Privacy notice for employees, workers and contractors

Introduction

This notice applies to all employees, workers and contractors ("Workers"). It does not form part of any contract of employment or other contract to provide services. As a Worker for the Equifax group within Europe specifically the UK, Ireland, Luxembourg, Spain or Portugal you are employed or engaged by one of the following companies:

- Equifax Limited
- TDX Group Limited
- Integrated Debt Services Limited
- Equifax Technology Ireland Limited
- Equifax International Treasury Services Unlimited Company
- 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 by which you are employed or engaged 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 employed or engaged by 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 UK & Wexford UKDPO@equifax.com

Equifax Dublin GlobalDPO@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.

What type of personal data do we process about you?

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

- 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.
- Next of kin and emergency contact information.
- Your personal public service number.
- Your bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- If your role involves driving, a copy of your driving licence.
- Current employment records (including job titles, work history, working hours, place of work, start date, training records, qualifications and professional memberships and professional body membership numbers).
- History of pay, bonus, student loan information and other benefits
- Details of performance and appraisals.
- Where applicable, disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.
- Photographs.
- Reason for leaving and confidential references provided by us, alongside information required in order to provide reference information.
- Details of any payments made on termination.

We may also process the following “special categories” of more sensitive personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation.
- Information about your health, including any medical condition, health and sickness records.

- 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 typically collect personal data about employees, workers and contactors through the application and recruitment process, either directly from candidates or from other trusted businesses or persons (Appendix 2) with whom we have an arrangement in place to obtain recruitment services. We may sometimes collect additional information from third parties including former employers (in the form of references). There are a multitude of forms that you may, during the course of your employment, complete and on which you provide personal data, and these forms are collected and processed by the HR team.

We also use background checking companies, who gather reference, credit, criminal conviction and other suitability data, which they may, where no clear certification has been obtained, provide to us.

We will collect additional personal data in the course of job-related activities throughout the period of your working for us. For instance, if you complete an Equality and Diversity Monitoring form, this may reveal certain information about your race or ethnicity, whether you consider yourself to be disabled, your sexual orientation, religion and belief and gender monitoring.

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

All employees have the option of having their photographs uploaded onto workday so that their picture appears by their profile. Use of your personal data on workday for these purposes is entirely voluntary and you can withdraw your consent at any time by removing your photograph from workday.

Necessary for the performance of a contract with you

The following purposes come under this category:

- Ensuring you are paid and that you have the correct tax and NICs and any other appropriate deductions (season ticket loans, student loans etc) deducted from any payments.
- Management and planning, including accounting and auditing.

- Administering your contract (eg by reviewing your working hours to check holiday and rest break entitlement, checking your start date for eligibility for age-related benefits).
- Making decisions about salary and other payment reviews.
- Assessing your suitability for the role, including decisions about promotions or other role changes.
- Where applicable, providing you with benefits including holiday, pension (including liaising with your pension provider/administrator), private medical insurance, and life assurance where such benefits form part of your contract, in addition voluntary benefits you opt in to.
- Ensuring (as far as possible) that your wishes are met regarding death in service payments and that your next of kin are contacted in the event of an emergency (hence the need for third party information, usually comprising details of partners and/or dependants).
- For enabling you to apply for flexible working or other family rights (such as maternity, paternity, parental leave) – this requires details of your partner/dependants.

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 are employed - 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

Compensation and Benefits:

- Provision of benefits that may not be deemed to be contractual, such as participation in the cycle to work scheme.
  The legitimate interest is to ensure you receive and we administer benefits which are not necessary for the performance of your contract.

Learning and Development:

- Personal data provided by you on training forms, and agreements, internal e-learning forums,, conference application forms, study and exam booking forms, supplier forms (including training provider forms).
  The legitimate interest is to ensure your continuing learning and development needs are addressed and documented.

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 in relation to grievance and disciplinary issues.
  The legitimate interest is to address issues and concerns from either side in the employment relationship.
- Personal data obtained in relation to performance and appraisal processes.
  The legitimate interest is to ensure your performance is assessed so that if there are improvements required they can be addressed and all levels of performance can be identified and, if appropriate, rewarded.
- Personal data obtained in relation to the monitoring of our IT systems.
  The legitimate interest is to ensure compliance with our IT policies and to ensure the integrity of our IT systems, to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- 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.
- Personal data obtained through swipecard technology.
  The legitimate interest is to ensure only authorised members of staff or authorised visitors are on site, thereby safeguarding systems and property from unauthorised access, destruction or theft. This information may also be used to provide evidence in relation to any issues regarding timekeeping and attendance.
- Reference information – it is our normal policy to provide only basic factual information about ex-employees (or departing employees) to prospective new employers. However, where we have legitimate concerns which, if not disclosed to a prospective new employer, could place us in breach of our duty of care to that prospective new employer, such information as we reasonably considers necessary will be disclosed in order to satisfy that duty.
- Running analysis of absence, performance, retention and benefits to establish whether the workforce is functioning well and happy.
  The legitimate interest is to ensure that the workforce is functioning well and to assess whether any future changes are required.

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 the contract we have entered into

with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers). Depending on the nature and importance of the information requested, we may either have to cease employing or engaging you 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. We may process special categories of personal data in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our data protection policy and related policies (such as managing sickness absence, complying with health and safety obligations and making reasonable adjustments to your workplace).
3. Where it is needed in the public interest, such as for equal opportunities monitoring (where such information is provided by you).
4. 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 Equifax Inc and sub processers within the Global Equifax group companies, third parties, including third-party service providers and any sub-contractors of those service providers. See below for further details.

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 personnel file is stored, 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.

Which third-party service providers process my personal data?

"Third parties" includes third-party service providers, including contractors and sub-contractors. This will include:

1. our pension provider (currently Aviva or New Ireland, depending on where you are engaged or employed);
2. benefits brokers (currently Mercer) and providers (for example, for life assurance, private medical insurance); and
3. our payroll administrator (if applicable).
4. our recognition and shares partners
5. travel scheme providers
6. IT providers

A full list of third-party service providers can be found in appendix 2.

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?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our retention policy in People Link under Working at Equifax, privacy.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal data in accordance with our retention policy.

What are your rights and obligations as a data subject?

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

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 is held securely within the HR system, Workday. All workers should avoid saving any personal data about any subject outside this portal, including any information relating to direct reports. 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.

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.

Version control		
Document created	April 2018	
Document updated	March 2019	Appendix 2 Benefit providers added
Document updated	July 2019	Appendix 1 UK registered address updated
Document updated	February 2020	Equifax International Treasury Services Unlimited Company added
Document updated	April 2020	Version control added
Document updated	May 2020	Appendix 2 Share purchase provider added
Document updated	June 2020	Appendix 2 benefit and wellbeing partners added
Document updated	December 2020	Duplin DPO contact email added. Appendix 2 benefit providers added. Consent example updated to remove reference to outlook

Appendix 1

Group Companies:

Equifax Limited
Address: 1 Angel Court, London, EC2R 7HJ

TDX Group Limited
Address: 8 Fletcher Gate, Nottingham, NG1 2FS

Integrated Debt Services Limited
Address: 8 Fletcher Gate, Nottingham, NG1 2FS

Equifax Commercial Services
Address: IDA Business & Technology Park, Rosslare Road, Drinagh, Wexford, Ireland, Y35 RF29

Equifax Technology Ireland
Address: Fourth Floor, Bloodstone Building, Blood Stoney Road, Dublin 2, Ireland

Equifax International Treasury Services Unlimited Company
Address: 25 - 28 North Wall Quay, Dublin, D01H104

Equifax Luxembourg S.a.r.l.
Atrium Business Park, 33 rue du Puits Romain - Boite 6, L-8070 Bertrange, Grand Duchy of Luxembourg

Credinformações – Informação de Crédito, Lda.,
Address: Av. D. João II, Lote 1.06.2.1ª Piso 3, Fração 304, em Lisboa

Equifax Ibérica S.L.
Address: Paseo de la Castellana, 259D, 26º, 28046, Madrid, Spain

TDX Indigo Iberia S.L.
Address: Calle Velazquez 50, 5ª planta, 28001 Madrid

Appendix 2

Trusted businesses, systems or persons:

Adobe (document signing)
Academy of Executive coaching
ADP & Softcom (Payroll)
Aires (Immigration support)
Arriva rail north Ltd (travel provider)
Aviva (Pension provider)
Ashbourne connect (Travel provider)
Apple (Childcare vouchers)
Barclay Simpson Associates Ltd
BI Worldwide (Bravo - recognition)
Bus eireann (Travel provider)
Bupa (healthcare provider)
Bupa Health Clinic
Centre for Civil Society (Living wage foundation)
CIFAS (Internal fraud database. See appendix 3)
Carlson Wagonlit (Travel booking)
Charles Cameron (Benefit provider)
Centre for creative leadership
Charities Aid Foundation (Give as you earn)
Cherry professionals
Concur (Expenses)
Cope occupational health
Corecom
Cushon (Benefit provider)
Cyclescheme (Benefit provider)
DAC Beachcroft LLP
Docusign (Document online signature)
Dublin bus (Travel provider)
Eversheds Sutherland LLP
First Advantage (Background screening)
Franklin covery europe Ltd
Freeths
Fusion Search
Fruition IT
Gemma Hayes Recruitment
General register office
general investment trust (Irish pension governance)
Gift voucher shop (employee benefits)
Global radio services limited
Groupscheme (Benefit provider)
Halborns Ltd (Legal advisor)
Hands on health UK wellbeing Ltd (wellbeing)
Harnham
Harvey nash ltd
Harmless CIC (wellbeing)
Hayes - UK &I
Health assured (EAP)
Howden (Benefit provider)
Iain Macdonald
I Realise
Innecto people consulting (benefits)
Interquest
Irish rail (Travel provider)
Irish life (healthcare
Identity manager (Access system)
Incorpore (benefit provider)
IBM (IT service provider)
Korn Ferry
Lee Hecht Harrison Penna Limited
LiveSmart (benefit provider)
LUAS (Travel provider)
McKenzie
Medmark (Occupational health)
Metrocard (Travel provider)
Mercer (Benefits provider)
Metlife (Insurance benefit)
Michael Page International
Moloney Search (recruitment agency)
Morgan Mckinely
NCT Bus (Travel provider)
Netdocs (Filing system)
New Ireland (Pension provider)
Northern (Travel provider)
Nudge (Benefit provider)
One4all (Cycle to work provider)
PageGroup
Pennies from heaven (Charitable salary sweep)
Personal Audit System (P11D)
Pincent masons
Pinnacle performance company
PMI Health Group (Occupational health)
Pump court chambers
PwC (Irish pension auditor)
Qualtrics (Opinion surveys)
Oracle (Purchase requisitions)
Randstad
Right management Inc
Robert Half Ltd
Robert Walters operations limited
Russam GMS
Security Watchdog (Background screening)
ServiceNow (AskHR – general queries)
Salary Finance (Benefit provider)
Simply health (Benefit provider)
Simard T/A The Gourmet society (Benefit provider)
Sitel (IT service provider)
Smith Stone Walters (Immigration support)
Stormfront (Benefit provider)
Swods express (Travel provider)
Softcom (Payroll)
The writer Ltd
The Queens hotel
Total publishing network SA
Tramlink (Travel provider)
Transition Partners
TrustID (Background screening)
TCS (IT service provider)
UBS (Stock and equity provider & ESPP)
Utmost (benefit provider)
Ventula consulting (recruiters)
Weare unstuck Ltd
West Yorkshire Passenger (travel provider)
Wexford Credit union (Benefit provider)
Williams Lea
Workday (HR Information System)
WSL (Benefit provider)
Xpertise recruitment
York Test (benefit provider)
Zurich (Insurance benefit)
4It

Appendix 3

Internal Fraud Database (UK Only)

We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by their staff and potential staff. "Staff" means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.

2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct and to verify your identity.

3. Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.

4. We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.

6. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

CONSEQUENCES OF PROCESSING

7. Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).

8. A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.

DATA TRANSFERS

9. Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

YOUR RIGHTS

10. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data is erased or corrected, and request access to your personal data.

11. For more information or to exercise your data protection rights please, please contact us using the contact details provided.

12. You also have a right to complain to the Information Commissioner's Office which regulates the processing of personal data.