



Privacy Notice for Employees and Applicants

Document Information:

Version	1.0
Author	Amanda Hamilton
Approved By	Harry Kounougakis
Last Reviewed	2025.08.01
Next Review	2026.08.01



About this Notice

This privacy notice (**Notice**) explains how Savanta and its associated Brands (**we, our, us, Savanta**) processes the personal data of staff including workers such as casual workers, agency workers, contractors, interns, volunteers, those workers we employ via our chosen employer of record partners and protective staff such as job applicants. It also explains your rights under data protection legislation.

Please note that any references to "employment" or "staff" are not intended to imply or confer any employment rights to non-employees.

This Notice applies alongside any other information Savanta provides about a particular use of personal data, for example when collecting data via an online or paper form.

If you are an employee based in California, please see our "Privacy Notice for the Collection for California Employees and Applicants".

Data Controller and Data Protection Officer details

For the purposes of any applicable data protection laws in England and Wales, including the Data Protection Act 2018 (DPA) the UK General Data Protection Regulation (UK GDPR) and General Data Protection Regulation EU 2016/679 (EU GDPR), Savanta is the Data Controller of your personal data. Next 15, Savanta's parent company, has appointed a Data Protection Officer, who can be contacted via:

- Email at dpo-hub@next15.com or
- By writing to: FAO Data Protection and Privacy Office, Savanta, 60 Great Portland Street, London, W1W 7RT.

How we collect your information

We may collect your personal data in a number of ways, for example:

- when you request information / assistance via an online form.
- via affiliate partners that you have consented / requested to provide Savanta with your data. This could include recruitment providers, partnership websites and or job mailing lists.
- from the information you provide to us before making a job application, for example when you come for an interview;
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters;
- from third parties, for example our vetted and approved reference and background checking vendors, the Disclosure and Barring Service (DBS) (if this is applicable – see the section below on Criminal Convictions Data) and your previous or current employers, in order to verify details about you and/or your application to work for us;

- from our chosen professional employer organisation and/or employer of record that we partner with (if this is applicable please see the section below on Employer of Record Appointments);
- during the course of your employment or engagement with us as a member of staff, for example when you provide or update your contact details, when you or another member of staff completes paperwork regarding your performance appraisals, staff surveys, when you take part in an activity / event and in the course of fulfilling your employment (or equivalent) duties more generally; and
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

The type of information we collect

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

Contact and communications information, including:

- your contact details (including email address(es), telephone numbers and postal address(es));
- contact details for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this Notice;
- records of communications and interactions that we have had with you;

Biographical, educational and social information, including:

- your name, title, gender, nationality and date of birth;
- your image and likeness as captured in photographs, in recorded video calls and or presentations. We may also process data of this nature taken at corporate events - for more information on this please see our **Savanta Global Events Privacy Notice**;
- details of your education and references from your institutions of study;
- lifestyle information and social circumstances;
- your interests and extra-curricular activities;
- third party profile information such as your LinkedIn profile during recruitment and selection;
- information that evidences periods of residency (such as utility bills, proof of mortgage and travel) or financial circumstances (such as bank statements and proof of income);
- information that evidences your family relationships (such as a birth, adoption, marriage or civil partnership certificate);
- national insurance number (or other tax identification number) and your passport number or national identity card details, country of domicile and your nationality;
- Right to Work details.



We will also allocate you a unique staff number and username.

Financial information, including:

- your bank account number(s), name(s) and sort code(s) (used for paying your salary and processing other payments);
- your tax status;
- pension membership;

Work related information, including:

- details of your work history and references from your previous employer(s);
- start date and if different, the date of your continuous employment;
- leaving date and your reason for leaving;
- location of employment or workplace;
- employment records including copies of right to work documentation, references, job title, work history, working hours, holidays, training records, compensation history and performance information;
- disciplinary and grievance information;
- your personal data captured in the work product(s) you create while employed by or otherwise engaged to work for Savanta;
- communications sent or received using work related communication systems;
- details of your professional activities and interests;
- your involvement with and membership of sector bodies and professional associations;

Online identifiers, including;

- details of your IP address, browser type and operating system when you visit our website or in relation to our IT set up.

Special Categories Data

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data and information about criminal convictions and offences, including information:

- revealing your racial or ethnic origin, data related to your religious beliefs, your sex life and/or sexual orientation;
- information concerning your health, medical conditions and disabilities;
- details around trade union membership;
- concerning criminal convictions (see the section below on Criminal Convictions Data).

For employees who reside in California please see Schedule 1: United States of America where we provide a fuller explanation the definition of special categories data under the CCPA/CPRA

How we use your personal data

Subject to applicable law, your personal data may be processed by us for the following purposes:

- Recruitment and selection
- To evaluate applications for employment and make decisions in relation to selection of employees;
- Pre-employment screening including, where relevant and appropriate, identity check, address records, right to work verification, prior employment and reference check, education qualifications, credit check, financial sanction check and criminal record checks (see the section below on Criminal Convictions Data);
- To make job offers, providing contracts of employment or engagement and preparing to commence your employment or engagement where you accept an offer from us;
- To contact you should another potentially suitable vacancy arise;
- To deal with any query, challenge or request for feedback received in relation to our recruitment and selection decisions.

Automated decision making and profiling

Your data will not be subject to automated decision making or profiling save for the following exceptions:

- Communications sent and received using work related chatbot systems including, but not limited to, the Savanta Chatbot, Microsoft Copilot, or Google Gemini may be stored for tracking and product improvement purposes.
- Where personal data is entered by the user into these work related chatbot systems, this information may also be collected and stored for tracking and product improvement.

Ongoing management

- to manage and maintain HR records, files and systems, including technical support and maintenance of HR systems and managing electronic and hard copy records in line with retention schedules;
- providing and administering remuneration, benefits, pensions and incentive schemes;
- to make appropriate tax and national insurance deductions and contributions;
- identifying and communicating effectively with employees;
- where appropriate, publishing internal or external communications or publicity material, including via social media;
- managing and operating performance reviews, capability reviews, attendance and talent programmes;

- managing grievances, allegations (e.g. whistleblowing, harassment), complaints, investigations and disciplinary processes, and making related management decisions;
- training, development, promotion, career and succession planning;
- business continuity planning and responding to active incidents;
- processing details with employee consent of membership of trade unions, works councils and other employee representative bodies.

Absence management and Health and Safety

- processing information about absence;
- processing medical information regarding physical or mental health or condition to assess eligibility for incapacity or permanent disability related remuneration or benefits:
 - determine fitness for work
 - facilitate a return to work
 - make adjustments or accommodations to duties or the workplace
- making management decisions regarding employment or engagement or continued employment or engagement or redeployment;
- conductin related management processes.

Compliance monitoring, security and systems use

- measuring the performance of Savanta's IT systems by monitoring usage of systems;
- auditing, monitoring, investigating compliance in relation to our policies, applicable law, the prevention and detection of criminal activity and to protect our assets and premises;
- in order to bolster our cyber security mitigation efforts across Savanta such as the implementation of data leak prevention solutions or anti phishing technologies.
- responding to legal and regulatory requests
- complying with lawful requests by public authorities, disclosure requests, or where otherwise required or authorised by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside the country or jurisdiction to which you are resident or employed.
- processing background checks for those categories(s) of employee that require it (see the section below on Criminal Convictions Data).
- using explorations and security tools in order to comply with requests made under data protection legislation. Please note that if we intend to use any tools of this nature in order to gather data for this purpose you will receive a memo in advance of the execution of search. For more information in relation to this please see our Data Subject Rights Request Policy.

Termination of employment and managing post-employment relationships

- Complying with reference requests where we are named by the individual as a referee;
- Administering termination and post-termination matters, e.g. outplacement services, liaison with employee legal representatives, enforcing restrictive covenants, expense reimbursements, employee benefits, conduct termination and post-termination litigation.

Special categories of data

In addition to what is set out above we process special categories of personal data for the reasons set out below. We will process this data on the basis that such processing is necessary to carry to meet our obligations under the law and to exercise rights (both yours and ours) in relation to your employment.

In particular we process the following types of special category personal data for the following reasons:

- your physical or mental health or condition(s), for example, where we are required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment – including as part of the recruitment process if necessary;
- in order to monitor our compliance with equal opportunities legislation;
- in order to investigate a complaint made by you or others, for example concerning discrimination or whistleblowing;
- administering family friendly leave;
- if it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention;
- if it is necessary for the establishment, exercise or defence of legal claims;
- in order to promote equality, diversity and inclusion (EDI) initiatives in the workplace; or
- where we have your explicit consent to do so.

Please note that if we process your special categories data in order to promote EDI in the workplace or to provide information to regulators, governing bodies or professional bodies to which you or Savanta is a member, we will only ever provide aggregate data or data that does not identify you as an individual. For more information, please contact the People Team or the Data Protection and Privacy Office.



Legal basis for processing your data

Every time we process personal data we must have a legal basis upon which to rely.

If you have any queries regarding the legal basis for processing your personal data please contact the Data Protection and Privacy Office.

We will only collect, use and share your personal information where we are satisfied that one or more of the following legal bases apply:

Performance of Contract

The processing is necessary for the performance of a contract to which you are a party or in order to take steps, at your request, prior to entering into such a contract, for example collecting bank details to pay your salary or processing information to provide you with the contractual benefits to which you are entitled.

Legal and Regulatory Obligation

The processing is necessary for compliance with a legal obligation or regulatory obligation to which we are subject such as transferring personal data to local tax authorities, providing up to date background checks on certain categories of employees (for example if we have an FCA regulated client who requires this check as part of their legal and regulatory obligations), avoiding unlawful termination, meeting statutory records keeping requirements or in order to comply with any requests from the FCA or other regulators as they may apply to Savanta.

Legitimate Interest

The processing is necessary for the legitimate interests pursued by Next15, Savanta or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal information. When we use legitimate interest as our legal basis for processing your information we conduct an assessment in order to risk assess our activities. Our legitimate interests include our interests in running Savanta in a professional sustainable manner, in accordance with all relevant legal and regulatory requirements and in line with industry best practice.

Consent

The processing is based on your consent. Where consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and that we can clearly demonstrate that your consent was given to us via an affirmative action on your part.

Information regarding such processing will be provided to you at the time that consent is requested. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent.

Vital Interests

The processing is necessary in order to protect an individual's vital interests in circumstances where there may be a life-threatening accident or illness as set out above.



Criminal Conviction Data

You may be asked to provide Savanta with details of criminal convictions where your role requires a DBS check. We will only use the criminal convictions data for the purpose for which it was collected and it will only be retained for a limited period with the upper limit being 6 months in line with legal and regulatory guidelines.

If we are required by law to conduct criminal background checks, the lawful basis upon which we will rely is that processing is necessary for the purposes of fulfilling our or our clients' obligations under employment, social security and social protection law and the condition under schedule 1 part 1(1) of the Data Protection Act 2018 has been met.

Further information can be found within Next 15's Special Categories Data and Criminal Offence Data Processing Policy. If you would like a copy of this policy document please contact the Data Protection and Privacy Office.

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 the above rules, where this is required or permitted by law.

Employer of Record appointments

If your engagement with Savanta has been facilitated by one of our Employer of Record partners, then please ensure that you have also read their Privacy Notice in order to understand how they will process your personal information as they are a separate legal entity. If you require any help in understanding your rights under their notice please contact the Data Protection and Privacy Office.

Data sharing

For the above purposes, personal information may be transferred within or outside of the jurisdiction where you are employed, perform work or where you reside, either within our Group or to third parties, including, but not limited to:

- any holding company, subsidiary, affiliate of Savanta as regulated by Next 15's Intra Group Data Transfer Agreement;
- with our chosen professional employer organisation and/or employer of record that we partner with;
- certain third parties such as suppliers and service providers including payroll, pension providers to whom we may disclose personal information when required by law or court order, or as requested by any government or regulator or law enforcement authority or agency.



Savanta may also disclose personal information to a third party where it is necessary to do so in order to protect or pursue our legitimate interests (ensuring this is proportionate and limited to information which is strictly necessary for the purpose of the processing activity). This may include, but not be limited to, disclosure to a party with whom we are in negotiation for the sale or transfer of a business, assets or services. Savanta will take appropriate steps to ensure that the recipient of personal information in such circumstances puts in place an adequate level of protection for such personal information in accordance with applicable legal requirements.

If you would like further information in relation to third parties that we share your data with please contact the Data Protection and Privacy Office.

How secure is my information with third-party service providers and other entities within our group?

All of our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. 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.

International data transfers

There may be circumstances where Savanta shares or discloses data outside the jurisdiction where you are employed, perform work or where you reside in relation to the provision of IT infrastructure or other professional services.

In these circumstances, and where applicable, your personal data will only be transferred on one of the following bases:

1. the transfer is subject to one or more of the "appropriate safeguards" for international transfers prescribed by applicable law (e.g. data transfer assessments and standard contractual clauses as adopted by the European Commission and UK Government respectively);
2. a European Commission decision or a decision by the Home Secretary provides that the country or territory to which the transfer is made ensures an adequate level of protection; or
3. there exists another situation where the transfer is permitted under applicable law (for example, where we have your explicit consent).

Please see Schedule 1 for country specific information.

Data retention

We will retain your Personal Data for as long as is reasonably necessary for the purposes explained in this Notice. This will usually be the period of your employment or other contract with us plus the length of any applicable statutory limitation period following your departure, although some data, such as pension information, may need to be kept for longer. We may keep some specific types of data, for example, tax records, for different periods of time, as required by law and in line with our HR retention schedule.



In some cases we may also retain your Personal Data for longer periods of time so that we have an accurate record of your dealings with us in the event of any complaints or challenges, or if we reasonably believe there is a prospect of litigation relating to your relationship with us. Where your Personal Data is no longer required we will ensure it is either securely deleted or stored in a way that no longer identifies you.

If you would like further details regarding our retention periods please contact the Data Protection and Privacy Office.

Your rights

Under data protection legislation you have the following rights:

- to obtain access to, and copies of, the personal data we hold about you.
- to require that we cease processing your personal data if the processing is causing you damage or distress;
- to require us to correct the personal data we hold if it is incorrect;
- to request that we erase your personal data;
- to request that we restrict our data processing activities in relation to your personal data;
- to object to certain data processing activities and
- the right to not be subject to any automated decision making processes or profiling without the opportunity for human review or intervention.

Please note that the above rights are not absolute, and requests may be refused where exceptions apply. Please see Schedule 1 for Country Specific Information.

If you have any questions about these rights please contact the Data Protection and Privacy Office.

Contact and Complaints

If you have any queries about this privacy notice or how we process your personal data, if you would like to make a complaint or if you wish to exercise any of your rights please contact the Data Protection and Privacy Office at dpo-hub@next15.com or in writing to:

The Data Protection and Privacy Office
60 Great Portland Street,
London,
W1W 7RT

If following such referral, you are still not satisfied with how your personal data is used by Savanta you have the right to complain. Please see Schedule 1 for Country Specific Information.



Changes to this notice

Savanta will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.



Schedule 1 Country Specific Requirements

Australia

Job Applicants

In addition to the information and safeguards set out above if you are a job applicant who resides in Australia or who is being employed by an entity based in Australia, we will also process your personal data in line with the Privacy Act 1988 (No.119,1988 (as amended) and the Australian Privacy Principles (APPs) contained within the Act where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

If your personal data is to be transferred out with Australia, we will take all reasonable step to ensure that the overseas recipient does not breach the APPs in relation to your personal data. This will include at a minimum, due diligence in relation to the third party and ensuring that the contract contains the relevant clauses to ensure the protection of your personal data.

Regulatory Body

Office of the Australian Information Commissioner (OAIC)
<https://www.oaic.gov.au/>

Canada

Savanta and its associated entities would not fall under one of the workplace categories to which The Personal Information Protection and Electronic Document Act 2000 ('PIPEDA') applies.

International Data Transfers

If your personal data is to be transferred out with Canada, we will take all reasonable step to ensure that the overseas recipient will provide an equivalent level of protection as afforded to you under the PIPEDA. This will include at a minimum, due diligence in relation to the third party and ensuring that the contract contains the relevant clauses to ensure the protection of your personal data.

Regulatory Body

Canada Federal –Office of the Privacy Commissioner of Canada (OPC)
<https://www.priv.gc.ca/en/>
Canada Alberta- Alberta Privacy Commissioner (Alberta OIPC)
<https://www.priv.gc.ca/en/>
Canada Quebec - Commission d'accès à l'information du Québec (Québec CAI)
<https://www.cai.gouv.qc.ca/english/>
Canada Ontario – The Office of the Information and Privacy Commissioner of Ontario.
(OIPC) <https://www.ipc.on.ca/>
Canada – Saskatchewan – The Office of the Saskatchewan Information and Privacy
Commissioner (OIPC) <https://oipc.sk.ca/category/news/>

China

In addition to the information and safeguards set out above if you are a job applicant who resides in China or who is being employed by an entity based in China, we will also process



your personal data in line with the Personal Information Protection Law (PIPL) where it gives you protections over and above that set out in the UK/EU GDPR.

Requirements and restrictions in relation to diversity data

If we intend to collect diversity data from candidates, we will only collect such data that might be related to the job posting. If certain types of diversity data falls into the scope of sensitive personal information as defined in PIPL we will obtain separate consent from candidates before collection.

International Data Transfers

If your personal data is to be transferred out with China we will execute a data transfer agreement which will include the standard contractual clauses as provided by the Cyber Space Administration of China (CAC).

Regulatory Body

Cyberspace Administration of China (CAC) (*国家互联网信息办公室*)
<http://www.cac.gov.cn/>

France

In addition to the information and safeguards set out above if you are a job applicant who resides in France or who is being employed by an entity based in France, we will also process your personal data in line with any local legislation where it gives you protections over and above that set out in the UK/EU GDPR.

Disclosure to works councils

We may have to disclose your POO to the Social and economic committees ('CSEs'). With respect to companies with more than 50 employees, the CSE is permitted access to a database containing all the information necessary for its recurrent research and consultation (e.g. indicators necessary to calculate a possible gender pay gap). This information would normally be provided without any identifiable personal data, as names are redacted and data is thus anonymised. If we are ever required to disclose PII to the CSE we will always notify you in advance.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

National Commission for Data Protection (*Commission Nationale de l'Informatique et des Libertés*) (CNIL)
<https://www.cnil.fr/en>

Germany

In addition to the information and safeguards set out above if you are a job applicant who resides in Germany or who is being employed by an entity based in Germany, we will also process your personal data in line with the Federal Data Protection Act ('BDSG') and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

Background checks related to financial or criminal records

Further to the information above in relation to background checks in the case of financial background checks we will only request this for what is known as 'special position of trust'.



These are positions in which the employee has access to cash, accounts, or valuable company secrets. Criminal record checks (e.g., through a police certificate of good conduct) will only be processed where required by law.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Federal - Federal Commissioner for Data Protection and Freedom of Information
(*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*)

https://www.bfdi.bund.de/DE/Home/home_node.html

State - State-level data protection authorities. Each state has their own data protection authority. (Landesdatenschutzbehörden) the link below will take you to a landing page where you can select the data protection authority that covers your area.

<https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html>

Hong Kong

In addition to the information and safeguards set out above if you are a job applicant who resides in Hong Kong or who is being employed by an entity based in Hong Kong, we will also process your personal data in line with The Personal Data (Privacy) Ordinance (Cap.486) ('PDPO') and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

If your personal data is to be transferred out with Hong Kong, we will take all reasonable step to ensure that the overseas recipient will provide an equivalent level of protection as afforded to you under the PDPO. This will include at a minimum, due diligence in relation to the third party and ensuring that the contract contains the relevant clauses as set out in the Guidance on Recommended Model Contractual Clauses for Cross border Transfers of Personal Data as issues by the Office of the Privacy Commissioner for Personal data.

Regulatory Body

Office of the Privacy Commissioner for Personal Data (個人資料私隱專員公署 (PCPD))

<https://www.pcpd.org.hk/>

India

In addition to the information and safeguards set out above if you are a job applicant who resides in India or who is being employed by an entity based in India, we will also process your personal data in line with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules') that have been framed under Section 43A of the Information Technology Act, 2000 ('the IT Act') and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

N/A

Regulatory Body

The Ministry of Electronics and Information Technology

<https://www.meity.gov.in/press-releases>

Italy

In addition to the information and safeguards set out above if you are a job applicant who resides in Italy or who is being employed by an entity based in Italy, we will also process your personal data in line with the Data Protection Code and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali* (GPDP))
[The Italian Data Protection Authority: Who We Are - Garante privacy en - Garante Privacy](#)

Malaysia

In addition to the information and safeguards set out above if you are a job applicant who resides in Malaysia or who is being employed by an entity based in Malaysia, we will also process your personal data in line with the Personal Data Protection Act 2010 (PDPA) and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

If your personal data is to be transferred out of Malaysia, we will take all reasonable step to ensure that the overseas recipient will provide an equivalent level of protection as afforded to you under the PDPA.

Regulatory Body

Department of Personal Data Protection (*Jabatan Perlindungan Data Peribadi*)
<https://www.kkd.gov.my/en/>

Netherlands

In addition to the information and safeguards set out above if you are a job applicant who resides in the Netherlands or who is being employed by an entity based in the Netherlands, we will also process your personal data in line with the Dutch GDPR Implementation Act and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

Further to the information above in relation to special category personal data in the case of health data we will only process this if the processing is necessary to reintegrate or supervise employees or benefit recipients in connection with sickness or occupational disability.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Data Protection Authority (*Autoriteit Persoonsgegevens*).
[Home | Autoriteit Persoonsgegevens](#)



Singapore

In addition to the information and safeguards set out above if you are a job applicant who resides in Singapore or who is being employed by an entity based in Singapore, we will also process your personal data in line with the Personal Data Protection Act 2012 (PDPA) and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

If your personal data is to be transferred out of Singapore, we will take all reasonable step to ensure that the overseas recipient will provide an equivalent level of protection as afforded to you under the PDPA.

Regulatory Body

Personal Data Protection Commission (PDPC).
[Personal Data Protection Commission Singapore | PDPC](#)

Spain

In addition to the information and safeguards set out above if you are a job applicant who resides in Spain or who is being employed by an entity based in Spain, we will also process your personal data in line with the Protection of Personal Data and guarantee of digital rights (SPDA) and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Spanish Data Protection Agency (*Agencia Española de Protección de Datos* (AEPD))
[Agencia Española de Protección de Datos | AEPD](#)

Sweden

In addition to the information and safeguards set out above if you are a job applicant who resides in Sweden or who is being employed by an entity based in Sweden, we will also process your personal data in line with the Sweden's Data Protection Act (Swedish Act) and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

Special Category Personal Data Processing

Further to the information above in relation to special category personal data we will only process this when necessary for us or you to fulfil obligations and exercise rights under labour laws or for social security or social protection purposes.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Privacy Protection Authority (*Integritetsskyddsmyndigheten*) (IMY)
www.imy.se



United Kingdom

In addition to the information and safeguards set out above if you are a job applicant who resides in the United Kingdom or who is being employed by an entity based in the United Kingdom, we will also process your personal data in line with the Data Protection Act 2018 and any local laws where it gives you protections over and above that set out in the UK/EU GDPR.

International Data Transfers

Please see the section on International Data Transfers set out within the body of the Notice.

Regulatory Body

Information Commissioner's Office (ICO)
<https://ico.org.uk/>

United States of America

In addition to the information and safeguards set out above if you are a job applicant who resides in the United States or who is being employed by an entity based in the United States, we will also process your personal data in line with any local state laws addressing employee privacy rights where it gives you protections over and above that set out in the UK/EU GDPR. If you are an employee based in California, please see our "*Privacy Notice for the Collection for California Employees and Applicants*".

Regulatory Body

Given the federalised nature of the US Privacy Framework please see your local implementing legislation.

Definition of Special Categories Data

Special categories data is a specific subset of personal information that includes certain government identifiers (such as social security numbers); an account log-in, financial account, debit card, or credit card number with any required security code, password, or credentials allowing access to an account; precise geolocation; contents of mail, email, and text messages; genetic data; biometric information processed to identify a consumer; information concerning a consumer's health, sex life, or sexual orientation; or information about racial or ethnic origin, religious or philosophical beliefs, or union membership.