

HAYS INTERNAL RECRUITMENT PRIVACY POLICY

INTRODUCTION

- This Internal Recruitment Privacy Policy applies to individuals who are seeking employment with Hays.
- This Internal Recruitment Privacy Policy describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.
- If you indicate that you would also like us to process your personal data to find you suitable roles with Hays' clients or other third parties, our General Privacy Policy will apply to you in respect of this processing. This can be found on our website.
- For the avoidance of doubt, this Internal Recruitment Privacy Policy does not apply to Hays' [Staff](#) when they apply for internal roles – if this is you, please see the separate Staff Privacy Policy which is accessible via the Hays Intranet.
- If you accept an offer of employment with Hays, you should refer to the Staff Privacy Policy for information about how we process [Staff](#) personal data, which will be provided to you during your onboarding process.
- For the purpose of applicable data protection legislation (including but not limited to the [General Data Protection Regulation](#) (Regulation (EU) 2016/679) (the "GDPR"), the company responsible for your personal data ("Hays" or "us") can be found in [Annex 1](#).
- This Internal Recruitment Privacy Policy may be amended from time to time. Please visit this page if you want to stay up to date, as we will post any changes in our approach to data privacy here.
- If you are dissatisfied with any aspect of our Internal Recruitment Privacy Policy, you may have legal rights and so, where relevant, we have described these as well.
- This Internal Recruitment Privacy Policy applies in relevant countries throughout our international network. Different countries may approach data privacy in slightly different ways and so we may also have country-specific parts to this Internal Recruitment Privacy Policy. You can find summaries of country-specific terms in [Annex 3](#). This allows us to ensure that we're complying with all applicable data privacy protections no matter where you are.

WHAT KIND OF PERSONAL DATA DO WE COLLECT ABOUT RECRUITMENT? -

- We collect data about you to enable the [Recruitment](#) process to run smoothly, for example where we have a legitimate interest when considering you for a role and to ensure that we are able to comply with our legal and regulatory obligations. Depending on the relevant circumstances and applicable local laws and requirements, we may collect some or all of the information listed below to help us with this, where appropriate. This is an international policy and it is important to note that in some jurisdictions, we are restricted from processing some of the data outlined below. In such cases, we will not process the data in those jurisdictions. For ease of reference, the most significant examples of data which we are permitted, or even obliged, to process in some jurisdictions, but are prohibited from processing in other jurisdictions, are set out in the second part of the list below:
 - name;

- age/date of birth;
 - contact details, such as address, email address and telephone number;
 - birth identification number;
 - sex/gender;
 - photograph;
 - marital status;
 - CV;
 - education details;
 - employment history and locations of previous employment;
 - referee details;
 - your signature, including in electronic form;
 - immigration status (whether you need a work permit);
 - nationality/citizenship/place of birth;
 - a copy of your driving licence and/or passport/identity card;
 - social security number (or equivalent in your country) and any other tax-related information;
 - details about your current or former role(s) including remuneration, pension and benefits arrangements;
 - extra information that you choose to tell us;
 - extra information that your referees choose to tell us about you;
 - any additional information required by local legislation; and
 - extra information that we find from other third party sources.
- As noted above, some of the more significant examples of data which we process in some jurisdictions, but are prohibited from processing others (and which we accordingly **do not process in such jurisdictions**) include:
 - financial information (including where we need to carry out financial background checks);
 - diversity information including racial or ethnic origin, religious or other beliefs, and physical or mental health, including disability-related information;
 - sexual orientation;
 - biometric information;
 - CCTV footage if you attend our premises;
 - details of any criminal convictions; and
 - communications that you send to Hays which pass through Hays' Systems , including emails, instant messages, social media posts, text messages and app-based messages (such as WhatsApp).
 - Please note that the above lists of the categories of personal data which we collect are not exhaustive.
 - We will process save or all of the above items of personal data to ensure the [Recruitment](#)

process can run smoothly and so that we can make an informed decision about your suitability for the role in question (or other appropriate roles that may be available, depending on the circumstances).

- Depending on the type of personal data in question and the grounds on which we may be processing it, should you decline to provide us with such data, we may not be able to continue with the [Recruitment](#) process.
- For details of the legal bases that we rely on to be able to use and process your personal data, please see the section below entitled "[Legal bases for us processing your data](#)".

HOW DO WE COLLECT YOUR PERSONAL DATA?

We collect your personal data in three primary ways:

1. [Personal data that you give to us](#);
2. [Personal data that we receive from other sources](#); and
3. [Personal data we collect automatically](#).

Below are some more details about each of these methods.

Personal data you give to us

- Hays needs to know certain information about you in order to properly conduct the [Recruitment](#) process.
- There are numerous ways that you can share your information with us. Where appropriate and in accordance with any local laws and requirements, these may include:
 - When you make a job application to Hays via our website or other recruitment portal;
 - When you make a job application to Hays via email;
 - When you make a job application to Hays via job boards (such as Monster and StepStone);
 - When you make a job application to Hays via networking websites (such as LinkedIn);
 - When you make a job application to Hays by submitting a CV or application, whether in hard copy or by electronic means;
 - When you register to receive more information from us at a job fair or other Hays careers event, including requesting that we send you a copy of a presentation we gave, where relevant;
 - When you apply for our mentoring or scholarship programmes;
 - When you fill out a candidate application form at the time of your interview;
 - When you had previously contacted Hays as a candidate, seeking Hays' services in finding employment with a third party organisation;
 - Information you provide to Hays' [Staff](#) in communications during the [Recruitment](#) process;
 - When you fill out our matchmaker test on our website (if available in your jurisdiction).

Personal data we receive from other sources

- We also receive personal data about you from other sources. Depending on the relevant circumstances and applicable local laws and requirements, these may include personal data received in the following situations:
 - information obtained about you when we searched third party sources such as LinkedIn and other job sites for potential [Recruitment](#) for roles at Hays;

- when a member of Hays' [Staff](#) refers you to us, for example via our internal recruitment teams, they will share personal information about you with us;
- if you were referred to us through a recruitment agency or consultant, they may have shared personal information about you with us;
- information obtained by one of our internal recruitment teams who received your information, for example, via a career website or graduate career book;
- information obtained via third parties such as former Hays employees who recommend you for a role;
- information obtained about you from third party service providers who undertake background checks about you on our behalf;
- your referees may disclose personal information about you to us; and
- if you 'like' our page on Facebook or 'follow' us on Twitter (or similar), we will receive your personal information from those sites.

Personal data we collect automatically

- Where appropriate and in accordance with any local laws and requirements, we may collect your personal data automatically the following ways:
 - communications that you send to Hays which pass through Hays' [Systems](#), including emails, instant messages, social media posts, text messages and app-based messages (such as WhatsApp).
 - when you visit our website, your IP address, the date and the times and frequency with which you access the website and the way you browse its content. We will also collect data from you when you contact us via the website, for example by using the chat function.
 - via cookies when you visit our website, in line with cookie settings in your browser. We may use data from your use of our websites to enhance other aspects of our communications with you. If you would like to find out more about cookies, including how we use them and what choices are available to you, please see our [General Privacy Policy](#).

HOW DO WE USE YOUR PERSONAL DATA?

We generally use [Recruitment](#) data in the following ways:

1. [To ensure the smooth running of the Recruitment process](#)
2. [Assessing your suitability for job roles](#);
3. [To undertake equal opportunities monitoring](#) (where applicable and in accordance with local law requirements);
4. [To help us to establish, exercise or defend legal claims](#); and
5. [To help us to help you and to understand our legal obligations if you suffer from a health condition or disability](#).

Below are some more details about each of these purposes.

To ensure the smooth running of the [Recruitment process](#)

- We have listed below various ways in which we may process or use your personal data for this purpose, where appropriate and in accordance with any local laws and requirements:
 - Collecting your data from you and other sources, such as your referees;
 - Passing on your details to recruiters who assist us with finding new members of [Staff](#);

- Enabling recruiters to contact you about the role;
- Enabling our hiring managers to decide whether to make you a job offer;
- Determining the terms on which you will work for us;
- Internal recruiters passing your details on to our hiring managers, to discuss your suitability for a role at Hays;
- Assessing your qualifications for a particular job or task, including decisions about appointment;
- Informing you of the result of your job application;
- Verifying information we have received, using third party resources (such as psychometric evaluations or skills tests) or through information requests (such as references, qualifications and potentially any criminal convictions, to the extent that this is appropriate and in accordance with local laws);
- Storing and transferring your details (and updating them when necessary) on and between our internal recruitment databases and applicant tracking systems;
- Complying with our legal obligations in connection with the detection of crime or the collection of taxes or duties;
- Keeping a record of when you attend an interview or other assessment;
- When making arrangements in order to offer you a job;
- Carrying out satisfaction surveys on our [Recruitment](#) process;
- Subject to specific local law requirements (acknowledging in some of the jurisdictions in which we operate, the extent to which it is permissible to carry out some of these forms of processing is limited):
 - monitoring communications that you send to Hays which pass through Hays' [Systems](#), including emails, instant messages, social media posts, text messages and app-based messages (such as WhatsApp);
 - keeping a record of security data so that we can be sure who is on our premises at any given time; and
 - running CCTV at our premises to ensure the safety and security of our [Staff](#) and property.
- Carrying out any other obligations or necessary requirements arising from the [Recruitment](#) process;
- If you are successful in being appointed to a role, transferring your personal data onto our internal HR systems; and
- If you are unsuccessful in your application for a role with Hays, we may process your personal data to introduce you to another member of the Hays team to discuss whether you wish for us to continue to process your personal data to help you to find a role with one of our clients. In those circumstances, you would become a 'candidate' and the terms of our General Privacy Policy would apply.

Assessing your suitability for job roles

- In addition to the usual human resources processes, as technology advances, it may be possible in the future for us to use machine learning, profiling and algorithms to help us to make [Recruitment](#) decisions and to more accurately assess your suitability for job roles and to help us make other decisions in our [Recruitment](#) processes. This is an exciting

opportunity for us to improve our business processes and to ensure that we all enjoy a successful workplace. In relevant circumstances, and where legally permissible, we may require your consent to carry out some of these activities.

To undertake equal opportunities monitoring

- We are committed to ensuring that our [Recruitment](#) processes are aligned with our approach to equal opportunities. In some jurisdictions, where the processing of such data is permissible in accordance with local law requirements, some of the data we may collect about you comes under the umbrella of "diversity information". This could be information about your ethnic background, gender, disability, age, sexual orientation, religion or other beliefs, child care / carer arrangements and/or social-economic background. Where appropriate and only in accordance with local law and requirements, we'll use this information on an anonymised basis to monitor our compliance with equal opportunities requirements.

To help us to establish, exercise or defend legal claims

- In more unusual circumstances, we may use your personal data to help us to establish, exercise or defend legal claims.

To help us to help you and to understand our legal obligations if you suffer from a health condition or disability

- If you suffer from any health conditions or disabilities, we may, subject to local laws and requirements, record details of them so that we can make reasonable adjustments to interview and other [Recruitment](#) procedures if required.

Please note that the above list of the ways in which we use your personal data for this purpose is not exhaustive.

We will only use your personal data for the purposes for which we collect 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 data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

To find out more about the legal bases that we rely on to be able to use and process your personal data in the above ways, please see the section below entitled "[Legal bases for us processing your data](#)".

Please note that in certain of the jurisdictions in which we operate, additional rules may apply in respect of how we use your personal data. For more information in relation to any such additional rules in your jurisdiction, please see [Annex 3](#).

WHO DO WE SHARE YOUR PERSONAL DATA WITH?

- Where appropriate and in accordance with local laws and requirements, we may share certain of your personal data, in various ways and for various reasons, with the following categories of people:
 - any of our group companies (this may include those in our overseas offices);
 - your family and personal representatives;
 - external third party organisations (for example those which carry out psychometric testing), business associates and professional advisers, to enable us to assess your suitability for the role;
 - where relevant, recruiters who will help us to find the right role for you;
 - individuals and organisations who hold information related to your reference or

application to work with us, such as current, or past employers, educators and examining bodies, immigration agencies and employment and recruitment agencies;

- third parties, in order to comply with our legal obligations, for example in relation to immigration requirements;
- third parties who hold information related to your financial record such as financial organisations, credit reference agencies and debt collection and tracing agencies;
- where appropriate, medical professionals such as your GP or an occupational health specialist;
- third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors, accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems;
- third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place;
- third parties involved in, or assisting with, litigation (including legal advisers, witnesses, experts and judicial and quasi-judicial authorities);
- third parties who we have retained to provide services such as reference, qualification and criminal convictions checks, to the extent that these checks are appropriate and in accordance with local laws; and
- if Hays merges with or is acquired by another business or company in the future, (or is in meaningful discussions about such a possibility) we may share your personal data with the (prospective) new owners of the business or company.

HOW DO WE SAFEGUARD YOUR PERSONAL DATA?

- We care about protecting your information. That's why we put in place appropriate measures that are designed to prevent unauthorised access to, and misuse of, your personal data. These include measures to deal with any suspected data breach.
- We are committed to taking all reasonable and appropriate steps to protect the personal data that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures.
- If you suspect any misuse or loss of or unauthorised access to your personal data please let us know immediately. Details of how to contact us can be found in [Annex 1](#).

HOW LONG DO WE KEEP YOUR PERSONAL DATA FOR?

- Subject to your rights (as explained in this Internal Recruitment Privacy Policy) we will ordinarily process your data from when you first contact us and retain it for a period until after the [Recruitment](#) process ends. The precise length of time will depend the type of data, our legitimate business needs and other legal or regulatory rules that may require us to retain it for certain minimum periods. For example, we may retain it for a certain period to comply with local law requirements in relation to immigration checks, or to enable us to respond to any queries you may have about the [Recruitment](#) process in the future.
- In determining the appropriate retention period for different types of personal data, we always consider the amount, nature, and sensitivity of the personal data in question, the potential risk of harm from unauthorised use or disclosure of that personal data, the purposes for which we need to process it and whether we can achieve those purposes by

other means (in addition of course to ensuring that we comply with our legal, regulatory and risk-management obligations, as described above).

- Once we have determined that we no longer need to hold your personal data, we will [Delete](#) it from our [Systems](#).

HOW CAN YOU ACCESS, AMEND OR TAKE BACK THE PERSONAL DATA THAT YOU HAVE GIVEN TO US?

One of the [GDPR's](#) main objectives is to protect and clarify the rights of EU citizens and individuals in the EU with regard to data privacy. Even if we already hold your personal data, you still have various rights in relation to it, which we have set out below.

To get in touch about these rights (including if you wish to exercise any of them), please contact us using the details listed in [Annex 1](#). We will seek to deal with your request without undue delay, and in any event within one month (subject to any extensions to which we are lawfully entitled). Please note that we may keep a record of your communications to help us resolve any issues which you raise.

The [GDPR](#) gives you the following rights in relation to your personal data:

Right to object

- This right enables you to object to us processing your personal data where we do so for one of the following four reasons: (i) because it is within our legitimate interests (ii) to enable us to perform a task in the public interest or exercise official authority; (iii) to send you direct marketing materials; and (iv) for scientific, historical, research, or statistical purposes.
- The "legitimate interests" category above is the one most likely to apply in relation to our [Recruitment](#) processes, and if your objection relates to us processing your personal data because we deem it necessary for our legitimate interests, we must act on your objection by ceasing the activity in question unless:
 - we can show that we have compelling legitimate grounds for processing which overrides your interests; or
 - we are processing your data for the establishment, exercise or defence of a legal claim.

Right to withdraw consent

- Where we have obtained your consent to process your personal data for certain activities (for example, for automatic profiling), you may withdraw this consent at any time and we will cease to carry out the particular activity that you previously consented to unless we consider that there is an alternative legal basis to justify our continued processing of your data for this purpose, in which case we will inform you of this condition.

Right to submit a data subject access request (DSAR)

- You may ask us to confirm what information we hold about you at any time, and request us to modify, update or [Delete](#) such information. We may ask you for more information about your request. If we provide you with access to the information we hold about you, we will not charge you for this unless your request is "manifestly unfounded or excessive". If you request further copies of this information from us, we may charge you a reasonable administrative cost, where legally permissible. Where we are legally permitted to do so, we may refuse your request. If we refuse your request we will tell you the reasons for doing so.
- Please note that in certain of the jurisdictions in which we operate, we comply with additional local law requirements regarding data subject access requests and may refuse

your request in accordance with such laws. For more information in relation to any such additional requirements in your jurisdiction, please see [Annex 3](#).

Right to erasure

- You have the right to request that we "erase" your personal data in certain circumstances. Normally, the information must meet one of the following criteria:
 - the data are no longer necessary for the purpose for which we originally collected and/or processed them;
 - where previously given, you have withdrawn your consent to us processing your data, and there is no other valid reason for us to continue processing;
 - the data has been processed unlawfully (i.e. in a manner which does not comply with the [GDPR](#));
 - it is necessary for the data to be erased in order for us to comply with our obligations as a data controller under EU or Member State law; or
 - if we process the data because we believe it necessary to do so for our legitimate interests, you object to the processing and we are unable to demonstrate overriding legitimate grounds for our continued processing.
- Please note that in certain of the jurisdictions in which we operate, we comply with additional local law requirements regarding the data subject right to erasure and may refuse your request in accordance with local laws. For more information in relation to any such additional requirements in your jurisdiction, please see [Annex 3](#).
- We would only be entitled to refuse to comply with your request for erasure for one of the following reasons:
 - to exercise the right of freedom of expression and information;
 - to comply with legal obligations or for the performance of a public interest task or exercise of official authority;
 - for public health reasons in the public interest;
 - for archival, research or statistical purposes; or
 - to exercise or defend a legal claim.
- When complying with a valid request for the erasure of data, we will take all reasonably practicable steps to [Delete](#) the relevant data.

Right to restrict processing

- You have the right to request that we restrict our processing of your personal data in certain circumstances. This means that we can only continue to store your data and will not be able to carry out any further processing activities with it until either: (i) one of the circumstances listed below is resolved; (ii) you consent; or (iii) further processing is necessary for either the establishment, exercise or defence of legal claims, the protection of the rights of another individual, or reasons of important EU or Member State public interest.
- The circumstances in which you are entitled to request that we restrict the processing of your personal data are:
 - where you dispute the accuracy of the personal data that we are processing about you. In this case, our processing of your personal data will be restricted for the period during which the accuracy of the data is verified;

- where you object to our processing of your personal data for our legitimate interests. Here, you can request that the data be restricted while we verify our grounds for processing your personal data;
- where our processing of your data is unlawful, but you would prefer us to restrict our processing of it rather than erasing it; and
- where we have no further need to process your personal data but you require the data to establish, exercise, or defend legal claims.
- If we have shared your personal data with third parties, we will notify them about the restricted processing unless this is impossible or involves disproportionate effort. We will, of course, notify you before lifting any restriction on processing your personal data.

Right to rectification

- You also have the right to request that we rectify any inaccurate or incomplete personal data that we hold about you, including by means of providing a supplementary statement. If we have shared this personal data with third parties, we will notify them about the rectification unless this is impossible or involves disproportionate effort. You may also request details of the third parties that we have disclosed the inaccurate or incomplete personal data to. Where we think that it is reasonable for us not to comply with your request, we will explain our reasons for this decision.

Right of data portability

- If you wish, you have the right to transfer your personal data between data controllers. In effect, this means that you are able to transfer the details we hold on you to another potential employer or a third party. To allow you to do so, we will provide you with your data in a commonly used machine-readable format so that you can transfer the data to another potential employer. Alternatively, we may directly transfer the data for you. This right of data portability applies to: (i) personal data that we process automatically (i.e. without any human intervention); (ii) personal data provided by you; and (iii) personal data that we process based on your consent or in order to fulfil a contract.

Right to lodge a complaint with a supervisory authority

- You also have the right to lodge a complaint with your local supervisory authority. Details of how to contact them can be found in [Annex 2](#).

If you would like to exercise any of these rights, or withdraw your consent to the processing of your personal data (where consent is our legal basis for processing your personal data), details of how to contact us can be found in [Annex 1](#). Please note that we may keep a record of your communications to help us resolve any issues which you raise.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the period for which we hold your data.

WHO IS RESPONSIBLE FOR PROCESSING YOUR PERSONAL DATA?

- You can find out which Hays entity is responsible for processing your personal data and where it is located in [Annex 1](#).
- If you have any comments or suggestions concerning this Internal Recruitment Privacy Policy please contact us using the details in [Annex 1](#). We take privacy seriously so we'll get back to you as soon as possible.

HOW DO WE STORE AND TRANSFER YOUR DATA INTERNATIONALLY?

- Hays is a global recruiter – this is what enables us to offer the level of services that we do.

In order for us to continue operating in this way and to carry out the purposes described in this Internal Recruitment Privacy Policy, your data may be transferred to the following recipients located outside of your jurisdiction:

- between and within Hays entities;
 - to a cloud-based storage provider; and
 - to other third parties, as referred to above under "[Who do we share your personal data with?](#)"
- We want to make sure that your data are stored and transferred in a way which is secure. We will therefore only transfer data outside of the European Economic Area or EEA (i.e. the Member States of the European Union, together with Norway, Iceland and Liechtenstein) where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, for example:
 - by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission for the transfer of personal data by data controllers in the EEA to data controllers and processors in jurisdictions without adequate data protection laws;
 - by signing up to the EU-U.S. Privacy Shield Framework for the transfer of personal data from entities in the EU to entities in the United States of America or any equivalent agreement in respect of other jurisdictions;
 - where we are transferring your data to a country where there has been a finding of adequacy by the European Commission in respect of that country's levels of data protection via its legislation;
 - where it is necessary for the conclusion or performance of a contract between ourselves and a third party and the transfer is in your interests for the purposes of that contract (for example, if we need to transfer your data to a benefits provider based outside the EEA); or
 - where you have consented to the data transfer.
 - To ensure that your personal information receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share your personal data with to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the law on data protection.

LEGAL BASES FOR US PROCESSING YOUR DATA

There are a number of different ways that we are lawfully able to process your personal data. We have set these out below.

Where processing your personal data is within our legitimate interests

- Article 6(1)(f) of the [GDPR](#) is relevant here – it says that we can process your data where it *"is necessary for the purposes of the legitimate interests pursued by [us] or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of [you] which require protection of personal data."*
- We consider the following to be non-exhaustive examples of processing activities that are in our legitimate interests to carry out so that we can run a successful [Recruitment](#) process:
 - assessing your suitability for a role at Hays;
 - informing you of the result of your job application;

- for our internal administrative purposes;
 - to make appropriate background checks; and
 - to assist us with establishing, exercising or defending legal claims.
- You can find further examples of ways in which we process your personal data for the purposes of our legitimate interests in the non-exhaustive list above under the heading, "[To ensure the smooth running of our recruitment process](#)".

Where processing your personal data is necessary for us to carry out our legal obligations

- As well as our obligations to you that arise in connection with our [Recruitment](#) processes, we also have other legal obligations that we need to comply with. Article (6)(1)(c) of the [GDPR](#) states that we can process your personal data where this processing "*is necessary for compliance with a legal obligation to which [we] are subject*".
- Examples of our legal obligations can be found in the non-exhaustive list set out above under the heading, "[To ensure the smooth running of our recruitment processes](#)".

Where processing your [Sensitive Personal Data](#) is necessary for us to exercise our rights or carry out our employment and social security law obligations

- Sometimes it will be necessary for us to process your [Sensitive Personal Data](#) during the course of the [Recruitment](#) process. Article 9(2)(b) of the [GDPR](#) allows us to do this where the processing is "*necessary for the purposes of carrying out the obligations and exercising [our or your] specific rights... in the field of employment and social security and social protection law*", as long as this is allowed by law.
- We process your [Sensitive Personal Data](#) for the purpose of ensuring our compliance with our [equal opportunities](#) obligations where this is in accordance with local law, but we may also process other elements of your [Sensitive Personal Data](#) during the course of the [Recruitment](#) process for other reasons. You can find out how we process your [Sensitive Personal Data](#) in the context of the [Recruitment](#) process in the non-exhaustive list under "To ensure the smooth running of the [Recruitment](#) process".
- Where appropriate and in accordance with any local laws and requirements, we may also process your medical data to enable us to provide you with adequate support if you suffer from a health condition or disability, in order to determine any reasonable adjustments to interview or other [Recruitment](#) procedures. You can find out more about this [here](#).
- Please note that in certain of the jurisdictions in which we operate, additional rules apply to how we process your [Sensitive Personal Data](#). For more information in relation to any such additional requirements in your jurisdiction, please see [Annex 3](#).

Where processing your personal data is necessary for us to establish, exercise or defend legal claims

- Sometimes it may be necessary for us to process personal data and [Sensitive Personal Data](#) in connection with exercising or defending legal claims. Article 9(2)(f) of the [GDPR](#) allows this where the processing "*is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity*".
- This may arise for example where we need to take legal advice in relation to legal proceedings or are required by law to preserve or disclose certain information as part of the legal process.

Where you give us your consent to process your personal data

- In very limited circumstances, we are required to obtain your opt-in consent before we can

undertake certain processing activities with your personal data. Article 4(11) of the [GDPR](#) states that opt-in consent is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*" In plain language, this means that:

- you have to give us your consent freely, without us putting you under any type of pressure;
 - you have to know what you are consenting to – so we'll make sure we give you enough information;
 - you should only be asked to consent to one processing activity at a time – we therefore avoid "bundling" consents together so that you don't know exactly what you're agreeing to; and
 - you need to take positive and affirmative action in giving us your consent – we're likely to provide a tick box for you to check so that this requirement is met in a clear and unambiguous fashion.
- As and when we introduce these processing activities requiring your consent, we will provide you with more information so that you can decide whether you want to opt-in.
 - Please note that in certain of the jurisdictions in which we operate, we comply with additional local law requirements regarding obtaining consent. For more information in relation to any such additional requirements in your jurisdiction, please see [Annex 3](#).
 - You have the right to withdraw your consent to these activities. You can do so at any time, and details of how to do so can be found above in the section entitled, "Right to withdraw consent".

We don't think that any of the above activities prejudice you in any way. However, you do have the right to object to us processing your personal data in certain circumstances. If you would like to know more about these circumstances and how to object to our processing activities, please see the subsection entitled "[Right to object](#)".

ANNEX 1 – HOW TO CONTACT US

<p>Country in which you apply to become a member of Hays' Staff</p>	<p>The Hays entity responsible for processing your personal data will depend on which of the below companies is the counterparty associated with the relevant arrangement</p>	<p>How you can get in touch with us:</p> <ul style="list-style-type: none"> • to access, amend or take back the personal data that you have given to us; • if you suspect any misuse or loss of or unauthorised access to your personal information; • to withdraw your consent to the processing of your personal data (where consent is the legal basis on which we process your personal data); • with any comments or suggestions concerning this Internal Recruitment Privacy Policy
<p>Germany</p>	<ul style="list-style-type: none"> • Hays AG, Mannheim • Hays Professional Solutions GmbH, Düsseldorf • Hays Talent Solutions GmbH, Düsseldorf • Hays Technology Solutions GmbH, Mannheim • Hays Holding GmbH, Mannheim 	<p>You can write to us at the following address: Hays AG Datenschutzbeauftragter/DPO, Willy-Brandt-Platz 1-3, 68161, Mannheim, Germany</p> <p>Alternatively, you can send an email to our German data protection officer and the data protection team at: datenschutz@hays.de</p>

ANNEX 2 – HOW TO CONTACT YOUR LOCAL SUPERVISORY AUTHORITY

Country in which you apply to become a member of Hays' Staff	Details of your local supervisory authority
Germany	<p>For the entities located in Mannheim, Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.</p> <ul style="list-style-type: none">• Post: Postfach 10 29 32, 70025 Stuttgart• Email: poststelle@lfdi.bwl.de• Phone: (+49) 0711/61 55 41 – 10• Fax: 0711/61 55 41 – 15 <p>For the entities located in Dusseldorf, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.</p> <ul style="list-style-type: none">• Post: Postfach 20 04 44, 40102 Düsseldorf• Email: poststelle@ldi.nrw.de• Phone: +49 (0)211/384 24 – 61; +49 (0)211/38424 – 86• Fax: 0211/384 24 – 10

ANNEX 3 – COUNTRY-SPECIFIC VARIATIONS TO OUR INTERNAL RECRUITMENT PRIVACY POLICY

JURISDICTION	COUNTRY SPECIFIC LEGAL REQUIREMENT
<p>Germany</p>	<p>Nothing in this Internal Recruitment Privacy Policy shall authorise Hays to collect and process your personal data in breach of the local data protection laws and regulations in this jurisdiction and the specific requirements set out by the local Data Protection Authority concerning the collection or processing of specific types of data, including Sensitive Personal Data.</p>
	<p>In Germany, we collect details of our Recruits' religious affiliation to facilitate our payroll process. As this is a necessary legal requirement, we don't seek your explicit consent to process this information.</p>
	<p>In Germany, your personal data may be processed for employment-related purposes where necessary for hiring decisions.</p> <p>Recruits' personal data may be processed to detect crimes only if there is a documented reason to believe that the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.</p> <p>In Germany, the processing of Sensitive Personal Data of Recruits for employment-related purposes is permitted if it is necessary to exercise rights or comply with legal obligations derived from labour law, social security and social protection law, and there is no reason to believe that you have an overriding legitimate interest in not processing the data.</p>
	<p>In Germany, consent must be provided in written form, unless a different form is appropriate because of extraordinary circumstances. If we obtain your consent for the processing of your Sensitive Personal Data, the consent must explicitly refer to these data.</p>
	<p>A Data Protection Officer (Datenschutzbeauftragter/DPO) has been appointed by Hays Germany in accordance with German national legislation (Bundesdatenschutzgesetz). They are responsible for the Hays Germany entities and you can find their contact details in Annex 1.</p>
	<p>In accordance with local law, we have the right to refuse to respond to your DSAR in circumstances where your data are only being held: (i) pursuant to a legal obligation to retain them; or (ii) for the purposes of monitoring data protection or safeguarding data, in each case where providing the information would require a disproportionate effort, and appropriate technical and organisational measures make processing for other purposes impossible.</p>

Where your data are not being processed in an automated way, unless your data are being processed unlawfully, we will not be required to erase your data if erasure would be impossible or would involve a disproportionate effort due to the specific method of storage, provided that we think your interest in erasure is minimal.

Where your data are being processed in an automated way, we will also have the right to refuse to erase your data if we have reason to believe that such erasure will adversely affect your legitimate interests, or if such erasure would cause us to breach any legal obligation to retain your data for a specific period. Instead, in these circumstances, processing of your data will be restricted in the particular ways envisaged by the GDPR.

As explained in the "*How long do we keep your personal data for?*" section above, we will retain your data for the statutory retention periods prescribed by law. An overview of the statutory retention periods which apply to Hays in Germany is available by contacting your local HR team.

Please note that we might retain your personal data for a longer period than prescribed by law provided that this is necessary for employment-related purposes, justified by our legitimate business needs, and/or other statutory rules.

GLOSSARY

- **Delete** – In this day and age, it is virtually impossible to guarantee the permanent and irretrievable deletion of electronic data. In addition, as we have explained to you in this Internal Recruitment Privacy Policy, sometimes we may be obliged by law or regulation, or need for risk-management reasons, to retain the ability to access certain elements of personal data. However, our commitment to you is that once your personal data reaches the end of its nominal retention period, or where we receive a valid request from you to erase it, we will put in place specific operational and Systems measures to ensure that your data is "put beyond use". By this we mean that while the data will still technically exist on an archive system, we will ensure that it cannot be accessed by any of our operational Systems, processes or Staff. Only a very (and we mean exceptionally) small number of senior Staff, in very (and, again, we mean exceptionally) limited and carefully prescribed situations, be able to restore your personal data so that it can be viewed for those legitimate purposes. Once we are clear that all relevant legally mandated retention periods have expired (which, for present purposes, we expect to be the period of up to nine months, unless we are legally required to hold your personal data for longer than this), we will go the additional final step of undertaking a "hard delete", whereby not even that very limited number of senior Staff would be able to restore your personal data.
- **General Data Protection Regulation (the "GDPR")** – a European Union statutory instrument which aims to harmonise European data protection laws. It has an effective date of 25 May 2018, and any references to it should be construed to include any national legislation implementing it.
- **Recruitment** – this refers to individuals who are seeking employment as members of Hays' Staff. It does not apply to candidates, that is applicants and potential applicants for all roles advertised or promoted by Hays on behalf of its clients or other third parties.
- **Sensitive Personal Data** – this is personal data consisting of information such as your racial or ethnic origin, your political opinions or religious beliefs, whether you are a trade union member, your physical and mental health, your genetic and biometric data, data relating to your sex life and sexual orientation, and whether you have or are alleged to have committed a criminal offence. Due to the nature of Sensitive Personal Data, data protection legislation is much stricter about how such data should be held and processed. We will only process your Sensitive Personal Data where appropriate and in accordance with local law requirements.
- **Staff** – includes current and former employees and interns engaged (or who have accepted an offer to be engaged) directly in the business of Hays as well as certain other workers who are or were engaged in the business of providing services to Hays (even though they are not classed as employees). For these purposes we also include employees of Hays who are engaged to work on client premises under the terms of a Recruitment Process Outsourcing (RPO) or Managed Service Provider (MSP). For illustrative purposes, it is generally the case that if an individual is granted access to the Hays Intranet, they will be covered by the terms of the Staff Privacy Policy, rather than this Internal Recruitment Privacy Policy.
- **Systems** – include telephone, computer, internet and Wi-Fi systems, software and portals, accounts and/or networks belonging, controlled or used by Hays that are used to transmit, undertake and/or receive communications or are otherwise used in the course of Hays' business, including candidate portal software and CRM systems.