

## Privacy Statement – Recruitment Services

Applicable Ltd understands the importance of ensuring that we collect, use, store, disclose, share, and dispose of (collectively ‘use’) information about you (‘personal data’, including ‘personal information’ as it may be defined under applicable data protection laws and regulations) in a fair, open, secure, and lawful way. This Privacy Statement – Recruitment Services (“Privacy Statement”) describes what personal data relating to you we hold, how we use it, and your choices and rights in relation to your personal data. This Privacy Statement applies to our use of personal data in relation to the Applicable’s recruitment processes and other related initiatives.

Please note that any use of Applicable’s websites, including any collection of personal data, other than in a recruitment context is subject to Applicable’s Privacy Statement for Website located at <https://www.applicable.com/en/information-security-and-privacy/>

We use your personal data in compliance with applicable data protection laws and regulations and Works Council Agreements (where applicable), based on the country in which you are seeking employment.

### Legal basis for using your personal data

When we process your personal data in connection with the purposes set out in this Privacy Statement, we may rely on one or more of the following legal bases, depending on the purpose for which the processing activity is undertaken:

- our legitimate interests as a global employer, or those of a third party, including for the purposes of recruitment, human resources management, managing our interactions with you, and record keeping in relation to recruiting and hiring; except where our interests are overridden by your interests or fundamental rights or freedoms which require the protection of personal data;
- for the purposes of entering into an employment contract with you and/or performance and administration of your employment contract if you are employed by us;
- where this is necessary to comply with a legal obligation placed on us;
- to protect the vital interests of any individual;
- where you have provided your consent.

## Collection, use, and disclosure of personal data

### Personal data we collect

Personal data is any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to you. We will generally collect personal data from you directly when you apply for a position with us. However, we may also collect personal data about you from third parties, including third party recruitment agents, interviewers, prior employers, your identified referees, and employment screening and vetting service providers, as well as publicly available sources (such as LinkedIn), to the extent permitted by applicable law.

The types of personal data that we collect about you and how that personal data is collected and accessed will depend on the employment laws, and data protection and privacy laws of the country in which the position you apply for is located.

Personal data that we may collect either directly or indirectly during the recruitment process can include:

- your name, email address, telephone or mobile number;
- your CV, resume, or cover letter and any documents in support of your job application;
- details submitted by you through a third-party recruitment agent and by recruiters when searching for jobs, creating a profile, and applying for job with Applicable;
- identification information, such as proof of identity;
- current and previous employment information (including salary, bonus, benefits and allowances), where permitted;
- references from your nominated referees and/or your previous employers;
- educational qualifications and achievements;
- results of any pre-employment testing such as skills testing (where required) and psychometric testing (where permitted and required);
- interview notes and video interviews;
- nationality, immigration status, passport, and work permits;
- job preferences such as willingness to travel and/or relocate;
- information obtained from background checks, where permitted;
- information relating to any previous job applications you have made to us and/or any previous employment with Applicable where this information is retained by Applicable;
- contact preferences;
- National Insurance / Tax number

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

We require certain information about you to support our recruitment process ('mandatory information'). If this information is not provided, our ability to consider you as a candidate may be limited.

### **How we use particularly sensitive personal data**

"Special categories" of particularly sensitive personal information require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent:
- Where we need to carry out our legal obligations and in line with our data protection policy.
- Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our data protection policy.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Where it is necessary for establishing, exercising or defending legal claims.

Less commonly, we may process this type of information where it is to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already

### **Information about criminal convictions**

We envisage that we will need to undertake and hold information about criminal convictions; this as a legitimate interest to satisfy obligations placed upon Applicable by our Customers, for the prevention of fraud and protection of the business against criminal activity.

We will use information about criminal convictions and offences as part of the recruitment process to establish whether or not to offer you a role.

The processing will be in accordance with our data protection policy, information security policy and other Applicable policies.

Checks regarding criminal convictions will be performed by a third party organisation and the information will be provided to you and to us. We will

advise you who the third party organisation is before this occurs and confirm your agreement to proceed and you will need to provide the necessary information to this third party. Applicable will bear all costs for this activity.

### How we collect your personal data

We may collect your personal data from you in a variety of ways, including:

- publicly available databases;
- social networking sites (such as LinkedIn), including when you include a link to your profile on any social networking site as part of your job application;
- third parties, including recruiters and placement firms, outsourcing providers, nominated references, previous employers; and referees;
- You contacting Applicable through our website and subsequent communications;
- You contact Applicable through our employees, and they introduce you to the role for which you are submitting an application.

### Use of your personal data

All personal data may be used for the purposes stated in this Privacy Statement.

We may use your personal data to:

- identify and contact you throughout the recruitment process;
- enable our personnel or recruitment agencies to search for you in databases to help us identify suitable candidates for vacancies;
- determine your suitability for current job opportunities with us;
- process your job application, and if successful, the details of your employment with us;
- check information provided by you, or third parties, including qualifications and references;
- perform administrative functions (e.g. keeping records in relation to recruiting and hiring);
- understand our applicant pool in order to better understand who is applying for roles at Applicable and how to attract top talent;
- record online interviews for review by recruiters and hiring managers if you expressly agree to being recorded;
- opt-you-in to our global talent database that you may receive future alerts about our job vacancies and events where you have registered to do so;
- comply with applicable laws and regulations;

- conduct or defend legal proceedings;
- improve our recruitment and hiring processes;

### **Disclosing your personal data**

We may disclose your personal data for any of the purposes set out in this Privacy Statement with:

- authorised personnel, including human resources personnel such as hiring managers, other interviewers, and IT and administrative support staff;
- agents and professional advisers of Applicable;
- authorised third party service providers providing services to Applicable, including placement firms, recruiters and other service providers;
- authorised personnel of third parties including companies who perform background checks. These companies may be based in another country to where your personal data is collected, and may obtain data from other countries where you have lived, worked or studied;
- auditors and investigators in connection with internal and external audits and investigations;
- third parties to provide references at your request or with your consent;
- a competent authority in accordance with, or as required by any applicable law, regulation or legal process;

### **Data sold or shared**

We do not sell or share personal data about job applicants and candidates.

### **Data disclosed for a business purpose**

We have disclosed the following categories of personal data about job applicants and candidates for business or commercial purposes:

- personal information and references to verify identity and confirm references.

Any third parties who process personal data on our behalf are contractually required to implement appropriate data protection and security measures to protect personal data and are not permitted to use personal data for any purpose other than the purpose for which they are provided with or given access to personal data.

## Security of your personal data

We are committed to protecting your personal data from accidental or unlawful destruction, loss, or alteration, and unauthorised access or disclosure by using a combination of physical, administrative, and technical safeguards and requiring that third parties to whom we disclose your personal data do the same.

## Retaining your personal data

We will retain your personal data for as long as is reasonably necessary and proportionate to fulfil the purpose for which it was collected, processed, or for another disclosed purpose, unless a longer retention period is required to comply with legal obligations, resolve disputes, protect our assets, or enforce our rights. The criteria we use to determine retention periods include whether:

- we are under a legal, contractual or other obligation to retain personal data, or as part of an investigation or for litigation purposes;
- personal data is needed to maintain accurate business and financial records;
- the personal data is sensitive personal data in which event we will generally retain this for a shorter period of time;
- you have consented to us retaining your personal data for a longer retention period, in which case, we will retain personal data in line with your consent.

If you become our employee, personal data collected during the recruitment process will become part of your employee record, which we will retain during your employment and for a period after your employment ceases (in accordance with country-specific privacy laws).

If we don't employ you, we may retain and use personal data collected during your application in accordance with our retention policies and schedules and applicable country-specific laws and regulations:

- to consider you for new and current job opportunities;
- for system administration;
- to perform research and analysis; and

Thereafter, we retain the minimum amount of your personal data necessary to record your recruiting interactions with us and, where possible, deidentify your personal data so that you can no longer be identified for the purposes of statistical reporting.

If we don't employ you, we may retain and use personal data collected during your application in accordance with our retention policies and schedules and applicable country specific laws and regulations:

- to consider you for new and current job opportunities;
- for system administration;
- to perform research and analysis; and

If you choose not to, we will record that fact and will only retain the minimum personal data necessary to ensure that we do not contact you again.

Thereafter, we retain the minimum amount of your personal data necessary to record your recruiting interactions with us and, where possible, deidentify your personal data so that you can no longer be identified for the purposes of statistical reporting.

## Your privacy rights

Data protection laws and regulations, in certain countries, provide you with specific rights in relation to your personal data. We are committed to upholding the following privacy rights:

- **Right to be informed / know:** you have a right to know what personal data, including the types of sensitive personal data, we have about you, what we do with it, where we get it from, who we disclose it to and share it with, how long we keep it and why we need it.
- **Right of access:** you have the right to access your personal data and obtain a copy of your personal data from us.
- **Right to correct:** you have the right to update inaccurate and/or incomplete personal data about you. We will review all information provided by you to us, to determine whether the information is inaccurate. We reserve the right to delete the information instead of correcting if such deletion does not impact you or you consent to the deletion of your personal data.
- **Right to delete:** you have the right to have your personal data erased, deleted or destroyed (i.e. right to be forgotten).
- **Right to data portability:** you have the right to move, copy or transfer your personal data in a safe and secure way and reuse it for your own purposes.
- **Right to withdraw consent:** you have the right to withdraw consent at any time regarding the use of your personal data (where applicable) or in relation to direct marketing activities.
- **Right to restrict use:** you have the right to limit the way we use your personal data.
- **Right to object:** you have the right to stop or prevent us from using your personal data. In particular, you can object to our use of your personal data for direct marketing or the sale of your personal data.

- **Right to challenge automated decisions:** you have the right to query and review decisions made about you using purely automated means (i.e. without human involvement or intervention).
- **Right to complain:** you have the right to make a complaint or raise a concern about how we use your personal data. Complaints may be made directly to us or a relevant Data Protection Authority.
- **Right to non-discrimination:** you have the right not to be discriminated against for exercising your privacy rights.

You may submit a request to enforce your rights at any time.

You can make a request regarding your privacy rights by contacting us through the following ways:

- Sending an email to [dpo@applicable.com](mailto:dpo@applicable.com)
- Write to us at Applicable Ltd, 3120 Great Western Court, Hunts Ground Road, Stoke Gifford, Bristol, BS34 8HP.

When you submit a request to us, you must provide sufficient information to allow us to verify that you are the person about whom the personal data relates. This information must contain sufficient detail to allow us to properly understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request.

Once we receive your request, we will begin the process to verify that you are the person that is the subject of the request. This may include matching identifying information provided by you with the information we have about you in our records.

Where permitted under applicable law, we may charge you a reasonable fee to access your personal data; however, we will advise you of any fee in advance.

Applicable will respond to all requests and complaints in accordance with our Data Subject Rights Policy and will acknowledge any requests within 10 days and respond substantively within 30 days.

We will retain correspondence, documents and information related to any requests or complaints for a period of 24 months or as required by any applicable laws and regulations.

In some situations, we may not be required to enforce these rights under applicable law and where exceptions may apply. We may also have a legitimate business interest to decline a request to action your rights. These exceptions to your rights may include our right to maintain personal data of job applicants and candidates for business purposes and solely internal uses reasonably aligned with the expectations as a job applicant or candidate, as well as to comply with any legal obligations, including maintaining proper records, or maintaining privilege or confidentiality of certain records, in compliance with applicable laws and regulations. We will inform you of our



decision to deny or grant your request and of any other action we have taken to respond to your request and enforce your rights.

### **Authorised agent Information?**

You may designate an authorised agent to make a request on your behalf. When your authorised agent makes a request related to your personal data, we will require the agent to provide written permission from you. We may also require that you verify your own identity directly with us at the time such a request is made. You or your authorized agent may contact us with requests, complaints, or questions regarding these rights.

### **How we use automated decision-making**

Automated decision-making refers to any time that we apply an algorithm or use artificial intelligence or related technologies to make a decision about you without human intervention.

We do not make any decisions about you using automated means, however, should our position change in this regard, we will update this Privacy Statement and inform you of your rights in accordance with relevant laws and regulations.

### **Cross border transfers**

Applicable operates in the United Kingdom, United States of America and Australia as well as using sub processors. We may transfer your personal data to countries where we do business or to international organisations in connection with the purposes identified above and in accordance with this Privacy Statement.

Your personal data may be accessed by authorised Applicable personnel, authorised service providers, and recruiters, and other stakeholders as identified in this Privacy Statement, both in the country where the position for which you are applying is based, as well as different countries in which Applicable operates in connection with the purposes identified in and in accordance with this Privacy Statement.

When we transfer your personal data outside of the country from where it was originally collected to a third country or international organization, we ensure that appropriate safeguards are in place, in line with applicable law, to ensure that your personal data is protected. You may obtain a request for details of these safeguards by contacting us.

### **Links to third party websites and applications**

Applicable may use third party websites for recruitment services.

We are not responsible for and make no representations or warranties in relation to the security, privacy practices and content of these websites.

Please ensure that you read the applicable privacy and cookies policies before sharing personal data on these websites. Your use of such websites is at your own risk. You may also interact with us through social media plug-ins by “liking” or sharing information related to Applicable careers and job postings. Social media plug-ins are operated by the social network themselves (such as Facebook, LinkedIn, etc.) and are subject to the terms of use, and privacy and cookies policies of the respective social network.

Please ensure that you are familiar with these.

### How to contact us?

- Sending an email to [dpo@applicable.com](mailto:dpo@applicable.com)
- Write to us at Applicable Ltd, 3120 Great Western Court, Hunts Ground Road, Stoke Gifford, Bristol, BS34 8HP.

### DataRep

Following the UK's exit from the European Union, as of the 1st January 2021 we are required to provide a Data Protection Representative within the EEA allowing data subjects to raise matters directly to this representative for the purposes of the EU GDPR. Applicable have appointed DataRep to undertake this role on our behalf and they can be contacted by email at [applicable@datarep.com](mailto:applicable@datarep.com) or at the postal address locations in the table below. Please note that when mailing enquiries, it is essential that you mark your letters for attention of 'DataRep' and not Applicable Ltd, but please refer clearly within your correspondence to Applicable Ltd.

Country	Address
Austria	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
Belgium	DataRep, Place de L'Université 16, Louvain-La-Neuve, Waals Brabant, 1348, Belgium
Bulgaria	DataRep, 132 Mimi Balkanska Str., Sofia, 1540, Bulgaria
Croatia	DataRep, Ground & 9th Floor, Hoto Tower, Savska cesta 32, Zagreb, 10000, Croatia
Cyprus	DataRep, Victory House, 205 Archbishop Makarios Avenue, Limassol, 3030, Cyprus
Czech Republic	DataRep, IQ Ostrava Ground floor, 28. října 3346/91, Ostrava-mesto, Moravska, Ostrava, Czech Republic
Denmark	DataRep, Lautruphøj 1-3, Ballerup, 2750, Denmark
Estonia	DataRep, 2 <sup>nd</sup> Floor, Tornimäe 5, Tallinn, 10145, Estonia
Finland	DataRep, Luna House, 5.krs, Mannerheimintie 12 B, Helsinki, 00100, Finland
France	DataRep, 72 rue de Lessard, Rouen, 76100, France
Germany	DataRep, 3rd and 4th floor, Altmarkt 10 B/D, Dresden, 01067, Germany
Greece	DataRep, 24 Lagoumitzi str, Athens, 17671, Greece
Hungary	DataRep, President Centre, Kálmán Imre utca 1, Budapest, 1054, Hungary

<b>Iceland</b>	DataRep, Kalkofnsvegur 2, 101 Reykjavík, Iceland
<b>Ireland</b>	DataRep, The Cube, Monahan Road, Cork, T12 H1XY, Republic of Ireland
<b>Italy</b>	DataRep, Viale Giorgio Ribotta 11, Paiono 1, Rome, Lazio, 00144, Italy
<b>Latvia</b>	DataRep, 4th & 5th floors, 14 Terbatas Street, Riga, LV-1011, Latvia
<b>Liechtenstein</b>	DataRep, City Tower, Brückenkopfgasse 1/6. Stock, Graz, 8020, Austria
<b>Lithuania</b>	DataRep, 44A Gedimino Avenue, 01110 Vilnius, Lithuania
<b>Luxembourg</b>	DataRep, BPM 335368, Banzelt 4 A, 6921, Roodt-sur-Syre, Luxembourg
<b>Malta</b>	DataRep, Tower Business Centre, 2nd floor, Tower Street, Swatar, BKR4013, Malta
<b>Netherlands</b>	DataRep, Cuserstraat 93, Floor 2 and 3, Amsterdam, 1081 CN, Netherlands
<b>Norway</b>	DataRep, C.J. Hambros Plass 2c, Oslo, 0164, Norway
<b>Poland</b>	DataRep, Budynek Fronton ul Kamienna 21, Krakow, 31-403, Poland
<b>Portugal</b>	DataRep, Torre de Monsanto, Rua Afonso Praça 30, 7th floor, Algès, Lisbon, 1495-061, Portugal
<b>Romania</b>	DataRep, 15 Piața Charles de Gaulle, nr. 1-T, București, Sectorul 1, 011857, Romania
<b>Slovakia</b>	DataRep, Apollo Business Centre II, Block E / 9th floor, 4D Prievozska, Bratislava, 821 09, Slovakia
<b>Slovenia</b>	DataRep, Trg. Republike 3, Floor 3, Ljubljana, 1000, Slovenia
<b>Spain</b>	DataRep, Calle de Manzanares 4, Madrid, 28005, Spain
<b>Sweden</b>	DataRep, S:t Johannesgatan 2, 4th floor, Malmo, SE - 211 46, Sweden
<b>Switzerland</b>	DataRep, Leutschenbachstrasse 95, ZURICH, 8050, Switzerland

### Updates to this Privacy Statement

We may update this Privacy Statement at any time for any reason. If we do, we will update the “Last Updated” information at the bottom of this Privacy Statement.

We encourage you to regularly review this Privacy Statement to stay informed about our privacy practices and whenever you submit personal data to us.