Privacy Notice for Applicants

Introduction

This notice applies to all applicants to roles in the Equifax group in Europe. It does not form part of any contract of employment or other contract to provide services. As an applicant to the Equifax group within Europe specifically the UK, Ireland, Luxembourg, Spain or Portugal, you are applying to one of the following companies:

- Equifax Limited
- TDX Group Limited
- Integrated Debt Services Limited
- Equifax Technology Ireland Limited
- Equifax Commercial Services Limited
- Equifax Luxembourg S.a.r.l.
- Equifax Iberica SL
- TDX Indigo Iberia SL
- Credinformações – Informação de Crédito, Lda

together, the "Group".

The member of the Group of which you are applying to will be the data controller in respect of your personal data.

References to your "personal data" will, as the context requires, include "special categories of personal data", which involves more sensitive information about you.

This privacy notice describes how we are or will be processing personal data about you during and after your working relationship with us. "Processing" covers such actions as collecting, using, storing, disclosing, erasing or destroying your personal data.

Identity and contact details of the data controller and the data protection officer

You are applying to one of the Equifax group companies. We are a "data controller". This means that we are responsible for deciding how we process personal data about you.

The contact details of the group companies can be found in Appendix 1.

A data protection officer (DPO) has been appointed for our companies as required, contact details are as follows:

Equifax Ltd UKDPO@equifax.com

Spain DPO@equifax.es

The DPO is responsible for overseeing compliance with this privacy notice and for handling any data protection queries or issues involving us. However, if you have any concerns, please speak to your recruiter in the first instance.

What type of personal data do we process about you?

We may process the following categories of personal data about you:

- Recruitment information (including any details provided by third party referees over which we have no control (should you have accepted a job offer but then subsequently decline or have your offer withdrawn due to unsatisfactory references or any other reason) and other information held on CV or passed to us by our recruitment agency, Seven Step or contractor agency.

- Copies of right to work verification details (such as passport details) provided by you to us.

- Other recruitment information (including third party references and other information held on CV or your cover sheet).

- Previous employment history, including education background information.

- Personal contact details such as name, title, address, telephone numbers, and personal email address.

- Your date of birth, gender, marital status and details of dependants.

- Your personal public service number.

- CCTV footage in respect of your visits to Group premises.

We may also process the following "special categories" of more sensitive personal data if you chose to provide it:

- Information about your race or ethnicity, religious beliefs, sexual orientation, nationality and immigration status.

- Information about criminal convictions and offences.

- Information about your trade union membership or that of a companion at a disciplinary/grievance meeting.

How do we collect your personal data?

We will collect personal data about you through the application and recruitment process, either directly from you or from our recruitment agencies. We may sometimes collect additional information from third parties including former employers (in the form of references).

What are the legal bases and the purposes for which we process your personal data?

We will only use your personal data as permitted by law. We will typically use your personal data in any of the following circumstances:

1. Where we have your consent to do so.
2. Where we need to perform the contract we have entered into with you.
3. Where we need to comply with a legal obligation.
4. Where the processing is necessary to perform a task in the public interest.

5. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We are required to specify what the legitimate interests are (see below for further details).

The examples given below do not form an exhaustive list of purposes for which your personal data will be processed, and we reserve the right to add to them at any time.

Consent

If your personal data is sent to us by a recruitment agency, the agency will firstly have obtained your consent to release that information to us. Once we have your personal data, we will process that information in accordance with the lawful bases set out above and explained as follows.

Necessary to comply with a legal obligation

The following purposes come under this category:

- Checking that you are legally entitled to work in the country of which you have applied to - your nationality and immigration status and information from related documents, such as your passport and other identification such as driving licence and immigration documentation.
- Handling any legal disputes involving you or third parties, including accidents at work.
- To prevent fraud.
- To comply with any necessary regulatory obligations.

Necessary to perform public interest task

- The completion of equality and diversity monitoring forms in order to redress diversity imbalance in the workplace.

Necessary for our legitimate interests or those of a third party

Recruitment:

- Personal data provided by you on new starter forms or temporary new starter forms, specifically your gender, mobile phone number, next of kin details.
  The legitimate interests are identity and reporting to relevant authorities, and for emergency contact/disaster recovery.
- Personal data provided by you on your CV and cover sheet.
  The legitimate interest is to ascertain your suitability for employment/engagement.

HR:

- Personal data obtained through our external background screening providers (which may include address history, employment history, education background, criminal records information (see below for more details), credit history and employment history.
  The legitimate interests are verifying the information provided by you on your CV, verifying the relevant qualifications/requirements for the role, verifying your employee declaration, as necessary for compliance and as required by regulatory bodies, and to ensure that there are no issues with your credit history that could place unnecessary risks on us or third parties.
- Personal data obtained through CCTV.
  The legitimate interest is the protection of health and safety (including the identification of individuals on premises in the event of a fire or other serious incident) and the prevention and detection of criminal acts.

If you fail to provide personal data

If you fail to provide certain information when requested, and we are unable to obtain it from a third party or publicly available source, we may not be able to perform recruitment activity necessary for our legitimate interests, or we may be prevented from complying with our legal obligations (such as ensuring you have legal right to work status in the Country of application). Depending on the nature and importance of the information requested, we may either have to cease the recruitment activity or withdraw an offer of employment or engagement.

How we use special categories of personal data

"Special categories" of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. Unless you go on to become a worker of the Group, it is unlikely that we will use special category data relating to you other than in the following circumstances:

1. Where it is needed in the public interest, such as for equal opportunities monitoring (where such information is provided by you).
2. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

We may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may use your special categories of personal data in the following ways:

- Information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- Information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and the health and safety of others and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits. We may obtain information relating to your physical and mental health from medical and occupational health professionals we engage and from our insurance benefit administrators.
- Information about your race or national or ethnic origin, religious or other beliefs, to ensure meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

We will only use information relating to criminal convictions where the law allows us to do so for determining suitability for employment.

We may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

With whom might we share your personal data?

We may have to share your data with third parties, including third-party service providers and any sub-contractors of those service providers. We will share your data with our trusted global recruitment partners Seven Step and if relevant for contractor activities, contractor agencies.

We require third parties to respect the security of your data and to treat it in accordance with the law.

If we need to transfer your personal data outside the EU we will ensure that a lawful basis is used for doing so. For instance, our HR system, Workday, where your application will be processed, is located on servers in the USA. Whilst the USA is not currently considered to have "adequate" data protection laws, EC standard contractual clauses are put in place with non-EEA countries. This means that we consider any transfer of data to Workday can be considered to be subject to appropriate safeguards.

Why might we share your personal data with third parties?

We may share your personal data with third parties where required by law for example, with tax authorities, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

How secure is your information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes unless they are data controllers in their own right in relation to your personal data. Where they operate as our "data processors" (ie they process your personal data on our behalf and acting only on our instructions), we only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about disclosure to other third parties?

We may share your personal data with other third parties, for example in the context of the possible sale or restructuring of the Group. We may also need to share your personal data with a regulator, to external legal or other professional advisers, or to otherwise comply with the law.

How long will we retain your personal data?

If you are unsuccessful with your application to join us, or if you choose not to join us, we will retain your information for no longer than 12 months for the purpose of defending any legal claims. If you are unsuccessful with your original application but are a strong contender for other roles, it is our normal practice to retain details contained in application forms for a period of 12 months unless you indicate otherwise.

If you are successful in your application for a role with us and take up that role, you will be issued with a different privacy notice which reflects your new status with us.

What are your rights and obligations as a data subject?

Your rights in connection with personal data

Under certain circumstances, by law 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 personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data 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 data. This enables you to ask us to delete or remove personal data, but only 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 exercised your right to object to processing (see below).

- 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.
- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal data to another party.
- Request the data which you have provided to us and which is processed by us by automated means, in a commonly-used machine readable format.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact the DPO in writing, or contact AskHR@equifax.com.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

What are your rights to withdraw consent to processing?

You may withdraw your consent to allow us to continue processing your personal data, but only where consent was sought as a lawful means of processing your personal data.

In the limited circumstances where you may have provided your consent to the processing of your personal data 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 you originally agreed to through that consent, unless we have another legitimate basis for doing so in law.

What are your rights to lodge a complaint about the way in which your personal data are being processed?

Firstly we would urge you to contact the DPO in writing. If you are not satisfied with the DPO's response, or if the entity you are contacting doesn't have a DPO you may contact:

United Kingdom - the Information Commissioner's Office ("ICO") Details of how to proceed can be found via the website https://ico.org.uk/concerns/.

Republic of Ireland – the Data Protection Commission, details of how to proceed can be found via the website https://www.dataprotection.ie/docs/Raise-a-Concern/1716.htm

Luxembourg - the National Commission for Data Protection, details of how to proceed can be found via the website https://cnpd.public.lu/en/particuliers/faire-valoir.html

Spain - la Agencia Española de Protección de Datos ("AEPD"), details of how to proceed can be found on the website http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/index-ides-idphp.php

Portugal – Comissão Nacional de Protecção de Dados , details of how to proceed can be found on the website https://www.cnpd.pt/english/bin/contacts/contacts.htm

You are free to contact the Commissioners at any time. However, the DPO may be able to answer your concerns or questions more quickly.

Personal data received from someone other than you

If we obtain personal data from someone other than you (such as a referee, or information from a regulator), we will provide you with information as to the source of such personal data and, if applicable, whether it came from publicly available sources.

What data security measures are in place to protect my personal data?

We have put in place measures to protect the security of your information. Details of these measures are available upon request. Employee/contractor/candidate personal data held securely within the HR system, Workday. Access to Workday records in relation to other workers is restricted to those who need to access them, for example, line managers and HR. You are also referred to our Corporate Information Security Policy which sets out the information security framework in operation. This will apply to your personal data as well as personal data of third parties.

Third party data processors will only process your personal data on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

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. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

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.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We do not propose to rely on automated decision making. However, please note that applicants for roles through our recruitment partners will be asked:

1. if they have the right to work in the UK (for roles in the UK);
2. if they agree to background screening; and
3. if they believe they have the skills for the role.

If an applicant answers “no” to any of these questions, then the application will fail, as these are the minimum legal and logistical requirements needed for the role.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

If you have any questions about this privacy notice, please contact the DPO where available in country or AskHR@equifax.com.