

Data Protection Regulation (GDPR)

Privacy Statement for Candidates

Daiwa Capital Markets Europe Limited

What is the purpose of this document?

Daiwa Capital Markets Europe Limited is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, temporary worker or contractor) either through an agency or through our website (via email). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation ((EU) 2016/679) (GDPR).

Data protection principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter and/or email;
- information about your current level of remuneration, including benefit entitlements;
- information about your entitlement to work in the United Kingdom;
- Any information you provide to us during an interview.

We may also collect store and use (where relevant) the following “special categories” of more sensitive personal information:

- Information about your race and religious beliefs. We will not ask for this information at the candidate stage, however if you volunteer such information we will process it in order to make suitable adjustments for the interview process and to ensure appropriate equal opportunity monitoring.
- Information about your health, including any medical condition, disability to ensure your health and safety in the workplace and make suitable adjustments for the interview process.
- Information about criminal convictions and offences.

For more detail on why we may collect this information, see below.

How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Obtained from your passport or other identity documents.
- Via the Adobe application form
- Recruitment agent, from which we collect the following categories of data: CV, Cover Letter Contact Details and Salary Expectations.
- Verifile background screening service from which they undertake a Disclosure and Barring Service in respect of criminal convictions and financial/credit checks.

- Your named referees, from whom we collect the previous employment and previous education references.
- Daiwa will only seek information from third parties if a permanent or fixed term job offer has been made to you and we will inform you that we are doing so.

How we will use information about you

We will use the personal information we collect about you to:

Assess your skills, competencies, qualifications, and suitability for the role.

- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.
- To maintain the physical security of our premises including by CCTV recording and keeping records of visits to our offices and issuing security passes.

We process your personal information as we have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your CV and covering letter and/or email, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is suitable and meets the criteria to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the meeting to decide whether to offer you the role. If we decide to offer you the role, we will then take up references, and carry out criminal record and credit checks if relevant for the role, and we may also carry out any other check if relevant, before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

How we use particularly sensitive personal information

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process.
- Where you volunteer such information, we will use information about your race or religion, to ensure meaningful equal opportunity monitoring, reporting and to make appropriate adjustments for the interview process.

Criminal Convictions and Credit Checks

Where relevant, we envisage that we will process information about criminal convictions and credit checks.

We will collect information about your criminal convictions and credit history if we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory). For some roles, Daiwa is obliged to seek information about criminal convictions and offences. Where the organisation seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data Sharing

Why might your personal information be shared with third parties?

Your information may be shared internally for the purposes of the recruitment exercise including between Daiwa Capital Markets Europe Limited and its affiliates and branches. This includes interviewers involved in the recruitment process, managers in the business area with a vacancy and Compliance staff if access to the data is necessary for the performance of their roles.

Daiwa will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The organisation will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service via a third party, to obtain necessary criminal and credit records checks. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Your data may be transferred outside the European Economic Area (EEA) where we use a third party platform such as Adobe, the role is sufficiently senior or you will have a reporting line into our parent company based in Japan. Such data will only be transferred: (i) once it has been suitably anonymised; (ii) we have obtained your explicit consent; or (iii) appropriate safeguards have otherwise been implemented.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

Data will be stored in a range of different places, including on your application record, in the HR management systems, on the Adobe cloud platform and on other IT systems (including email).

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

DATA RETENTION

How long will you use my information for?

We will retain your personal information for a period of six (6) months after we have communicated to you our decision about whether to employ you directly or via an employment agency. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy. Destruction of your personal information will involve deletion of the data physically and from our active electronic files and be beyond the use of those staff involved in the recruitment process, however this may be retained on back-ups in order to comply with other regulatory and legal obligations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

Rights of access, correction, erasure, and restriction

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

Request erasure of your personal information. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below).

Object to processing of your personal information 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. You also have the right to object where we are processing your personal information for direct marketing purposes.

Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing or via email at DPO@uk.daiwacm.com

Right to withdraw consent

When you applied for this role through a recruitment agency, you may also have provided consent to us processing your personal information for the purposes of the recruitment exercise. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact the Data Protection Officer at DPO@uk.daiwacm.com. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely.

Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO at DPO@uk.daiwacm.com. 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 or the supervisory authority in your home territory. We would however appreciate the chance to deal with your concerns before you approach the ICO or a relevant supervisory authority, so please contact us in the first instance.

I, _____ (candidate name), acknowledge that on _____(date),

I received a copy of the Candidate Privacy Notice and that I have read and understood it.

Signature

.....

Name

.....