

Data Privacy Notice for
Henley & Partners Candidates or Job Applicants

DATA PRIVACY NOTICE FOR HENLEY & PARTNERS CANDIDATES OR JOB APPLICANTS

A. INTRODUCTION

The Henley & Partners Group (“we”, “us”, “our” or “Henley”) is committed to maintaining the highest standards in data privacy, confidentiality and information security. Henley is committed to protecting the privacy and security of your personal information.

This notice applies to candidates or job applicants only.

We process your data in an appropriate and lawful manner, in accordance with the applicable laws and regulations to which Henley is subject, including without limitation the general Data Protection Regulations (Regulations (EU) 2016/679, herein “GDPR”) which is in force as of 25 May 2018.

For the purpose of these data protection laws, the Henley entity that is to be your Employer is a Data Controller (as defined in the GDPR). This means that we are responsible for deciding how we hold and use personal information about you. You are provided with a copy of this privacy notice because you are applying to work with us. The purpose of this notice is to set out the basis on which your personal data is processed by us, and to make you aware of how we handle your personal data, our obligations in regard to processing your personal data responsibly as well as your data protection rights.

We will comply with local data protection laws in jurisdictions we operate in and to do so the personal information we hold about you must be:

1. used by us lawfully, fairly and in a transparent way;
2. collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
3. relevant to the purposes we have told you about and limited only to those purposes;
4. accurate and kept up to date;
5. kept only as long as necessary for the purposes we have told you about; and
6. kept securely.

We have appointed a Data Protection Officer (the “DPO”) who can be contacted regarding any comments, questions, queries or complaints regarding Data Protection or the processing of your personal data, using the details set out below:

Mr Sorin Brici
Henley & Partners Austria GmbH
Linke Wienzeile 8/14
1060 Vienna
Austria
Email: DPO@henleyglobal.com

You can address any comments, queries or complaints to this address with words “Data Protection Matter” in the subject line.

For non-EU Henley employees, Henley & Partners Group Holdings Ltd, Aragon House, Dragonara Road, Saint Julians’ Malta STJ 3140, acts as the EU Data Representative of Henley & Partners Group companies located outside the European Economic Area (“EEA”). You may address any issue, queries or concerns which you may have with regards to data protection to the EU Data Representative by sending an email with “Data Protection Matter” in the subject line to the following address:

Henley & Partners Group Holdings Ltd.
Aragon House
Dragonara Road
St Julian’s STJ 3140
Malta
Email: eurepresentative@henleyglobal.com

B. INFORMATION WE PROCESS

The personal data we will collect, process, use or store in connection with your application to work with us will include the following categories of personal information: (i) information you have provided in your application form, including name, title, address, telephone number, personal email address, date of birth, gender, employment history, educational degrees and qualifications; (ii) information set out in your CV and covering letter, including past and present work experience/employers; (iii) any information you provide us during an interview; and (iv) a copy of your passport and/or national ID.

We may also collect, process, store and use the following ‘special categories’ of more sensitive personal information (“Sensitive Data”): (i) original of your passport and/or national ID with regards to the potential work opportunity, in order to comply with local employment law obligations in jurisdictions we operate in; (ii) information about criminal convictions or offences, we will only collect information about

criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so, usually prior to the recruitment of an employee we request a police clearance certificate and/or good conduct certificate from jurisdictions you have been/are resident in; and (iii) any health related data, including any medical condition, health or sickness records for the purposes of ensuring your health and safety in the workplace and assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness or health. In such situations, we may request that you provide a valid medical certificate to ensure you are fit to work.

C. LEGAL BASIS OF PROCESSING

1. How is your personal information collected?

We collect personal information about you through the application and recruitment process, directly from you.

We may also collect information about you from other sources. Such other sources include employment agencies or recruiters or other third parties who introduced you to us. We may also collect information about you through former employers or colleagues who may provide us with references about you.

We may obtain personal data from you from public sources prior to the commencement of employment, when we carry out internal background checks on you. We may also use due diligence or compliance software for this purpose and in certain cases we may even procure a background verification report from a third party service provider such as HireRight. If we are to procure a verification report, we will always notify you prior to carrying this out in order to obtain your explicit consent.

2. How we will use your personal information

We will use personal information we collect about you to:

- verify your skills, qualifications and suitability for the role we intend to hire you for;
- carry out background or reference checks, where applicable;
- communicate with you about the recruitment process;
- keep records relating to our hiring process; and
- comply with legal or regulatory requirements in jurisdictions we operate in.

We will need to process your personal information to decide whether or not to enter into a contract of employment with you. We will use your personal data primarily to perform and fulfill our recruitment obligations and to comply with local law employment obligations in each of the jurisdictions we operate in.

In some limited circumstances, we may use your personal information to pursue legitimate interest of our own or those of third parties, provided your interests and fundamental rights do not override those interests. With regards to Sensitive Data, we may use or process this type of data in the following circumstances: (i) in limited circumstances, where we have obtained your explicit consent; (ii) where we need to carry out legal obligations or exercise rights in connection with your recruitment; or (iii) where it is needed and required in the public interest, such as for equal opportunities monitoring.

3. Do we need your consent to process your personal data?

We do not need your consent if we use your personal information prior to employment because we process your data based on the legal grounds listed above.

In certain cases however it may be necessary for us to obtain your prior (explicit) consent and that is if the purpose of the processing cannot be based on one of the legal grounds listed above.

Automated decision-making takes place when an electronic system uses personal information to make decisions without human intervention. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

4. If you fail to provide personal information

If you fail to provide certain information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to perform our recruitment obligations successfully or we may be prevented from complying with our legal obligations in jurisdictions that we operate in. For example, if we require a background check to be completed or references to be provided for this role and you fail to provide us with relevant details, we will not be able to take your application further.

5. 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 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, compatible with the rules set out above, where this is permitted by applicable law i.e. where we have a legal ground to process your data.

D. DISCLOSURE OF PERSONAL INFORMATION TO OTHER MEMBERS OF HENLEY & PARTNERS GROUP

There may be instances where personnel of other members of the Henley & Partners Group (for a full list of Henley & Partners Group companies please visit our webpage at (<https://www.henleyglobal.com/worldwide-offices/>) get involved in the recruitment process and therefore your personal information will be shared with those Henley group companies.

All Henley & Partners Group companies respect the security of your personal information and treat it in accordance with the data protection laws in the jurisdictions we operate (including the GDPR) and apply the security measures and safeguards as described below in section G.

E. SHARING YOUR PERSONAL INFORMATION WITH THIRD PARTIES

As part of the due diligence and Know Your Employee/Associated Persons procedure we conduct on job applicants we may share your personal data, including a passport copy and your CV, with a third party due diligence/background verification report provider, such as HireRight, whom we may commission to conduct further due diligence on you. Where such service providers store and process your data in their capacity as data processors they will do it on the basis of strict confidentiality and subject to the appropriate security measures and safeguards as described below in section G. Where such service providers process your personal data in their own right (in their capacity as data controllers) we may provide you with their data privacy notice relating to your personal data.

We may also be required to share your personal information with government authorities in the country where you seek to obtain employment i.e. for work permit or visa purposes.

F. TRANSFER OF PERSONAL INFORMATION TO THIRD COUNTRIES

Where we share your personal data with internal or external third parties, this may in some instances involve transferring your personal information outside the jurisdiction where your potential employer is established and sometimes outside the EEA.

With regards to transferring your data outside the EEA, we will transfer your personal information in accordance with the EU Commission standard contractual clauses (European Commission: Model contracts for the transfer of personal information to third countries) to ensure your personal information is transferred securely and in compliance with data protection legislation, including the GDPR.

G. DATA SECURITY

We have put in place appropriate security measures to prevent your personal information against unlawful or unauthorized processing of personal information, and against accidental loss of, or damage to, personal information. Such measures shall include (but are not limited to): (a) encrypting the personal information which we process, (b) ensuring the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that we use; (c) ensuring that the availability of and access to personal information can be restored in a timely manner after an accident; (d) regularly assessing and evaluating the effectiveness of the technical and organizational measures adopted; and (e) carrying out a data protection impact assessment prior to implementing a new set of processing operations.

All personal information is stored in a secure environment and we have physical and electronic data access controls in place whereby access is granted only to persons authorized to access the data on a need to know basis, all of whom process personal data with our instructions and are bound by confidentiality obligations not to disclose any personal information.

We have data integrity controls in place which include firewalls, antivirus software, backup and recovery systems and internal and external network penetration testing.

We have put in place a procedure 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. Please contact us on DPO@henleyglobal.com for further details with respect to our technical and organizational security measures.

No method of transmission of data is one hundred percent (100%) secure and absolute security cannot be guaranteed.

H. DATA STORAGE

Should your application be unsuccessful we will only retain your personal information for a period of 6 months after we have communicated to you our decision to not appoint you for the specified role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates/job applicants on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way.

After this period, we will securely destroy your personal information in accordance with our data retention policy and the applicable data protection laws and regulations in jurisdictions we operate in.

Should we make the decision to offer you the specified role and we enter into an employment agreement, we will then provide you with our Privacy Notice for Employees which will further inform you about how we handle your personal data as an employee of Henley.

I. DATA MINIMISATION

Whenever and to the extent possible, we anonymize the data which we hold about you when it is no longer necessary to identify you from the personal information which we hold about you.

J. YOUR DUTY TO INFORM US OF CHANGES

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 your recruitment process with us.

K. YOUR RIGHTS IN CONNECTION WITH PERSONAL INFORMATION

You are entitled to exercise the following rights:

a. Right to Access Information

You have the right to request information as to whether or not your personal information is being processed by us as well as information as to how and why it is processed. You may send an email to DPO@henleyglobal.com requesting information as to the personal information which we process on you individually. You shall receive one copy free of charge via email of the personal

information which is undergoing processing. We may charge a reasonable fee, if your request is clearly unfounded, repetitive or excessive in which case we may also refuse to comply with your request in these circumstances.

b. Right to Object

You may ask us not to process your personal information for certain purposes, for example, marketing purposes, and your data will no longer be processed for such purposes.

c. Right to Correction

You have the right to ask for correction of any inaccurate personal information about you that we have processed, update any data which is out-of-date and the right to have incomplete personal information completed, including by means of a supplementary statement.

d. Right to Erasure

You have the right to obtain the erasure of personal information we have concerning you when your personal information is no longer required where:

- you withdraw your consent to us processing your personal information;
- your personal information no longer needs to be processed; or
- your personal information has been unlawfully processed.

e. Right to Restriction of Processing

You have the right to restrict our processing activities where:

- you contest the accuracy of this personal information, for a period enabling us to verify the accuracy of the same personal information;
- our processing is deemed unlawful, and you oppose the erasure of your personal information and request restriction of its use instead;
- we no longer need your personal information for the purposes stated in this notice, but you require it for the establishment, exercise or defense of legal claims; or
- you have objected to our processing pending the verification whether the legitimate grounds of our processing activities overrode those pertaining to you.

f. Right of Data Portability

As from 25 May 2018, you shall have the right to receive your personal information in a structured and machine-readable format and transmit this data to another Data Controller (as defined in the GDPR).

L. RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information 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, unless we have another legitimate basis for doing so in law.

M. COMPLAINTS

We welcome any comments, complaints and queries in relation to data protection. As indicated above, you may contact our DPO at DPO@henleyglobal.com and we shall try our best to deal with any issue or concern you may have.

If we fail to address your concerns you have the right to lodge a complaint with the data protection authority in the jurisdiction you or the Henley entity (your potential recruiter) is based in or if the Henley entity you are dealing with is based outside the EEA you may lodge a complaint with the Information and Data Protection Commissioner in Malta at www.dataprotection.gov.mt.