where it is necessary for the prevention and detection of crime or fraud

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the recruitment process relating the role for which you have applied.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with data processing rules, where this is required or permitted by law.

Who has access to data?

The organisation takes the privacy of job applicants very seriously and has a range of policies and processes in place to safeguard their personal information. Your information may be shared internally amongst Chugai Group, including with members of HR, management and managers in the business area in which you have applied. Whenever Chugai shares your personal data with the company group, this will be done on a need-to-know basis.

Access to systems that hold recruitment-related information is restricted to authorised personnel. Your information is stored on systems that are protected by secure network architectures and are backed-up on a regular basis (to a second secure location) for disaster recovery and business continuity purposes; and to avoid the risk of inadvertent erasure or destruction. Anyone with access to personal information held in the organisations systems is required to complete privacy and data protection training on a regular basis.

With whom do we share the information?

The organisation shares your data with third parties in order to obtain pre-employment references from other employers. The organisation also has contracts with third party service providers, who may

provide support in respect our recruitment and selection processes e.g. recruitment agencies and pre-employment psychometric testing service providers. These third parties will process applicant information in accordance with our instructions and make decisions regarding the information as part of the delivery of their services; they are also required to put in place appropriate security measures that ensure an adequate level of protection for personal information. In these circumstances the data will be subject to confidentiality arrangements.

In some circumstances, disclosures of applicant personal information to the police (and other law enforcement agencies) are permitted by the privacy and data protection legislation, if they are necessary for the prevention or detection of crime and/or the apprehension or prosecution of offenders. Each police request to the organisation is dealt with on a strictly case by case basis to ensure that any such disclosure is lawful and proportionate.

The organisation may also disclose your personal information to a third party in the following circumstances:

- If it is necessary to do so in order to establish or defend the organisation's legal rights (i.e. in the context of a court case involving CPE or CPU)
- In an emergency where the health or personal security of an applicant is at risk
- Where the organisation is otherwise required or permitted by law

Transferring information outside the EEA

The organisation and their service providers may process your personal information in countries both within, and outside, the United Kingdom (UK) and the European Economic Area (EEA).

Whenever we transfer your personal data out of the UK or the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield regime which requires them to provide similar protection to personal data shared between the Europe and the US.

Automated Processing and Profiling

Under data protection legislation we have to let you know when we use your personal information to do something 'automatically' using our computers or other systems or use it to make an automated decision (without human intervention) that significantly affects you.

Neither CPE nor CPU makes any recruitment related decisions based solely on the use of automated systems, databases or computer applications.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies (Information Security Policy and Backup and Disaster Recovery Standard Operating Procedure) and controls (such as Role Based Access Control, Auditing, Anti-malware software, Data Encryption, Firewalls, Intrusion Detection Systems, Vulnerability Scanning and Patching, plus others) in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed

except by authorised employees in the performance of their duties. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

If your application for employment is successful, the organisation will then use your personal information to manage and administer its employment relationship with you. If your application is unsuccessful, CPE/CPU will retain your personal information for 12 months from the date on which the relevant recruitment campaign is closed.

This is for the following reasons:

- To respond to correspondence, concerns or complaints
- To maintain records according to rules that apply to us (for example employment law)
- To establish and defend any legal rights

Your rights

As a data subject you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your 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;
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing;
- request a restriction of processing of your personal data; and
- in some cases, request the transfer of your personal data.

If you would like to exercise any of these rights, please contact the DPO.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes to which you originally agreed.

Supervising Body

You have the right to make a complaint at any time to the Information Commissioner's Office (**ICO**), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

Changes to this page

It's likely that we'll need to update this statement from time to time, so check back here regularly to find out more. Your continued use of the site will mean that you accept those revisions.